İSTANBUL ÜNİVERSİTESİ YAYINEVİ

İdare Hukuku ve İlimleri Dergisi, 23: 179-225

DOI: 10.26650/ihid.24.005
http://dergipark.gov.tr/iuihid
http://ihid.istanbul.edu.tr

İdare Hukuku ve İlimleri Dergisi

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

Başvuru: 20.05.2024
Revizyon Talebi: 15.11.2024
Son Revizyon: 17.11.2024
Kabul: 20.11.2024
Online Yayın: 25.11.2024

Hizmet Kusurunu Siber Alana Uyarlama Çabasına Bir Öneri Olarak: Dijital Hizmet Kusuru

As a Proposal for the Effort to Harmonize the Service Fault to Cyberspace: Digital Service Fault

Egemen Karaca*

Öz

Bu çalışma, Türk İdare Hukuku'nda mündemiç, idarenin kusura dayanan sorumluluğunu ifade etmek için kullanılan hizmet kusuru teorisinin, günden güne gelişen ve hızlı bir şekilde değişen dijital dünyaya uyum sağlayamaması nedeniyle mevcut sorumluluk şartlarının dijital ortamın kendine özgü özelliklerini dikkate alarak idarenin dijital ortamdaki faaliyetlerinden kaynaklanan kusurlu sorumluluğuna uyarlanmasını önermektedir. Bunu yaparken de mevcut teori olan hizmet kusuru kavramı ile karışmaması ve faaliyetin görüldüğü ortamın özelliklerinin vurgulanması için dijital hizmet kusuru kavramı kullanılmaktadır. Bu kapsamda dijital hizmet kusuru kavramı, idarenin dijital ortamdaki kamu hizmeti ve kolluk faaliyetlerinden kaynaklanan kusurlu davranışlarının tazmininde kullanılabilecek bir sorumluluk kavramı olarak önerilmektedir. Dijital hizmet kusuru kavramı lex lata içerisinde yer almamaktadır. Bu nedenle çalışma kapsamında, lex ferenda açısından idarenin dijital dünyadaki kusurlu davranışlarından kaynaklanan zararlara yönelik sorumluluğunun, hizmet kusurundan belirli yönlerden farklılaşmasına ve bunun da ayrı bir kavramla nitelendirilmesine yönelik gerekliliği açıklamak amaçlanmaktadır. Kavramın ileri sürülmesine ilişkin temel dayanak noktası, klasik sorumluluk şartlarının mevcut haliyle dijital ortamdaki idarenin faaliyetlerinden kaynaklanan mali sorumluluk uyuşmazlıklarına uygulanması halinde kuvvetle muhtemel zarara uğrayan taraf açısından hakkaniyetli sonuçlar veremeyecek olması düşüncesidir. Bu doğrultuda dijital hizmet kusuru, idarenin sorumluluk şartlarının dijital ortama özgü nitelikler dikkate alınarak güncellenmesi ihtiyacına bir öneri olarak sunulmaktadır. Dijital hizmet kusuru ve hizmet kusuru, sorumluluğun ilk şartı olan idari davranış unsuruna göre birbirinden ayırt edilebilecektir. Bu çerçevede hizmet kusuru/dijital hizmet kusuru ayrımını ilk olarak, idari davranışın idarenin dijital kamu hizmeti yahut dijital ortamdaki kolluk faaliyeti kapsamında olup olmaması belirleyecektir. Bu nedenle dijital alandaki bir faaliyet unsuru, her iki teoriyi birbirinden ayıran bir özellik gösterecektir. Bununla birlikte eğer uyuşmazlık dijital hizmet kusuru kapsamında değerlendiriliyorsa yani idarenin dijital alandaki bir faaliyetinden kaynaklanıyorsa artık zarar, illiyet bağı ve kusur unsurları yönünden mevcut hizmet kusuru teorisinden ayrılan, farklı bir değerlendirme yapılması ihtiyacı ortaya çıkacaktır. Nitekim çalışma kapsamında da neden böyle bir ihtiyaç olduğu, sorumluluk şartları ele alınarak açıklanmaya çalışılmaktadır. Çalışma kapsamında ulaşılan sonuç ister dijital hizmet kusuru ister başka bir kavram ile nitelendirilsin, idarenin dijital ortamdaki faaliyetlerinden kaynaklanan kusurlu davranışlarında zararların giderilebilmesi için mevcut kavramların ve şartların bu ortama özgü özellikler dikkate alınarak geliştirilmesine ihtiyaç olduğudur.

Anahtar Kelimeler

Siber güvenlik • Kişisel veriler • Dijital varlıklar • İdarenin mali sorumluluğu • Dijital kamusal alan

* **Sorumlu Yazar:** Egemen Karaca (Arş. Gör.) Dokuz Eylül Üniversitesi, Hukuk Fakültesi, İdare Hukuku Anabilim Dalı, İzmir, Türkiye. E-posta: egemen.karaca@deu.edu.tr, ORCID: 0000-0003-3851-0092
Atıf: Karaca, Egemen. "As a Proposal for the Effort to Harmonize the Service Fault to Cyberspace: Digital Service Fault" (2024) 23 İdare Hukuku ve İlimleri Dergisi 179. https://doi.org/10.26650/ihid.24.005

Abstract

This study proposes the adaptation of the current liability conditions to the unique characteristics of the digital environment, addressing the fault-based liability of the administration under Turkish Administrative Law. The theory of service fault, which is traditionally used to express the fault-based liability of the administration, has been unable to keep pace with the rapidly evolving and changing digital world. While doing so, the concept of "digital service fault" is used to avoid confusion with the existing theory of service fault and to emphasize the characteristics of the environment in which the activity occurs. In this context, the concept of digital service fault is proposed as a liability concept that can be used to compensate for the administration's faulty actions arising from its public service and administrative law enforcement activities in the digital environment. The concept of digital service fault does not exist in Lex Lata. Therefore, this study aims to explain the necessity of differentiating the administration's liability for damages caused by its faulty actions in the digital domain from service fault in certain respects and the need for this differentiation to be conceptualized separately from a Lex Ferenda perspective. The main rationale behind proposing this concept is the concern that applying the classical liability conditions as they currently stand to financial liability disputes arising from the administration's activities in the digital environment would likely fail to yield fair results for the injured party. In this regard, the digital service fault is presented as a suggestion for updating the administration's liability conditions by considering the specific characteristics of the digital environment. Digital service fault and service fault can be distinguished based on the element of administrative conduct, which constitutes the first condition of liability. Within this framework, the distinction between service fault and digital service fault will primarily be determined by whether the administrative conduct falls within the scope of the administration's digital public service or its law enforcement activity in the digital environment. Therefore, an activity element in the digital realm can serve as a distinguishing characteristic between these two theories. However, if the dispute is evaluated within the scope of digital service fault—meaning it originates from an activity of the administration in the digital environment—a need arises for a different assessment that departs from the existing service fault theory in terms of the elements of damage, causation, and fault. Accordingly, this study aims to explain why such a need exists by analyzing the conditions of liability. The conclusion reached in this study, regardless of whether it is labelled digital service fault or another concept, is that to remedy damages arising from the administration's faulty actions in the digital environment, there is a need to develop the existing concepts and conditions by considering the specific characteristics of this domain.

Keywords

Cybersecurity • Personal data • Digital assets • Financial liability of administration • Digital public domain

Giriş

Teknolojinin gün geçtikçe gelişmesi neticesinde, kamu hizmetlerinin yürütülmesine hâkim olan değişkenlik ve uyarlama ilkesi uyarınca teknolojik gelişmelerin kamu hizmetlerine entegre edilmesi bir ihtiyaç olup hizmetin gereği gibi işleyebilmesi için beraberinde bir çağa ayak uydurma zorunluluğu da getirmektedir. Bu kapsamda son yıllarda birçok kamu hizmeti dijital ortama aktarılmış ve kamu hizmetlerinde dijital dönüşüm süreci oldukça hızlanmıştır. Hizmetlerin dijitalleşmesinin sağladığı faydalar, dijital ortamın kendine özgü risklerini de beraberinde getirmektedir. Bu risklerden biri de idarenin dijital ortamdaki faaliyetlerinde yetersiz kalması durumunda mali açıdan sorumluluğunun doğması ihtimalidir. İdarenin mali açıdan sorumluluğu aslen kusura dayanmakla birlikte, bazı durumlarda kusuru bulunmasa bile sorumlu olduğu risk ve kamu külfetleri karşısında eşitlik ilkesine dayanan iki tür sorumluluk esası bulunmaktadır. İdarenin kusura dayanan sorumluluğunu ifade etmek için kullanılan hizmet kusuru kavramı bu çalışmanın yola çıkış noktasını oluşturmaktadır.

Hizmet kusurunun, idarenin kusura dayanan mali sorumluluğunu ifade etmek için kullanılan bir kavram olmasına karşın bazı yönlerden idarenin dijital alandaki faaliyetlerden kaynaklanan sorumluluğunu karşılamasında yetersiz kaldığı düşüncesiyle mevcut çalışma hazırlanmaktadır. Nitekim dijital alandaki varlıkların kendine özgü özellikleri, kusurun yoğunluğu meselesi, kitlesel zarar görme potansiyeli, zararın tespit ve değerlemesi, kusurun kime atfedileceği sorunu, dijital ortamdaki idari davranış ve zarar arasındaki illiyet bağı ilişkisi gibi birçok konu idarenin dijital alandaki faaliyetlerinden kaynaklanan zararlardaki sorumluluğunu etkileyebilecek özelliğe sahiptir. Bu sayılanlar idarenin sorumluluk şartlarına işaret etmektedir. Diğer bir ifadeyle idarenin dijital alandaki faaliyetlerinden kaynaklanan sorumluluğunda, çalışma bakımından kusura dayanan sorumluluğunda, sorumluluk şartlarının belirli yönlerden geliştirilmesine ihtiyaç duyulmaktadır. Bu gibi farklılaşan faktörler ve dijital ortamın kendine özgü özellikleri dikkate alınarak idarenin dijital alandaki faaliyetlerinden kaynaklanan sorumluluğuna yönelik hizmet kusurunun özel bir alt türü olarak dijital hizmet kusuru kavramının kullanılması önerilmektedir.

Bu çalışma hizmet kusuru kavramının ve uygulamasının değişen ve gelişen teknolojik çağda belirli meseleler açısından yetersiz kaldığı düşüncesinden yola çıkarak lex ferenda açısından dijital hizmet kusuru gibi farklı bir kavrama gerek duyulduğuna dikkat çekmek amacıyla hazırlanmaktadır. Bu nedenle çalışmadan beklenen çıktı, daha sonradan bu konuda yapılacak çalışmalarda kümülatif düşünce temelinde mevcut çalışmanın eleştirilip değerlendirilerek idarenin dijital alandaki sorumluluk anlayışının oluşmasına ve gelişmesine katkı sunulabilmesidir.

I. Dijital Hizmet Kusuru Kavramı

Dijital hizmet kusuru kavramını ortaya koyabilmek için bu kavramın neyi ifade ettiği, neyi ifade etmediği ve bu kavrama neden ihtiyaç duyulduğuna yönelik gerekçelerimiz üç başlıkta sorulan sorularla açıklanmaya çalışılacaktır. Böylelikle kavramın kapsamının ve sınırlarının daha rahat anlaşılabileceğini ve hizmet kusurundan ayrı olarak neden bir kavram önerilmesi amacı güttüğümüzü daha kolay izah edebileceğimizi düşünüyoruz. Ayrıca bu soruların, gelecekte ortaya çıkacak teknolojik ve hukuki gelişmelerin ilerleyen zamanlarda kavrama ve kavramın öneriliş amacına uyarlanabilmesini kolaylaştıracağına inanıyoruz.

A. Dijital Hizmet Kusuru Kavramı Neyi İfade Etmektedir?

Türkiye Cumhuriyeti Anayasası'nın 125'inci maddesinin birinci fıkrası ve son fıkrası Türk İdare Hukuku öğretisinde idarenin mali sorumluluğunun temellerini oluşturmaktadır. Dijital hizmet kusuru, hizmet kusurunun özel bir alt türü olarak önerildiğinden öncelikle kısaca hizmet kusurundan bahsetmekte fayda bulunmaktadır. İdarenin sorumluluğunun şartlarından biri olan hizmet kusuru, özel hukuktaki haksız fiilden farklı olup[1] idare hukukuna özgü bir kavramdır.[2] Kusuru niteleyen hizmet kelimesi, kusurun idari faaliyet türleri olan[3] kamu hizmeti ve kolluktan kaynaklandığını ifade etmektedir. Bu çerçevede idarenin faaliyetleri dolayısıyla hizmet kusurunun meydana gelebileceği söylenebilir. İdare hukuku öğretisinde hizmet kusuru, idarenin hizmetlerinin kuruluş ve işleyişlerinde meydana gelen aksaklıklar olarak ifade edilmektedir. Hizmetin geç işlemesi, hizmetin kötü işlemesi ve hizmetin hiç işlememesi görünümünde üç şekilde ortaya çıkabilmektedir.[4] Niteliği gereği anonimdir yani belirli bir kişi yahut gruba indirgenemez.[5] Diğer bir ifadeyle kusurun idarenin personelinin davranışına izafe edilmesine gerek olmayıp, idari faaliyetin kuruluş

[1] İdarenin sorumluluğunu haksız fiil sorumluluğuna dayandıran aksi yöndeki görüş ve bu görüşe yönelik eleştiriler için bkz. Turgut Tan, *İdare Hukuku* (9th edn, Turhan 2020) 475.

[2] Ali Ulusoy, *Yeni Türk İdare Hukuku* (Yetkin 2019) 560; Kemal Gözler, *İdare Hukuku Cilt 2* (3rd edn, Ekin 2019) 1084.

[3] Klasik ayrımda idarenin faaliyetleri kamu hizmeti ve kolluk faaliyeti olarak sınıflandırılmaktadır. Ancak farklı görüşlerde kamu hizmeti ve kolluk faaliyetleri yanında idarenin özendirme ve destekleme, regüle etme gibi faaliyetlerinin de bulunduğu belirtilmekte ve kamu hizmeti faaliyetine ek olarak bu faaliyetler de ayrı başlıklandırma yöntemiyle sayılmaktadır. Bu konuda bkz. Aydın Gülan, *İdare Hukuku Ders Notları* (İstanbul Üniversitesi Hukuk Fakültesi) 133 <https://cdn.istanbul.edu.tr/FileHandler2.ashx?f=2015-2016-idare-hukuku-ders-notlari-teskilat-haric.pdf> Erişim Tarihi 20 May 2024; özendirme ve destekleme faaliyeti hakkında bkz. Necip Taha Gür, *İdarenin Özendirme ve Destekleme Faaliyeti* (On İki Levha 2019) 25; özendirme ve destekleme faaliyeti yanında öngörme ve alternatif belirtme, özyönetim işlerinin de ayrı bir faaliyet olarak değerlendirilmesine yönelik bkz. Ramazan Yıldırım and Serkan Çınarlı, *Türk İdare Hukuku Dersleri Cilt: II* (Astana 2019) 229, 238, 252. Biz çalışmamızda klasik ayrım olan kamu hizmeti ve kolluk faaliyeti sınıflandırmasını esas alacağız. Klasik ayrıma yönelik bkz. Bahtiyar Akyılmaz, Murat Sezginer and Cemil Kaya, *Türk İdare Hukuku* (17th edn, Seçkin 2023) 585,614.

[4] Lütfi Duran, *Türkiye İdaresinin Sorumluluğu: Sorumluluğun Temeli ve Sebepleri, Sorumluluğa Yol Açan Olgular* (TODAİE 1974) 28-30.

[5] Ragıp Sarıca, 'Hizmet Kusuru ve Karakterleri' (1949) 15(4) İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 858; Anonimlikten çıkarak belirli bir kişi ya da guruba indirgenebilen ve on(lar)a atfedilebilen görev kusuru ise hizmet kusurunun bir parçası olmayıp hizmet içindeki kişisel kusurun bir türüdür bkz. Oğuz Sancakdar, Lale Burcu Önüt, Eser Us Doğan, Mine Kasapoğlu Turhan and Serkan Seyhan, *İdare Hukuku Teorik Çalışma Kitabı* (11th edn, Seçkin 2022) 855; Yasin Yerebasmaz, *Yargı Kararları Işığında Hizmet Kusuru Kişisel Kusur Ayrımı* (Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü 2012) 14-18.

veya görülüşünden kaynaklanması yeterlidir. Hizmet kusuru, öğretide bazı yazarlar tarafından sadece idarenin kusura dayanan sorumluluğunun bir şartı olan kusuru[6] ifade etmek için değil genel anlamda idarenin kusura dayanan sorumluluğunu ifade etmek için geniş anlamıyla kullanılmaktadır.[7] Nitekim bu çalışmada da hizmet kusuru ifadesi, geniş anlamıyla idarenin kusura dayanan sorumluluğunu ifade etmek için kullanılmaktadır.

Hizmet kusuru kavramının başına eklediğimiz dijital kelimesi ile sanal dünyada görülen idari faaliyetlerin kuruluş ve işleyişinde ortaya çıkan kusurlardan kaynaklanan, idarenin mali sorumluluk türü ifade edilmektedir. Hizmet kusuru ile özellikleri temel olarak aynı olan dijital hizmet kusuru kavramının ayırt edici noktası, kamu hizmeti ve kolluk faaliyetlerinin dijital ortamda görülmesi sırasında ortaya çıkan sorumluluğu ifade etmesidir. Siber alan veya aynı anlamı karşılayacak şekilde kullanılan dijital ortam kavramının neyi ifade ettiğini de açıklamak gerekmektedir. Siber alan veya siber uzay (cyberspace) tanımları farklılık gösterse de ülkemiz açısından 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kapsamında *"doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler"* olarak ifade edilmiştir.[8] Bununla beraber Amerika Birleşik Devletleri Ticaret Bakanlığı Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ise siber alanı *"bilgi ortamı içinde, internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ve denetleyiciler de dahil olmak üzere, bilgi teknolojisi altyapılarının ve bunlara bağlı verilerin birbirine bağımlı ağından oluşan küresel bir alan"* olarak tanımlamaktadır.[9]

Tanımlardan da anlaşılabileceği üzere siber alan veya buna tekabül edecek şekilde kullanılan dijital alan ifadeleri yalnızca internet ortamını değil bu ortama bağlantıyı sağlayan altyapı ve hizmetleri yani maddi dünyadaki varlıkları, fiziksel altyapıyı da içermektedir. Mevcut çalışma bakımından idarenin siber alan veya dijital ortamdaki faaliyetlerinden kaynaklanan sorumluluk ifadesiyle, idarenin dijital ortamdaki faaliyetleri olan dijital kamu hizmetleri ve internet-intranet ortamındaki dijital kolluk faaliyetlerinden[10] kaynaklanan sorumluluğu kastedilmektedir. Diğer bir ifadeyle idarenin internet veya kapalı ağ sistemlerinde yürüttüğü faaliyetlerinden kaynaklanan sorumluluğu ifade edilmektedir. Belirtmek gerekir faaliyetin gerçekleşmesini temin

[6] Kusur yerine hizmet kusuru ifadesinin kullanılmasına yönelik eleştiri için bkz. Gözler (n 2) 1085-1087.

[7] Bu yönde kullanımlar için bkz. Sıddık Sami Onar, *İdare Hukukunun Umumî Esasları III. Cilt* (3rd edn, Hak 1966) 1694; İl Han Özay, *Günışığında Yönetim II: Yargısal Korunma* (On İki Levha 2010) 207; Turan Yıldırım, Melikşah Yasin, Nur Kaman, H. Eyüp Özdemir, Gül Üstün and Özge Okay Tekinsoy, *İdare Hukuku* (7th edn, On İki Levha 2018) 840; Ulusoy (n 2) 560-563; Sancakdar, Önüt, Us Doğan, Kasapoğlu Turhan and Seyhan (n 5) 833.

[8] T.C. Ulaştırma ve Altyapı Bakanlığı, *2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı* (Faaliyetler-Siber Güvenlik, 2020) 10 < https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf > Erişim Tarihi 29 May 2024

[9] National Institute of Standards and Technology, 'Guide for Conducting Risk Assessments-Information Security' (2012) Rev. 1 800-30 NIST Special Publication Appendix-B B-3 < https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf > Erişim Tarihi: 08.10.2024.

[10] Bu faaliyetler hakkındaki açıklamalar için bkz. 'İdarenin Dijital Alandaki Bir Faaliyeti' başlığı.

eden bilgisayarlar, sunucular, kablolar gibi fiziki varlıkların kuruluş ve işleyişinde bir kusur bulunması eğer ki idarenin dijital ortamdaki söz konusu faaliyetlerine etki ediyorsa bu eksiklikler de zararın ve kusurun tespitinde fayda sağlayacaksa dijital hizmet kusuru kapsamında değerlendirilebilecektir. Çalışmada, dijital kamu hizmeti veya idarenin dijital ortamdaki kolluk faaliyeti kapsamına giren bir idari davranıştan kaynaklanan tam yargı davasında, idarenin asli sorumluluk türü olan kusura dayanan sorumluluğu çerçevesinde evvelemirde dijital hizmet kusurunun dikkate alınması önerilmektedir. İdarenin internette siber güvenliği sağlama yükümlülüğü bulunduğu alanlarda bunu temin ve tesis edememesi ve bundan kişilerin zarar görmesi, e-devlet ve buna bağlı olarak internet ortamında sunduğu kamu hizmetlerinde aksama ve bundan kaynaklanan bir zarar mevcudiyeti, idarenin internet ortamını düzenler ve denetlerken Anayasa'nın gereklerine aykırı olarak bu ortama müdahalede bulunması ve bundan dolayı zararın ortaya çıkması gibi hallerde dijital hizmet kusuru gündeme gelebilecektir. Nihayetinde dijital hizmet kusurunu, idarenin dijital kamu hizmetleri ve dijital ortamdaki idari kolluk faaliyetlerinin kuruluş ve işleyişindeki aksaklıklardan kaynaklanan mali sorumluluğu olarak tanımlayabiliriz.

B. Dijital Hizmet Kusuru Kavramı Neyi İfade Etmemektedir?

Dijital hizmet kusuru kavramının neyi ifade ettiğini ortaya koyabilmek için bu kavramın neyi ifade etmediğini de açıklamak gerektiği kanısındayız. Öncelikle dijital hizmet kusuru, özel hukuk sorumluluğunu yahut hâksiz fiil sorumluluğunu ifade etmemektedir. Özel hukuk ilişkisinden kaynaklanan uyuşmazlıklar adli yargıda giderilmektedir. Bu kapsamda özel hukuk kişisinin sorumluluğunda gerçekleşen dijital ortamdaki hizmetlerden kaynaklanan ya da özel hizmetlerin görüldüğü sistemlerin güvenlik eksikliğinden kaynaklanan zararlar dijital hizmet kusuru kapsamında yer almayacaktır. Diğer bir ifadeyle kamu hizmeti ve kolluk faaliyetleri dışında kalan ve özel hukuk kişilerinin faaliyetleri kapsamında bulunan dijital ortamdaki hizmetlerin kuruluş ve işleyişinden kaynaklanan sorunların dijital hizmet kusuru çerçevesinde değerlendirilmesi mümkün olmayacaktır. Örneğin, bir bankanın sitesine yapılan siber saldırılar, bir sosyal medya platformunda gerçekleştirilen kimlik hırsızlıkları ya da dijital alışveriş mecralarında gerçekleştirilen hack saldırıları dijital hizmet kusuru olarak nitelendirilemeyecektir. Ancak elbette bu durumun istisnaları söz konusu olabilir. Özel hukuk kişilerinin dijital ortamdaki faaliyet alanlarına yapılan bu tür saldırıların internet hizmetinin kuruluş veya işletilişinden, örneğin ülke genelinde internet sunucularının çökmesi nedeniyle zafiyet oluşması gibi, kaynaklanması halinde bir illiyet bağı kurulabildiğinden idarenin de sorumluluğu gündeme gelebilecektir.

Diğer yandan dijital hizmet kusuru, idarenin kusursuz sorumluluğu kapsamındaki sorumluluk türünü de ifade etmemektedir. Nitekim idarenin kusursuz sorumluluğu

temel itibariyle risk ve kamu külfetleri karşısında eşitlik ilkesinden oluşmakta olup[11] dijital hizmet kusuru bu kapsamda değerlendirilemeyecektir. Zira dijital hizmet kusuru; idarenin dijital alandaki kusura dayanan sorumluluğu olduğundan, idarenin kusursuz sorumluluğunun bu kapsamda ele alınabilmesi mümkün değildir. Bu nedenle idarenin siber alandaki kusursuz sorumluluğuna ilişkin tartışmalar dijital hizmet kusuruna ilişkin çalışmamızın kapsamı dışında kalmaktadır.[12]

Genel çerçevesiyle dijital hizmet kusuru, hizmet kusurunun dijital ortamdaki görünüşü olduğundan hizmet kusuru kümesi dışında kalan kusurların dijital hizmet kusuru olarak değerlendirilmesi uygun olmayacaktır. Ancak hizmet kusuru içerisinde ve dijital hizmet kusuru dışında kalan kısım da dijital hizmet kusuru içerisinde değerlendirilemeyecektir. Bu çerçevede maddi dünyada gerçekleşen idarenin eylem ve işlemlerindeki kusurlar bu küme dışında kalacaktır. Dijital hizmet kusurunun, dijital dünyadaki idarenin faaliyetlerinden kaynaklanan kusur olarak düşünülmesi nedeniyle dijital dünya dışındaki idarenin faaliyetleri dijital hizmet kusuru olarak değerlendirilemeyecektir.

C. Bu Kavrama Neden İhtiyaç Duyulmaktadır?

Dijital hizmet kusuru kavramını tamamlamak amacıyla bu kavrama neden ihtiyaç duyulduğunu ve hizmet kusuru değil de neden dijital hizmet kusuru ifadesinin tercih edildiğini gerekçelendirmek gerekmektedir. Aksi takdirde bir amaca hizmet etmeyen sınıflandırma ve kavramlaştırma çabası, hukuk literatürünü gereksiz olarak genişletmeye çalışmaktan başka bir sonuç doğurmayacaktır.

İdarenin dijital ortamdaki faaliyetlerinin gün geçtikçe çoğalması karşısında, bu ortamdaki faaliyetlerden kaynaklanan zararların ortaya çıkma ihtimali çoğalmaktadır. İdarenin sorumluluk sahasının, dijital ortamda görülen kamu hizmetlerinin genişlemesiyle birlikte giderek artması bu alandaki sorumluluğun sınırlarını belirleme ihtiyacını da beraberinde getirmektedir. Maddi dünyada gerçekleşen idarenin faaliyetlerinin tespiti, dijital alana göre oldukça kolaydır. Nitekim bu nedenle de maddi dünyada ortaya çıkan zararların tazmini taleplerinde, diğer şartların yanında zararın kesin ve belirlenebilir olması gerekmektedir. Ancak dijital ortamdaki faaliyetlerden kaynaklanan zararların kaynağını tespit edebilmek ve zarar ile faaliyet arasında nedensellik ilişkisi kurabilmek maddi dünyadaki kadar kolay olmamaktadır. Bunu biraz daha açmak gerekirse, idarenin dijital ortamdaki faaliyetlerinden kaynaklanan sorumluluk uyuşmazlıklarında, sorumluluğun şartları olan *zarar*, zarar ile faaliyet arasındaki *illiyet bağı* ve *kusurun* daha farklı ele alınmayı gerektirdiği noktasından

[11] Gözler (n 2) 1188, 1261; Metin Günday, *İdare Hukuku* (11th edn, İmaj 2017) 379, 382; Cüneyt Ozansoy, *Tarihsel ve Kuramsal Açıdan İdarenin Kusurdan Doğan Sorumluluğu* (Yayınlanmamış Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü 1989) 294; Ahmet Yayla, *İdarenin Kusursuz Sorumluluğu* (On İki Levha 2015) 30.

[12] Bununla birlikte dijital hizmet kusurunun, kusursuz sorumluluğa etki edebilmesi mümkün olabilir bkz. "Dijital Hizmet Kusurunun İdarenin Kusursuz Sorumluluğuna Sirayet Etmesi" başlığı.

yola çıkılmaktadır. Bununla birlikte *idari davranış* unsuru ise hizmet kusuru ve dijital hizmet kusuru arasında belirleme yani ayrım yapma fonksiyonu görecektir. Öncelikle uyuşmazlığa konu *idari davranış* ele alınacak ve idarenin dijital alandaki bir faaliyeti söz konusuysa dijital hizmet kusuru yönünden diğer şartlar incelenebilecektir. Akabinde *zarar* şartı açısından, bir siber saldırı nedeniyle ortaya çıkan zararı hesaplayabilmek farklı bir yaklaşım gerektirmektedir.[13] Diğer yandan özellikle verilerin korunamaması nedeniyle ortaya çıkan zararlarda, zararın henüz kesinleşmemiş ve hatta gerçekleşmemiş olması mevcut teoride benimsenen anlayıştan kopma ve 'potansiyel' nitelik taşıyan zararı kesinleştirme ihtiyacı doğurmaktadır.[14] *İlliyet bağı* şartı açısından dijital ortamda gerçekleşen zararlarda, faaliyet ile zararın ilişkisini ortaya koyabilmek çok kolay bir mesele değildir.[15] Örneğin bir doğal afet sırasında haberleşmenin bilerek ve isteyerek kesilmesi halinde meydana gelen ölüm olayının bu haberleşme kesintisinden kaynaklandığını ortaya koyabilmek; keza kişisel verilerin devlete ait bir sistemden çalınması ile spam arama ve mesajlara maruz kalmak ve kişinin manevi bütünlüğünün bundan etkilenmesi arasında bağlantı kurmak ve bunu yargı makamı önünde kanıtlayabilmek kolay olamayacak ve hatta sonuçsuz kalabilecektir. *Kusur* şartı açısından ise dijital ortamdaki faaliyetlerden kaynaklanan kusurun ispatı davacı açısından oldukça güçtür. Bu nedenle dijital hizmet kusuruna ilişkin uyuşmazlıklarda, kusuru ispat faaliyetinin tersine çevrilmesi önerilmektedir.[16] Kusur ile ilgili olan bir diğer nokta ise bilişim sistemlerinin bünyesinde risk ihtiva etmesidir. Bu nedenle sistemsel ve hukuki risk değerlendirmesi ihtiyacının bir hizmet gereği olarak öngörülmesi ve uygulanmaması halinde kusurun varlığının kabulü önerilmektedir.[17]

Teorik açıklamaları örneklerle somutlaştırmak gerekirse, birçok kişinin kişisel verilerinin dark web olarak bilinen karanlık ağ üzerinden satışa çıkarıldığı iddia edilmektedir.[18] Hala satışta olduğu ileri sürülen bu veriler içerisinde Türkiye Cumhuriyeti Kimlik Numarası, ad soyad, adres, aile ilişkileri, medeni durum, cep telefonu gibi bilgiler de bulunmaktadır. Bu bilgilerin nereden ya da hangi dijital ortamdan ele geçirildiğine yönelik çeşitli iddialar ileri sürülmüştür. Bu iddialardan biri ise söz konusu verilerin e-devlet platformu üzerinden çalındığına yöneliktir.[19] Ancak söz konusu iddia Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından kabul edilmemiş ve

[13] Bu konudaki hesaplama metoduna yönelik açıklama için bkz. 'Zarar' başlığı.

[14] Bu konudaki ölçeklendirme (skala) sistemi önerisi için bkz. 'Delil ve Zararın Tespiti' başlığı.

[15] Bu konudaki açıklamalar için bkz. 'Faaliyet ile Zarar Arasında İlliyet Bağı' başlığı.

[16] Bu konudaki öneri için bkz. 'Delil ve Zararın Tespiti' başlığı.

[17] Bu konudaki öneri için bkz. 'Kusur' başlığı.

[18] Mert Sarıca, 'Was Turkey's e-Government Hacked?' (Hack 4 Career, 21 June 2023) < https://www.mertsarica.com/was-turkeys-e-government-hacked/> Erişim Tarihi 27 May 2024.

[19] Konuya yönelik iddia X, eski adıyla Twitter, platformu üzerinden İbrahim Haskoloğlu tarafından ileri sürülmüş olup ilgili iddia için bkz. Esen Dolma, 'Uzmanlar yanıtladı: 10 soruda e-Devlet'ten veri sızıntısı' (Oksijen, 18 June 2023) < https://gazeteoksijen.com/turkiye/uzmanlar-yanitladi-10-soruda-e-devletten-veri-sizintisi-181501 > Erişim Tarihi 27 May 2024.

söz konusu verilerin az sayıda kullanıcıya yönelik oltalama (phishing) yöntemi[20] ve zararlı yazılımlar ile elde edildiği ileri sürülmüştür.[21] Yine Yüksek Seçim Kurulu'nun verilerinin hacklendiğine yönelik haber yapılmıştır.[22] Günümüzde bu veriler casus yazılımlar aracılığıyla yayılmaya devam etmekte ve kişiler spam aramalara, kısa mesajlara, phishing saldırılarına maruz kalmakta ve hatta bazı uygulamalarda cep telefonu numarasıyla dahi kişilerin T.C. kimlik numarası ve adres bilgilerine ulaşılabilmektedir.[23] Hatta bir varsayımda bulunursak, bu bilgiler ile kişiler aleyhine yargı organlarında husumet yöneltilebilmesi ve bazı durumlarda ilgililerin haberleri dahi olmadan yasal takip başlatılabilmesi ve yasal süresi içerisinde itiraz edilmeyen bu takibin kesinleşmesi ihtimal dahilindedir. Keza cep telefonu aramaları ile yaş, cinsiyet, medeni ve aile durumu bilgileri kullanılarak dolandırıcılık gibi suçların da işlenmesi muhtemeldir.[24] Eğer bu örnekteki gibi milyonlarca kişiye ilişkin veriler e-Devlet üzerinden çalındıysa burada sistemsel zafiyet bulunduğu ileri sürülebilecektir. Ancak verilerin çalınması ve karanlık ağ üzerinde satışa çıkarılması halinde zarara uğranıldığından bahsedilebilir mi? Böyle bir durumda ilgililer tarafından tam yargı davası açılsa bile klasik hizmet kusuru teorisi içerisinde zararın niteliği açısından kesin ve gerçekleşmiş olması gerektiğinden[25] açılan davanın reddedilmesi ihtimal dahilindedir.[26] Nitekim verilen örneğe dönüldüğünde, idarenin dijital ortamdaki mezkûr faaliyetinden kaynaklanan zararın potansiyel olma niteliği baskındır. Dijital hizmet kusuru ile esasında zararın mevcut teoride benimsenen potansiyel niteliğini değiştirerek bu belirsizliği belirli hale getirmek, üzerinde düşünülebilir bir husustur. Çalınan verilere önceden belirlenmiş genel, soyut ve objektif kurallar ile değer biçilerek (belki de bir skala-ölçek belirlenerek[27]), verilerin rıza dışında üçüncü kişilerin eline geçmesi

---

[20] Oltalama yani phishing sosyal mühendislik yöntemi olup kişinin güvenini kazanarak, elektronik iletişimde kullanılan kullanıcı adı, şifre ve kredi kartı bilgileri gibi çeşitli verileri çalmaya yönelik eylemleri ifade etmektedir. Hedeflere genellikle e-posta gönderilerek bu bilgiler elde edilmektedir ancak farklı phishing yöntemleri de bulunmaktadır bkz. Vaishnavi Bhavsar, Aditya Kadlak and Shabnam Sharma, 'Study on Phishing Attacks' (2018) 183(33) International Journal of Computer Applications < https://www.ijcaonline.org/archives/volume182/number33/ > Erişim Tarihi 27 May 2024.

[21] Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 'e-Devlet Kapısı Kullanıcı Hesaplarının Sızdırıldığı İddiaları Hakkında Basın Açıklaması' (CBDDO, 26 February 2023) < https://cbddo.gov.tr/duyurular/6627/-e-devlet-kapisi-kullanici-hesaplarinin-sizdirildigi-iddialari-hakkinda-basin-aciklamasi- > Erişim Tarihi 27 May 2024; ayrıca güncel bir iddiayla ilgili bkz. British Broadcasting Corporation (BBC), '108 milyon kişinin verileri çalındı iddiası: Bakanlık ne açıkladı, tepkiler ne oldu?' (BBC, 12 September 2024) < https://www.bbc.com/turkce/articles/cn8789ez2q7o > Erişim Tarihi 02 October 2024.

[22] Zeki Seskir, 'Hacklenmemek Elimizde mi?' (Medium, 18 October 2017) < https://medium.com/duzensiz/hacklenmemek-elimizde-mi-79bcefc08fbc > Erişim Tarihi 25 May 2024.

[23] Webteknohaber, 'Sadece Telefon Numarasıyla Türkiye'deki Herkesin Tüm Kişisel Bilgilerini Gösteren Bir İnternet Sitesi Ortaya Çıktı' (WebTekno, 09 June 2023) < https://www.webtekno.com/turkiye-herkesin-kisisel-bilgilerini-gosteren-internet-sitesi-h135098.html > Erişim Tarihi 02 October 2024.

[24] Umut Yakar, 'Facebook, Yemeksepeti, LinkedIn ve Clubhouse'dan Çalınan Bilgileriniz ile Neler Yapılabilir?' (WebTekno, 17 April 2021) < https://www.webtekno.com/facebook-calinan-bilgileriniz-ile-neler-yapilabilir-h108701.html > Erişim Tarihi 02 October 2024.

[25] Danıştay 10 D, 2019/752-2023/2146, 25.04.2023: *"idari eylem nedeniyle uğranılan zararın tazmini istemiyle tam yargı davası açılabilmesi için; maddi olayın, zarara sebep olan eylemin idariliğinin ve yol açtığı zararın kesin olarak ortaya konulması zorunludur.";* Danıştay 8 D, 2021/1776-2023/1839, 07.04.2023; Şenel Sarsıkoğlu, 'İdarenin Mali Sorumluluğu Açısından Zarar Kavramı' (2016) 65(4) Ankara Üniversitesi Hukuk Fakültesi Dergisi 2412-2414.

[26] Dijital hizmet kusurunda henüz kesinleşmemiş ancak gelecekte kesin olmasa bile gerçekleşmesi ihtimal dahilinde olan ve bu nedenle duyulan korkudan kaynaklanan zararın tazmini hakkında bkz. "Zarar" başlığı.

[27] Bkz. "Delil ve Zararın Tespiti" başlığı.

halinde zararın meydana geldiğinin kabul edilmesi bir öneri olarak sunulabilir. Diğer yandan ise manevi zarar ileri sürülse bile Türk idari yargı rejiminde manevi zararın tazmininde genellikle düşük bedellere hükmedilmesi[28] nedeniyle giderim davacı yönünden tatmin edici bir miktar olarak nitelendirilmeyebilir.

Konuyu yalnızca kişisel verilerle sınırlamak doğru olmayacaktır. Yapay zekanın hızla gelişmesi nedeniyle yakın gelecekte yapay zekâ kamu hizmetlerinde de sıklıkla kullanılmaya başlanacak ve bu noktada yapay zeka sistemini kullanan idare konuşlandırıcı olarak nitelendirilecektir.[29] Avrupa Birliği (AB) Hukuku'nda yapay zeka sistemlerinin kabul edilemez riskler dışında kullanımına izin verilmesi nedeniyle yüksek riskli yapay zeka sistemlerinin idareler tarafından kullanılması da mümkün hale gelecektir.[30] Nitekim Türk Hukuku'nda henüz regüle edilmeyen[31] yapay zeka sistemlerinin idarenin faaliyetlerinde kullanılması halinde idarenin sorumluluğuna yol açabilecek zararların ortaya çıkması muhtemeldir.[32] Örneğin, Çin'de olduğu gibi yapay zeka sistemleri kullanarak insanları sosyal puanlama sistemine veya ırkına göre tespit edip izlemeye almak[33] ve otomatik sistemlerle kamusal alanlarda bunu sürekli hale getirmek insan hakları açısından bir ihlal olduğu gibi kişilerin mesleki ve özel hayatını da gelecek yönünden etkileyecek potansiyele sahiptir. Yapay zekâ sistemlerinin kolluk faaliyetlerinde kulla-

---

28 Gözler (n 2) 1309; Müzeyyen Eroğlu Durkal, 'Tam Yargı Davalarında Manevi Tazminat' (2017) 131 Türkiye Barolar Birliği Dergisi 203-205.

29 Nitekim Avrupa Birliği Hukuku'nda yakın zamanda yürürlüğe giren Artificial Intelligence Act (Yapay Zeka Tüzüğü) 3'üncü maddesi kapsamında yapay zeka sisteminin profesyonel olmayan kişisel bir faaliyet sırasında kullanıldığı durumlar haricinde, kendi yetkisi altında bir yapay zeka sistemi kullanan gerçek veya tüzel kişi, kamu otoritesi, ajans veya başka bir kurum konuşlandırıcı (deployer) olarak tanımlanmış (önceki taslak metinlerinde kullanıcı olarak kabul edilmekteydi) ve mezkur düzenlemenin 26'ncı maddesinde yüksek riskli yapay zeka sistemlerinde konuşlandırıcıların yükümlülükleri öngörülmüştür bkz. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] COR 1 (AI Act Regulation).

30 Anılı düzenlemenin 27'nci maddesinde ise kamu hukukuna tabi otoriterler ve kamu hizmeti gören özel hukuk kişilerinin, yüksek riskli yapay zekâ sistemleri konuşlandırılmadan önce sistemin temel haklar üzerinde yaratacağı etkiye ilişkin değerlendirme yapma yükümlülüğü bulunmaktadır bkz. AI Act Regulation, art. 27.

31 Ancak belirtmek gerekir ki Türkiye'nin de üyesi olduğu Avrupa Konseyi tarafından, "Yapay Zeka ve İnsan Hakları, Demokrasi ve Hukukun Üstünlüğüne İlişkin Avrupa Konseyi Çerçeve Sözleşmesi (The Council of Europe Framework Convention on artificial intelligence and human rights, democracy, and the rule of law)" 17 Mayıs 2024 günü kabul edilmiş olup Sözleşme'nin 7'nci bölümünde yapay zekaya ilişkin etkili gözetim mekanizmaları kurulması, uluslararası işbirliği yapma ve belirli aralıklarla faaliyetlerini raporlama gibi üye devletlere yönelik yükümlülükler öngörülmektedir. Bu kapsamda yakın zamanda Türkiye'de de yapay zekayı regüle etmeye yönelik düzenlemeler yapılmasını beklemekteyiz. Bir piyasaya dönüşmesi ve kamu ve özel sektöre potansiyel etkileri nedeniyle yapay zekaya yönelik müstakil bir bağımsız idari otorite kurularak, alana ilişkin uzmanlık gerektiren gözetim ve denetim faaliyetinin bu kurum tarafından yapılması gerektiği kanaatindeyiz.

32 İdarenin yapay zekâ teknolojilerini faaliyetlerinde geniş anlamıyla kullanması durumunda ortaya çıkabilecek sorumluluğa yönelik inceleme için bkz. Serkan Seyhan, *Yapay Zekâ Teknolojileri Kapsamında İdarenin Sorumluluğu* (On İki Levha 2023) 271-339; Ahmet Yayla, *İdare Hukuku Bakımından Yapay Zeka* (Seçkin 2023) 153-175; Mutlu Kağıtçıoğlu, 'Yapay Zekâ ve İdare Hukuku (Bugünden Geleceğe Yönelik Bir Değerlendirme)' (2021) 11(1) Hacettepe Üniversitesi Hukuk Fakültesi Dergisi 149-157.

33 Çin bu uygulamayı büyük çoğunluğu Müslüman olan Uygur Türklerini izlemek ve tanımlamak için de kullanmakta olup uygulama çerçevesinde Uygur Türk'ü gibi gözükenlerin geliş-gidiş kayıtlarını tutmaktadır. Bu türdeki uygulamalar otomatikleşmiş ırkçılıkta yeni bir çağ başlatacak potansiyele sahiptir bkz. Paul Mozur, 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority' (New York Times, 14 April 2019) <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> Erişim Tarihi 23 May 2024; ayrıca Çin'de sosyal kredi sistemi açısından idarenin algoritmalara dayalı tespiti ve bu sistemin regülasyonuna yönelik inceleme için bkz. Ömer Faruk Erol, *Algoritmik Regülasyon: Yapay Zekâ ve İdarenin Regülasyon Faaliyeti* (On İki Levha 2023) 119-123.

nılması halinde meydana gelecek kusurlarda zararın belirlenmesi ve kesinleştirilmesi, sistemin kendisinden kaynaklanan özellikler nedeniyle yine çokça tartışma yaratacaktır. Nitekim bu sistemlerde sorumluluğun kime ait olduğunu tespit etmek de oldukça güçleşecektir. Keza yapay zekâ sistemlerini kullanan, konuşlandıran, sağlayan, ithal eden, dağıtan gruplardan hangisine sorumluluğun yöneltilebileceği hangi sektörlerde sorumluluğun ne şekilde paylaştırılacağı ülkemizde netlik kazanmadığı gibi uluslararası alanda da tartışılmaya devam etmektedir.[34]

Siber saldırı sonucuna ilişkin başka bir örnek olarak, sistemin şifrelenmesi, sisteme giriş yetkilerinin kaldırılması ve sistemin kullanılamaması gibi durumların da ortaya çıkması mümkündür. Saldırganlar tarafından fidye yazılımı olan ransomware aracılığıyla sisteme erişim için fidye istenmesi de bazı durumlarda ortaya çıkmaktadır. Böyle bir durumda, zararı tamamen belirleyebilmek mümkün olmadığı gibi ileriye yönelik zararların ortaya çıkma ihtimali de bulunmaktadır. Gelecekteki muhtemel sorunları bunlarla sınırlayabilmek mümkün olmadığı gibi teknolojik gelişmelerin yönünü ve kullanım alanını öngörebilmek de pek mümkün görünmemektedir. Ancak maddi dünyada sıkça görünümü olan hizmet kusurunun dijital ortamın kendine özgü zaman-mekân-vasıta farklılıkları nedeniyle dijital ortamdaki vakıalara uygulanabilmesi için sorumluluğun şartları, sorumluluğu etkileyen haller gibi bazı yönlerden farklılaşması gerektiği düşüncesindeyiz. Bu farklılıkların mevcut hizmet kusuru kavramını etkilememesi ve maddi dünya ile dijital dünya arasında idarenin mali sorumluluğu açısından bir fark yaratılmasının gerekli olduğu düşünüldüğünden, hizmet kusurunun dijital ortamdaki görünüşünün farklı bir kavram ile nitelendirilmesine ihtiyaç vardır. Bu nedenle hizmet kusurunun dijital ortamdaki görünüşüne yönelik en azından bir başlangıç yapabilmek amacıyla dijital hizmet kusuru kavramının kullanılabileceği düşünülmektedir.

II. Dijital Hizmet Kusurunun Sorumluluk Şartları Açısından İncelenmesi Ve Dijital Hizmet Kusurunun İdarenin Kusursuz Sorumluluğuna Sirayeti

Dijital hizmet kusurunu, idarenin dijital ortamdaki faaliyetlerinden kaynaklanan kusura dayanan sorumluk türü olarak önermekteyiz. Nitekim bu özel görünüş sorumluluğunun uygulanabilmesinin mevcut hizmet kusuru teorisinin şartlarının dijital ortama özgü esaslar dikkate alınarak geliştirilebileceğini düşünmekteyiz. Esasen dijital hizmet kusurunun, mevcut hizmet kusurundan (idarenin kusura dayanan sorumluluk anlayışından) ayrılması gerektiğini savunduğumuz nokta, *sorumluluk şartlarının* dijital hizmet kusuru açısından daha farklı ele alınması gerekliliğinden kaynaklanmaktadır.

[34] Örneğin sağlık hizmetlerinde yapay zekanın kullanımı ve hekimlerin sorumluluğu yönünden senaryolara dayalı bir öneri için bkz. W. Nicholson Prince II, Sara Gerke and I. Glenn Cohen, 'Potential Liability for Physicians Using Artificial Intelligence' (2019) 322(18) Journal of the American Medical Association 1766 < https://jamanetwork.com/journals/jama/article-abstract/2752750 > Erişim Tarihi: 15.10.2024.

İdarenin sorumluluğundan bahsedebilmek için idari bir davranış, zarar, davranış ve zarara arasında illiyet bağı ve kusur şartlarının gerçekleşmesi gerekmektedir.[35] Buna karşılık kusursuz sorumluluk açısından ise kusur şartı dışında diğer şartların varlığı mevcut olmalıdır.[36] Esasen vurgulanması amaçlanan nokta, ayrım yapmanın yani dijital hizmet kusuru diye bir kavram ileri sürmenin temel amacı sorumluluk şartlarının idarenin dijital alandaki faaliyetlerinden kaynaklanan uyuşmazlıklarda daha farklı ele alınması gerektiği düşüncesidir. Kusur şartı, idarenin kusursuz sorumluluğu ve kusura dayalı sorumluluğu arasındaki belirleyici unsur ise de dijital hizmet kusuru tüm sorumluluk şartları bakımından farklı ele alınmayı gerektirmektedir. Her ne kadar idarenin dijital alandaki faaliyetlerinden kaynaklanan kusursuz sorumluluğu farklı bir çalışmanın konusunu oluşturabilecek kapsam ve nitelikte ise de dijital hizmet kusuru iddiasıyla bir uyuşmazlığın gündeme gelmesi halinde kusur şartının bulunmaması durumunda kusursuz sorumluluk açısından da kısa bir değerlendirme yapmanın konuyu daha anlaşılabilir kılacağı düşünülmektedir.

Dijital hizmet kusuru açısından sorumluluk şartı olan idari bir davranış, hizmet kusuru ve dijital hizmet kusuru arasında ayrım yapmayı sağlayacak unsur olarak önerilmektedir. Bu nedenle çalışma kapsamında, idarenin dijital alandaki faaliyeti tasnif unsuru olarak kabul edilmektedir. Zarar, illiyet bağı ve kusur unsurlarının ise idarenin dijital ortamdaki faaliyetlerinden kaynaklanan uyuşmazlıklarda daha farklı ele alınması gerektiği düşünülmektedir.

Bu başlık kapsamında idarenin dijital ortamdaki faaliyetlerinden kaynaklanan uyuşmazlıklarda niçin sorumluluk şartlarının daha farklı ele alınması gerektiği açıklamaya çalışılacaktır. Ardından da idarenin dijital ortamdaki faaliyetlerinden kaynaklanan mali sorumluluk uyuşmazlıklarında dijital hizmet kusurunun kusursuz sorumluluğa etkisi tartışılacaktır. Önemle vurgulamak gerekir ki burada öne sürülen gerekçeler, sorumluluk şartlarının bu alandaki faaliyetler açısından daha farklı ele alınması gerektiğini ispatlamak amacıyla kaleme alınmaktadır. Bunların ne şekilde geliştirilmesi gerektiği ise farklı bir çalışmanın konusunu oluşturabilecek kapsamdadır. Her ne kadar bu başlık kapsamında şartların nasıl ele alınabileceğine yönelik öneriler sunulsa da temel odak noktası farklı bir kavrama ihtiyaç duyulduğuna dikkat çekmektir.

A. İdarenin Dijital Alandaki Bir Faaliyeti

Klasik sorumluluk şartları açısından idarenin mali sorumluluğunun doğabilmesi için idari bir davranışın bulunması gerekmektedir.[37] Bu davranış aktif yani yapma şeklinde olabileceği gibi pasif yani yapmama/eylemsizlik şeklinde de

[35] Onar (n 7) 1714-1725; Gözler (n 2) 1294-1347; Ender Ethem Atay, *İdari Yargılama Hukuku* (Seçkin 2021) 347-359; Gürsel Kaplan, *İdari Yargılama Hukuku* (7th edn, Ekin 2020) 316-324.

[36] Özay (n 7) 207; Atay (n 35) 381; Kaplan (n 35) 316.

[37] Atay (n 35) 347; Yıldırım and Çınarlı, (n 3) 309.

gerçekleşebilecektir.[38] İdarenin dijital alanda sunduğu kamu hizmetleri[39] ve idarenin dijital kamu düzenini korumaya yönelik kolluk faaliyetleri, idarenin siber dünyadaki faaliyetleri olarak kabul edilecektir. Nitekim idarenin hizmet kusurunun ortaya çıkış nedenlerinden olan hizmetin hiç işlememesi yani eylemsizlik halinin dijital idari faaliyetler yönünden de ortaya çıkması mümkün olup sistemin şifrelenmesi sonucu işlevsiz hale gelmesi ve idarenin burada önlem almamış olması buna örnek verilebilir. Bu çerçevede dijital idari faaliyetler; dijital kamu hizmeti ve dijital kolluk faaliyetleri ayrımıyla sorumluluğun ilk şartını oluşturmaktadır. Nitekim bir uyuşmazlığın dijital hizmet kusuruna ilişkin olup olmadığı noktasında bu başlık kapsamındaki unsur yani idarenin faaliyeti belirleyici nitelik taşıyacaktır. Yani hizmet kusuru ile dijital hizmet kusuru arasında tasnif yapmayı sağlayacaktır. Bu noktada idarenin dijital alandaki bir faaliyeti yani dijital kamu hizmeti yahut dijital kolluk faaliyeti söz konusuysa dijital hizmet kusuru asli sorumluluk sebebi olarak incelenebilecektir.

1. Dijital Kamu Hizmetleri

Kamu hizmetlerindeki dijital dönüşümlerin temelleri çok öncelerde atılmaya başlansa da Covid-19 pandemisi kamu hizmetlerindeki dijital dönüşümün küresel çapta hızlanmasına vesile olmuş ve dijital yönetim anlayışında yeni bir çağ başlatmıştır.[40] Ancak buna rağmen veri yönetiminde bir kereye mahsus olma ilkesine (the once-only principle)[41] yönelik uygulamalar ve idari prosedürlerin yaygınlaşarak otomasyona geçirilmesi gibi yeni zorlukların ortaya çıkması nedeniyle kamu hizmetlerinde dijital dönüşüm ve uyumlaştırma çalışmaları nispeten yavaş ilerleyebilmektedir.[42] Türkiye'de dijital kamu hizmetleri, esasında ilk aşamada e-Devlet ve UYAP sistemindeki gelişmelerle başlamış ve süreç içerisinde gelişerek Dijital Vergi Dairesi, üniversitelerin elektronik ortamdaki eğitim sistemleri, mahalli idarelerin e-hizmetleri, kamu kurum ve kuruluşlarının Elektronik Belge Yönetim Sistemleri (EBYS) gibi çok sayıda ve çeşitli hallere bürünmüştür. Dijital kamu hizmeti kavramının önceki tanımları e-Devlet sistemi[43] esas alınarak yapılmış ve *"dijital ortamda kamu hizmetlerinin*

[38] Halil Kalabalık, *İdare Hukuku Dersleri Cilt: II* (6th edn, Seçkin 2024) 365; Atay (n 35) 347.

[39] Kamu hizmeti kavramı ve açıklaması için bkz. Aydın Gülan, 'Kamu Hizmeti Kavramı' (1988) 9(1-3) İdare Hukuku ve İlimleri Dergisi 147-150.

[40] Michael E. Milakovich, *Digital Governance* (2nd edn, Routledge 2021) 150; Covid-19 salgınının Türkiye'deki dijital dönüşüme etkisine ilişkin bkz. Mehpare Çaptuğ, 'Covid-19 Salgınının Kamu Hizmetlerinin Dijitalleşmesi Sürecine Etkisi ve Sonuçları' (2021) 23(2) Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 1317-1322.

[41] Bir defaya mahsus olma ilkesinin (The Once-Only Principle) tanımı AB'ye üye devletlere göre farklılaşmakta olup bazı durumlarda verinin tek bir veri tabanında depolanmasını bazen de verilerin sadece bir kez toplanıp birden fazla veri tabanında depolanabilmesini ifade eder bkz. Robert Krimmer, Tarmo Kalvet, Maarja Toots, Aleksandrs Cepilovs and Efthimios Tambouris, 'Exploring and Demonstrating the Once-Only Principle: A European Perspective' (2017) dg.o '17: 18th Annual International Conference on Digital Government Research 547 < http://dx.doi.org/10.1145/3085228.3085235 > Erişim Tarihi 29 May 2024.

[42] The Federal Council of Switzerland, 'Digital public services' (*Federal Department of Finance-Digital Public Services Switzerland,* 26 February 2024) < https://www.efd.admin.ch/efd/en/home/digitalisation/digital-public-services.html > Erişim Tarihi 29 May 2024.

[43] Geçmişten yakın bir tarihe kadar yapılan e-Devlet tanımlarının derlemesi hakkında bkz. Mehmet Mecek, 'E-Devlet ve E-Belediye: Kavramsal Çerçeve ve Türkiye'de Belediye Web Sitelerine Yönelik Yapılan Çalışmaların İncelenmesi' (2017) 22(15) SDÜİİBFD (Kayfor15 Özel Sayısı) 1819-1823.

açık internet ağı üzerinden veya belirli kullanıcıların erişebildiği kapalı ağ ortamında44 yazı ses ve görüntü gibi verilerin iletilebilmesi, işlenilebilmesi ve depolanarak korunabilmesi uygulamalarına dayanılarak işleyen ve sonucunda da yeni bir katkı sağlamayı amaçlayan hizmetler" olarak tanımlanmıştır.[45] Ancak öğretide, bu tanım kapsamında form doldurma gibi kamu hizmetini hazırlayan ara işlemlerin kamu hizmeti olarak düşünülmemesi gerektiği vurgulanmıştır.[46] Gerçekten de işlemin tamamlayıcı niteliğinde olan ara işlemler ve süreçlerin müstakil bir kamu hizmeti olarak kabul edilebilmesi kamu hizmeti teorisinin temel mantığına da aykırı düşecektir. Ancak belirtmek gerekir ki güvenli işlem zincirindeki ara nitelik taşıyan bu tür muamelelerin nihai işlemi yahut hizmetin sunulmasını etkileyecek derecede aksaklığa yol açması halinde sorumluluğa da yol açabilmesi muhtemel hale gelecektir.

Dijital kamu hizmetinin mevzuatımızda tanımı henüz yapılmamış olsa da E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik'in[47] 4'üncü maddesinde e-Devlet Hizmeti *"hizmet süreçlerinin vatandaş odaklı olarak yeniden yapılandırılmasını da içerecek şekilde, kurumlar arası veri paylaşımı esasına dayalı olarak yürütülmesi için kurumlar tarafından, hızlı, güvenli, etkili, verimli, şeffaf ve hesap verebilir, temel hak ve özgürlüklere riayet edilerek ve mahremiyet gözetilecek şekilde elektronik ortama aktarılan her bir kamu hizmeti"* olarak tanımlanmıştır. Esasında bu tanım dijital kamu hizmetinin tanımı da olabilecek mahiyettedir.[48] Tanım kapsamında elektronik ortama aktarılan her bir kamu hizmeti e-Devlet hizmeti olarak kabul edilmektedir. Bu kapsamda e-Devlet üzerinden sağlanmasa bile e-Devlet entegrasyonu çerçevesinde son kullanıcı tarafından sistemine erişim sağlanan ve maddi dünyada kamu hizmeti mahiyeti taşıyan ancak bununla birlikte elektronik ortamda sunulan hizmetler de e-Devlet hizmeti olarak kabul edilecektir. Tanım çerçevesinde kanaatimizce UYAP, Dijital Vergi Dairesi, e-SGK gibi hizmetler e-Devlet Hizmetleri olarak kabul edilecektir. Bununla birlikte e-Devlet entegrasyonu sağlanmamış olsa bile bazı mahalli idarelerin kamu hizmetlerini internet üzerinden sunduğu hizmetler de dijital kamu hizmeti kapsamında değerlendirilecektir. Bunun yanında kapalı ağ sistemi olarak ifade edilen intranetteki belirli hizmetlerin de bir kamu hizmetinin görülmesi için araç olarak kullanılması halinde bu sistemlerin de dijital kamu hizmeti kavramı çerçevesinde değerlendirilmesi uygun olacaktır. Böylelikle intranetteki sistem arızalarının kamu hizmetinin işleyişine etki etmesi hali yasal temele oturtulabilecektir.

---

44 İntranet olarak ifade edilen kapalı ağ ortamına kolluk kuvvetleri tarafından kullanılan PolNet, istihbarat organizasyonları ve silahlı kuvvetler tarafından kullanılan çeşitli bilgi ve teknoloji sistemleri ve bazı kurum içi EBYS'ler örnek verilebilir.

45 Yılmaz Karakoyunlu, 'Türkiye'de e-Devlet Forumu Açılış Konuşması' (Hürriyet, Bilişim Zirvesi 2001)'den aktaran Yücel Oğurlu, *İdare Hukukunda "e-Devlet" Dönüşümü ve Dijitalleşen Kamu Hizmeti* (On İki Levha 2010) 144.

46 Oğurlu (n 45) 145.

47 E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik, RG 03.09.2016/29820.

48 E-Devlet ve Bilgi Toplumu Kanunu Tasarısı Taslağında yer verilen "e-Devlet Hizmeti" ifadesi yerine "dijital kamu hizmeti" kavramı tercihine yönelik bkz. Oğurlu (n 45) 146.

Dijital kamu hizmetleri, geleneksel kamu hizmetlerinin aksine genellikle 7/24 kullanıma açıktır ve internetin açık kaynak yapısı ilgililerin bilgiye hızlı bir şekilde ve kendi amaçları doğrultusunda erişmelerine olanak tanımaktadır.[49] Bununla birlikte dijital kamu hizmetleri internet ortamında sunulurken ve yürütülürken, kamu hizmetlerinin yürütülmesine hakim olan ilkelere[50] ek olarak E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik'in 5'inci maddesinde yer verilen ilkelere de riayet edilmesi gerekecektir. Bu madde kapsamında kullanıcı odaklı olma, siber güvenliğin temini, kesintisiz ve kaliteli hizmet temini, bilişim sistemlerinin güvenliğine yönelik ulusal ve uluslararası standartlara uyulması gibi önemli temel ilkeler benimsenmektedir. Ancak kamu hizmetlerinin kurulması, değiştirilmesi ve kaldırılmasına yönelik esaslar çerçevesinde dijital kamu hizmetlerinin ve bu hizmetlerin yürütülmesine ilişkin temel ilkelerin kanun ile yasama organı tarafından yapılmasına ihtiyaç olduğu görüşündeyiz.[51] 2009 döneminde Başbakanlık tarafından E-Devlet ve Bilgi Toplumu Kanun Tasarısı taslağı ile bir girişimde bulunulmuş olsa da bu süreç nihayete erdiril(e)memiştir.[52] Her ne kadar dijital kamu hizmetleri, maddi dünyadaki kamu hizmetlerinin elektronik ortamdaki birer uzantısı olsa da bu hizmetlerin görülmesine ilişkin usul ve esaslar dijital ortamın doğası gereği daha farklıdır. Nitekim bu konuda bir Yönetmelik çıkarılmış olması ve bu Yönetmelik kapsamında çeşitli ilkeler öngörülmesi de görüşümüzü destekler niteliktedir.

Dijital kamu hizmetlerinin sistemlerindeki geçici veya kalıcı arızalardan kaynaklanan zararlar halinde dijital hizmet kusuru gündeme gelebilecektir. Nitekim bu sistemlerin kurulması ve işletilmesi ilgili kamu tüzel kişisinin sorumluluğunda olup bunların kurulması ve/veya işletilmesine ilişkin hizmet alımı usulü uygulansa bile hizmetin denetim ve gözetiminin nihai sorumluluğu kamu tüzel kişisindedir.[53]

---

[49] Milakovich (n 40) 178.

[50] Dijital kamu hizmetlerinde ayrıca Türkiye'nin AB katılım sürecindeki mevzuat uyumlaştırma çalışmalarının sonucu olarak ortaya çıkan yeni ilkelere, aslında bu ilkeler evrensel kamu hizmeti ilkeleri olarak da değerlendirilebilir, yer verilmesine yönelik bir görüş için bkz. Simge Demir Bayram, *Kamu Hizmetinde Dijital Dönüşüm ve E-İhale Süreci* (On İki Levha 2023) 78.

[51] Öğretide kamu hizmetlerinin dijital ortama taşınması planlandığında öncelikle mevzuatın dijital ortama uyumlaştırılması ve içtihatların da bunlar doğrultusunda geliştirilmesi gerektiği, ayrıca klasik idari sorumlulukla birçok yönden ayrılan farklı sorumluluk türlerinin ortaya çıkabileceği de belirtilmektedir bkz. Oğurlu (n 45) 212.

[52] Türkiye Cumhuriyeti Kalkınma Bakanlığı, *On Birinci Kalkınma Planı (2019-2023) e-Devlet Hizmetlerinin Geliştirilmesi Çalışma Grubu Raporu* (T.C. Kalkınma Bakanlığı 2018) 23 < https://www.sbb.gov.tr/wp-content/uploads/2020/04/e-DevletCalismaGrubuRaporu.pdf > Erişim Tarihi 02.10.2024: *"Geçmişte e-Devlet konusuyla ilgili bir temel kanun çıkartmak amacıyla bazı çalışmalar yapılmıştır. Örneğin, 2009 yılı aralık ayında 'e-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı' başlığı altında bir metin Başbakanlık tarafından kamuoyu ve kamu kurum ve kuruluşları ile paylaşılmış ama bu metnin TBMM'de tartışılıp yasalaşma imkânı olmamıştır."*

[53] Kamu hizmetinin özel kişilerce görülmesine ve sorumluluğun belirlenmesine yönelik ayrıca bkz. 'Sorumluluk Alanının ve Hasmın Belirlenmesi' başlığı.

2. Dijital Kolluk Faaliyetleri

Genel idari kolluk faaliyetlerinin temel amacı kamu düzenini tesis ve temin etmek olup kamu düzenin unsurları olan genel güvenlik, toplumsal sağlık, dirlik ve esenlik ve genel ahlakın korunmasına yönelik faaliyetlerin sürdürülmesi ile kamu düzenin sağlanacağı kabul edilmektedir.[54] Özel idari kolluk faaliyetleri açısından ise kendi kanunlarıyla öngörülmüş olan özel amacın gerçekleşmesi ile kamu düzenin de tesis ve temin edileceği düşünülmektedir. Her ne kadar 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[55] bulunsa ve bu Kanun kapsamında yürütülen faaliyetlerden bir kısmı, dezenformasyona yönelik filtrelemeler gibi, dijital kolluk faaliyeti olarak nitelendirilse bile dijital hizmetlere ve bundan kaynaklanan kamusal yetki ve yükümlülüklere ilişkin müstakil bir kanuni düzenleme bulunmamaktadır ve bu kurallar ülkemizde henüz tedvin edilmemiştir. Buna karşılık AB açısından baktığımızda Dijital Hizmetler Yasası (Digital Services Act – DSA)[56] olarak adlandırılan 2022/2065 sayılı Tüzük, aracılık hizmetleri (intermediary services) olarak adlandırılan yer sağlama (hosting), basit iletim (mere conduit) ve önbellek (cache) hizmetlerine yönelik müstakil bir düzenlemedir. Bu düzenleme dijital hizmetleri tek bir çatı altında önemli ölçüde toplamakta ve bunlara ilişkin kurallar öngörmektedir. Bu düzenleme ile mevzuatımız karşılaştırıldığında, örneğin sadece erişimin engellenmesi usulü bile çok farklı düzenlemelerde öngörülmektedir.[57] Bu mevzuat dağınıklığı hem yargı yerlerinde hem de idareler açısından hangi kuralın uygulanacağına yönelik karmaşıklığı beraberinde getirebilecek potansiyeldedir. Bu nedenle kuralları sistematik biçimde tedvin etmek faydalı olabilecektir. Başka bir örnek ise siber güvenlik açısından verilebilir. AB müktesebatında Birlik genelinde yüksek düzeyde siber güvenliğe yönelik ortak tedbirlerin alındığı 'NIS 2' olarak adlandırılan 2022/2555 sayılı Direktif yürürlüktedir.[58] Bu Direktif kapsamında genel çerçevesiyle üye Devletlerin siber güvenlik stratejileri benimsemeleri, siber kriz yönetim makamları oluşturmaları, kritiklik atfedilen kuruluşların siber güvenlik risk yönetimine ilişkin tedbirler alması

[54] Günday (n 8) 292; Akyılmaz, Sezginer and Kaya, *Türk İdare Hukuku* (n 3) 620.

[55] İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Kanun Numarası: 5651, Kabul Tarihi: 04.05.2007, RG 23.05.2007/26530.

[56] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2016] OJ L 277.

[57] 5651 sayılı Kanun'un 8, 8/A maddeleri haricinde, 5809 sayılı Kanun'un 60'ıncı maddesi, 1262 sayılı İspençiyari ve Tıbbi Müstahzarlar Kanunu'nun 18'inci maddesi, 6361 sayılı Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketleri Kanunu'nun 46'ncı maddesi, 5395 sayılı Çocuk Koruma Kanunu'nun 41/G maddesi, 633 sayılı Diyanet İşleri Başkanlığı Kuruluş ve Görevleri Hakkında Kanun'un 6'ncı maddesi, Telsiz Ekipmanlarının Piyasa Gözetimi ve Denetimine Dair Yönetmelik'in 19'uncu maddesi gibi çok farklı düzenlemelerde erişimin engellenmesi müessesine yer verilmektedir. Konu hakkında güncel, ayrıntılı ve sistematik bir sınıflandırma için bkz. Mehmet Bedii Kaya, 'Türkiye'de İnternete Kim, Neden ve Nasıl Müdahale Ediyor?' (İnternet-Hukuk-Yetki-Kontrol, 25 August 2024) < https://mbkaya.com/internet-hukuk-yetki-kontrol/ > Erişim Tarihi: 08.10.2024; ayrıca bkz. Mehmet Bedii Kaya, *Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi* (On İki Levha, 2010) 85-120.

[58] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333.

ve bunları raporlaması, siber güvenlik bilgi paylaşımına ilişkin kurallar ve yükümlülükler oluşturulması, kuralların uygulanmasına yönelik denetim mekanizmaları sağlanması öngörülmektedir. Bununla birlikte ülkemiz açısından Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği'nin 35'inci maddesi kapsamında siber saldırılara yönelik tedbirlerle ilgili yükümlülükler öngörülmektedir. Ancak bu düzenleme NIS 2 ile kıyaslandığında hem ikincil düzenleme niteliğindedir hem de onun kadar ayrıntılı ve sistematik değildir.

Ülkemiz siber güvenlik politikasıyla ilgili olan bir diğer husus ise Siber Güvenlik Kurulu, 5809 sayılı Elektronik Haberleşme Kanunu[59] Ek madde 1 kapsamında 2014 yılında kanuni temele oturtulmuştur.[60] Mezkûr maddenin ikinci fıkrası kapsamında Kurul'un siber güvenlik ile ilgili olarak politika, strateji ve eylem planlarını onaylamak, kritik altyapıların belirlenmesine ilişkin teklifleri onaylamak, siber güvenlikle ilgili düzenlemelerden kısmen veya tamamen muaf tutulacak kurum/kuruluşları belirleme gibi çeşitli görevler verilmiştir. Ancak 2018 yılında yayımlanan 703 sayılı Kanun Hükmünde Kararname'nin[61] 205'inci maddesi ile siber güvenlik yönünden çeşitli icrai yetkilere sahip olan bu Kurul'un kuruluşuna ilişkin birinci fıkra ve çalışma esaslarına ilişkin üçüncü fıkra mülga edilerek Kurul mülga hale gelmiştir.[62] Geriye yalnızca görevleriyle ilgili olan ikinci fıkra kalsa da bu görevleri yerine getirecek Kurul kaldırılmıştır. Bu kapsamda belirli aralıklarla Siber Güvenlik Kurulu tarafından hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planları, 2020-2023 dönemi için Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanmış ve yayınlamıştır.[63] Yayınlanan bu planlarda eylem maddeleri hizmete özel olarak nitelendirildiğinden yalnızca ilgili kurumlarla paylaşılmaktadır. Güncel durumda siber güvenlik ile ilgili çeşitli görevler 1 sayılı Cumhurbaşkanlığı Kararnamesi uyarınca; Dijital Dönüşüm Ofisi bünyesindeki Siber Güvenlik Dairesi Başkanlığına (m. 527/B), Cumhurbaşkanlığı Güvenlik ve Dış Politikalar Kuruluna (m. 26), Dışişleri Bakanlığı bünyesinde İstihbarat ve Güvenlik İşleri Genel Müdürlüğü (m. 140) ve Bilgi Teknolojileri Genel Müdürlüğüne (m. 143/Ç), Milli Savunma Bakanlığı bünyesinde Muhabere ve Bilgi Sistem Dairesi Başkanlığına (m. 343), Sanayi ve Teknoloji Bakanlığı bünyesinde Milli Teknoloji Genel Müdürlüğüne (m. 388/A) verilmektedir. Ayrıca güncel bir gelişme olarak 2024-2028 yıllarına ilişkin Ulusal Siber Güvenlik Stratejisi ve Eylem

[59] Elektronik Haberleşme Kanunu, Kanun Numarası: 5809, Kabul Tarihi: 05.11.2008, RG 10.11.2008/27050 (Mükerrer)

[60] Siber Güvenlik Kurulu kanuni temele oturtulmadan önce Bakanlar Kurulu'nun 11.06.2012 gün ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar'ın, (RG 20.10.2012/28447), 4'üncü maddesi ile kurulmuştur.

[61] Anayasada Yapılan Değişikliklere Uyum Sağlanması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun Hükmünde Kararname, Karar Numarası: 703, RG 09.07.2018/30473 (3. Mükerrer).

[62] İkinci fıkranın bırakılmasının Kurul'un mülga olmasını engellemediğine yönelik destekler nitelikte bkz. T.C. Ulaştırma ve Altyapı Bakanlığı, *2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı* (n 8) içinde 'Kritik Altyapı Sektörleri' tanımı.

[63] ibid.

Planı da yakın zamanda yayınlanmıştır.[64] Bu kapsamda siber zafiyetlerin önüne geçilebilmesi amacıyla AB siber güvenlik düzenlemelerinde benimsenen siber dayanıklılık yani ex ante denetime dayalı siber güvenlik, tasarımdan itibaren güvenlik (security-by-design) hedeflerinin bu plan kapsamında da hedef olarak belirlendiği görülmektedir.[65] Bu da ülkemizin siber güvenlik anlayışının oluşması bakımından dikkat çekici ve önemli bir gelişmedir.

Dijital kolluk faaliyetlerinin temel amacını dijital kamu düzeninin korunması olarak belirtebiliriz. Ancak dijital alanda kamu düzeni arayışını, maddi dünyadaki ve devletin egemenlik sınırları içerisindeki kamu düzeni gibi algılamak çok mümkün değildir. Nitekim dijital dünyada, maddi dünyadaki gibi birbirini tellerle ve duvarlarla ayıran sınırlar olmadığından devletin internetteki egemenlik alanını belirleyebilmek, interneti düzenlemek ve kontrol altında tutmak kolay bir faaliyet olarak değerlendirilememektedir. Ayrıca maddi dünyadaki kamu düzeninin unsurları, dijital boyutta farklılaşmaktadır. Örneğin, kamu düzenin unsuru olan genel güvenlik, dijital ortamda siber güvenlik kavramında vücut bulmaktadır. Esasında siber güvenlik, genel güvenliğin ve dolayısıyla kamu düzeninin sınırlarını aşarak bünyesinde milli güvenlik ile ilgili meseleleri de barındırmaktadır. Bu yönüyle dijital kamu düzeninin unsurlarını saptayabilmek zorlaşmaktadır. Ancak genel bir ifadeyle idarenin dijital ortamdaki önleyici kolluk faaliyetlerini, dijital kamu düzenini sağlamaya yönelik faaliyetler olarak belirtebiliriz. Dijital kolluk faaliyeti ile ilgili olan bir diğer zorluk ise suçun ortaya çıktığı anı belirlemedeki zorluk nedeniyle dijital ortamda adli ve idari ve hatta milli güvenlik nedeniyle siyasi kolluk[66] ayrımını yapabilmek de güçleşmektedir. Ayrıca yakın gelecekte blokzincir tabanlı ağ, semantik web teknolojilerinin gelişmesi ve kullanımının yaygınlaşmasıyla birlikte veri güvenliğinde artışlar olmasına karşın izleme faaliyetlerinin teknik açıdan zorlaşması muhtemeldir.[67]

Dijital kolluk faaliyetlerine, siber güvenliğin sağlanmasına yönelik aktiviteler, sanal devriyeler, erişimin engellenmesi ve bant genişliğinin daraltılması gibi uygulamalar örnek gösterilebilir. Dijital kolluk faaliyetlerinden kaynaklanabilecek zararlar çeşitli görünümlerde ortaya çıkabilir. Bunlardan bir kısmı veri güvenliğinin ihlalinden, bir kısmı sisteme erişimin geçici veya kalıcı engellenmesinden, bir kısmı

64 T.C. Ulaştırma ve Altyapı Bakanlığı, *2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı* (UAB 2024) 27 <https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf > Erişim Tarihi: 08.10.2024.

65 T.C. Ulaştırma ve Altyapı Bakanlığı, *2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı* (n 64) 25, 27.

66 Siyasi kolluk için bkz. Sancakdar, Önüt, Us Doğan, Kasapoğlu Turhan and Seyhan (n 5) 760.

67 Christian Wirth and Michael Kolain, 'Privacy by BlockChain Design: A BlockChain-enabled GDPR-compliant Approach for Handling Personal Data' (2018) Proceedings of 1st ERCIM Blockchain Workshop 2018 4-6 < https://doi.org/10.18420/blockchain2018_03 > Erişim Tarihi 30 May 2024; ancak blokzincir teknolojisinde verilerin silinememesi ve yok edilememesi de ayrı bir sorun teşkil etmekte olup konuyla ilgili bir inceleme için bkz. Osman Gazi Güçlütürk, 'Blokzincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinemezlik, Yok Edilemezlik Sorunu' (2019) 1(2) Kişisel Verileri Koruma Dergisi 37; kişisel verilerin otomatik araçlarla analiz edilmesi ise işin farklı bir boyutunu oluşturmakta olup bkz. Atila Erkal, 'Kişisel Verilerin Önleyici ve Koruyucu Faaliyetler Kapsamında Otomatik Araçlarla Veri Analizi/Değerlendirilmesi Suretiyle İşlenmesi ve Alman Federal Anayasa Mahkemesi Yaklaşımı' Cemil Kaya (ed) *Kişisel Verilerin Korunması Hukuku ve Bilgi Edinme Hukuku: Çeşitli Açılardan Bakış* (On İki Levha 2023) 23-77.

iletişimin kesilmesinden kaynaklanabilir ki örnekler bunlarla sınırlandırılamayacak kadar fazladır. Bir diğer mesele ise dijital kolluk faaliyetlerinin yalnızca merkezi idarenin denetimi ve gözetiminde gerçekleşmesi beklenemez. Dijital ortamda bir alana (domaine) sahip olan kamu kurum ve kuruluşlarının tümünün en azından alanın güvenliğini sağlamak yönünden sorumlulukları kabul edilmelidir. Örneğin bir belediyenin internet sitesine siber saldırı yapılması ve bilgilerin çalınması durumunda burada ilgili belediyenin dijital kolluk faaliyetini yerine getirememesi sebebiyle sorumluğu esas olmalıdır. Norveç'te bulunan Østre Toten Belediyesi'nin bilgi güvenliğiyle ilgili kusurlu kabul edildiği bir olayda Norveç Veri Koruma Kurumu (Datatilsynet) tarafından Belediye aleyhine 4 milyon Norveç kronu idari para cezası verilmiştir[68]. Yine bir başka örnek olarak, Norveç Parlamentosu'nun yetersiz güvenlik önlemlerinden dolayı birçok milletvekilinin ve idari personelin e-posta hesaplarına yetkisiz erişim yapılmıştır. Bu olay neticesinde yetersiz güvenlik önlemlerinin yetkisiz erişime yol açması ve erişimi kolaylaştırması nedeniyle ulusal veri koruma kurumu Datatilsynet tarafından Parlamento aleyhine idari para cezası verilmiştir[69]. Parlamentoya para cezasının uygulanmasının ardından devlet kurumları ve hatta özel kuruluşlar iki aşamalı güvenlik yöntemine geçiş yapmaya başlamışlardır. Türkiye açısından bakıldığında ise Kişisel Verilerin Korunması Kanunu'nun[70] 18'inci maddesinin ikinci fırkası uyarınca kişisel verilerin ihlal edilmesi durumunda ilgili kamu tüzel kişisine idari para cezası uygulanamamaktadır.[71]

İdari para cezası uygulanması meselesi bir kenara bırakıldığında verilerin çalınması halinde zarar görenlere karşı idarenin mali sorumluluğu gündeme gelebilecektir[72]. Ancak burada sorumluluk şartları açısından zararın maddi olmasından ziyade manevi olma ihtimalinin daha yüksek olduğu görüşü bulunmaktadır.[73] Kişisel veri tartışmaları bir yana kişisel olmayan ancak maddi ve/veya manevi nitelikte değeri bulunan verilerin[74] çalınması, sisteme erişimin engellenmesi, bant genişliğinin daraltılarak iletişimin kesilmesi, sistemsel verilerin silinmesi, üst verinin (metadata) ele geçirilerek alt veya kişisel veri hakkında bilgi çıkarımı yapılması, hukuka aykırı siber gözetim yapılması gibi çok farklı biçimlerde ortaya çıkabilecek durumlardan kaynaklanan zararlarda ne olacağı hala belirsizliğini sürdürmektedir. Örneğin Bilgi Teknolojileri ve İletişim Kurumu (BTK), 6 Şubat 2023 depremi sırasında kurtarma

68 Datatilsynet, 21/00480-14, 07.01.2022.

69 Datatilsynet, 20/03500-10, 04.03.2022.

70 Kişisel Verilerin Korunması Kanunu, Kanun Numarası: 6698, Kabul Tarihi: 24.03.2016, RG: 07.04.2016/29677.

71 Konuya ilişkin inceleme için bkz. Talha Erdoğmuş, 'Kişisel Verileri İhlal Eden İdareye Karşı İdari Para Cezası Uygulanamaması Sorunu', (2023) 10(1) İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 165.

72 Kişisel verilerin korunamamasından kaynaklanan sorumlulukla ilgili bkz. Damla Gürpınar, 'Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk' (2017) 18(2) Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi (Prof. Dr. Şeref Ertaş'a Armağan) 69.

73 Halil Altındağ, 'Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu' (2019) 18(2) İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi 395-396; bu konu zarar başlığı altında ayrıca değerlendirilecektir.

74 Örneğin non-fungible token (NFT), kripto varlıklar, şirket sırları gibi. Tüzel kişilere ait veriler de 6698 sayılı Kanun'un 3'üncü maddesine istinaden kişisel veri niteliğinde olmadığından bu kapsamda değerlendirilebilir.

çalışmaları devam ederken sosyal medya platformlarında bant daraltma uygulamasına başvurmuş ve bu mesele kamuoyunda çokça tartışma yaratmıştır.[75] Zira enkaz altındaki insanların bu platformlar aracılığıyla sesini duyurabildiği ve bant daraltma sonucunda iletişimin kurulamadığı, bant daraltmanın yasal dayanağı bulunmadığı yönünden eleştiri getirilmiştir.[76] Ancak burada idarenin sorumluluğuna gidildiğinde zararın ispatı ve illiyet bağı meselesi nedeniyle idarenin kusura dayanan sorumluluğu yani hizmet kusurunu tespit etmek çok güç olacaktır. İşte idarenin dijital alandaki yetersizliklerinden yani kusurlarından kaynaklanan sorumluluk türünün yeni bir kavramla nitelendirilmesi ve bu alana ilişkin tazmin yöntemlerinin geliştirilmesi adil ve hakkaniyetli çözümlerin üretilebilmesini sağlayabilecektir.

B. Zarar

Dijital hizmet kusurunun en temel sorunlarından biri zarar unsurunun tespit edilebilmesi meselesidir. İdarenin sorumluluğunun doğabilmesi için ortaya bir zarar çıkması gerekmektedir. Bu zarar maddi nitelikte olabileceği gibi manevi nitelikte de olabilecektir. Dijital dünyada kişilerin yakındıkları zararlar örneğin; kişisel bilgi veya fikri mülkiyet gibi bilgi varlıklarında bilginin kendisi kaybolmasa bile üzerindeki kontrolün kaybedilmesi, internet sitelerine yapılan 'Denial-of-Service (DoS)[77]' atakları gibi saldırılarla faaliyetlerinin tamamen veya kısmen kesintiye uğraması veya güvenlik ihlalinden ya da botnet olarak kullanılmak suretiyle siber saldırının gerçekleştiği konum olarak gösterilmesinden dolayı kişinin itibarının ve/veya gizliliğinin zarar görmesi şeklinde ortaya çıkabilir.[78] Dijital varlıkların soyut doğası ve kayıpları, maddi varlıklar zarar gördüğünde ortaya çıkan kayıplardan farklı özellikler göstermektedir.[79] Zararın gerçekleşmiş olması ve kesin bir zarar bulunması nitelikleri gereği, maddi dünyadaki zarar anlayışını esas alarak sonuca varmak yetersiz kalacaktır. Çünkü maddi varlıklar ile dijital varlıkların özellikleri birbirinden farklılık arz etmektedir. Dijital varlıklardan kaynaklanan zararın hem dijital dünya açısından hem de maddi dünya açısından etkisi olabilir. Örnek vermek gerekirse bir video oyun

---

[75] Füsun Sarp Nebil, 'Depremde bant daraltma yapan BTK nedenini açıklasın' (*T24,* 21 March 2024) < https://t24.com.tr/yazarlar/fusun-sarp-nebil/depremde-bant-daraltma-yapan-btk-nedenini-aciklasin,44048#:~:text=%226.02.2023%20depreminin%20hemen%20sonras%C4%B1nda,tarihinde%20bant%20daraltma%20uygulamas%C4%B1na%20gidilmi%C5%9Ftir. > Erişim Tarihi 31 May 2024.

[76] Bant genişliğinin daraltılması uygulamasına sosyal medyada eleştiriler getirilmesi ve kamuoyunda büyük tepkiler gösterilmesi hakkında bkz. Türkiye Mimarlar Mühendisler Odası Birliği Bilgisayar Mühendisleri Odası, *6 Şubat 2023 Kahramanmaraş Depremleri Raporu* (BMO, 6 August 2023) 4 < https://www.bmo.org.tr/wp-content/uploads/2023/10/BMO-Deprem-Raporu.pdf > Erişim Tarihi 02.10.2024; ayrıca Türkiye Barolar Birliği tarafından 4982 sayılı Bilgi Edinme Hakkı Kanununa istinaden konuya ilişkin bilgi edinme başvurusu yapılmışsa da talep kurum içi düzenleme nedeniyle reddedilmiş, müteakiben Bilgi Edinme ve Değerlendirme Kuruluna yapılan başvurunun da reddi üzerine açılan davada bilgi edinme talebinin reddi işleminin iptaline karar verilmiştir bkz. Ankara 6 İdare Mahkemesi, 2023/1222-2024/459, 29.03.2024 < https://d.barobirlik.org.tr/2024/20240704karar.pdf > Erişim Tarihi 31.05.2024.

[77] Mevzuatımızda Denial of Service (DoS), hizmet dışı bırakma; Distributed Denial-of-Service (DDoS) dağıtık hizmet dışı bırakma olarak tanımlanmaktadır bkz. Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği, RG: 13.07.204/29059.

[78] Ian Walden, *Computer Crimes and Digital Investigations* (2nd edn, Oxford 2016) 27,28.

[79] G. Stevenson Smith and Anthony J. Amoruso, 'Using real options to value losses from cyber attacks' (2006) 2(3-4) Journal of Digital Asset Management 151 < https://doi.org/10.1057/palgrave.dam.3650033 > Erişim Tarihi 01.06.2024.

içerisindeki item (öğe) o oyun ile ilgilenenler açısından çok değerli kabul edilirken ve maddi dünyada da ticareti yapılırken o oyun ile ilgilenmeyenler açısından herhangi bir değere sahip olmayabilir. Bu nedenle itemin değerini tespit etmek de oldukça güçleşebilir. Aynı örnek non-fungible tokens (NFTs) ve kripto varlıklar açısından da verilebilir. Örnekler yazılımlar, sosyal medya hesapları, algoritmalar[80], veri tabanları, web sayfaları, dijital ortamdaki şirket sırları, bulut bazlı hesaplar ve dijital fikri mülkiyet içeren diğer türdeki dijital varlıklar açısından da çoğaltılabilir.[81] Zira siber saldırılar açısından gizli ve kritik veri sızıntısı, fırsat kaybı, verilerin zarar görmesi, sistemin işler hale getirilmesindeki maaliyetler zararın hesaplanması açısından özellik gösterecektir. Bir diğer örnek olarak sosyal medya platformlarına erişim engeli getirildiğinde yahut bant daraltma uygulamasına gidildiğinde ve bu idari tedbirin farzı misal hizmet kusuru teşkil etmesi halinde bu platformlar üzerinden gelir sağlayanların kayıplarını tespit etmek bir işletmenin maddi dünyadaki zararını tespit etmek kadar kolay olmayabilir. Bunun yanına bir de manevi zarar kalemi eklendiğinde dijital varlığa ilişkin kaybın manevi bütünlüğe etkisi de bir ihtimal dahilinde dikkate alınmayabilir. Özellikle siber saldırılarda zararın bir kısmının potansiyel nitelik taşıması halinde yapılacak hesaplama yönteminde belirsiz zararların da tahmin yöntemiyle hesaplanması ihtiyacıdır.[82]

Dijital alanda gerçekleşen kişisel verilerin çalınması konusu ele alındığında, idarenin sorumluluğuna yönelik olarak manevi zararın doğması mümkündür ve maddi zarara kıyasla manevi zararın ortaya çıkması daha muhtemeldir.[83] Bu kapsamda manevi zararın, Danıştay'ın genel kabulünün[84] aksine tatmin edici ve idareyi tekrar sorumluluk doğuracak eylemden uzaklaştırıcı nitelikte caydırıcı olması gerçekten de faydalı olabilir.[85] Nitekim kişisel veriler açısından manevi tazminat yaklaşımında farklılaşma olması gerektiği ileri sürülmüştür.[86] İdarenin, kişisel verileri gereği gibi muhafaza edememesi durumunda hizmet kusuru nedeniyle sorumlu olacağına yönelik içtihat bulunmaktadır.[87] Nitekim siber saldırıdan kaynaklanan verilerin çalışması

---

80 Erol (n 33) 25-29.

81 Luke Lee, 'Examining the Legal Status of Digital Assets as Property: A Comparative Analysis of Jurisdictional Approaches' (2024) SSRN 2 < http://dx.doi.org/10.2139/ssrn.4807135 > Erişim Tarihi: 03.10.2024.

82 Örneğin ransomware saldırılarında finansal kayıpların modellenmesine yönelik bkz. Chris Beck, Alexandre Boumezoued, Yousra Cherkaoui, Eliott Pradat and Blake Fleisher, ' Modelling Financial Losses From a Ransomware Attack Using a Casual Approach' (Milliman, 2023) < https://www.milliman.com/-/media/milliman/pdfs/2023-articles/10-13-23_modeling-financial-losses-from-a-ransomware-attack.ashx > Erişim Tarihi: 15.10.2024.

83 Cemal Başar, *Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması* (On İki Levha 2020) 323-325.

84 Danıştay manevi zarar hesabında manevi tazminatın bir zenginleşme aracı olmadığını kabul etmektedir bkz. Danıştay 13 D, 700/2839, 01.06.2023; Danıştay 10 D, 2022/898-2023/1620, 29.03.2023.

85 Bu kapsamda manevi zararın Danıştay'ın genel kabulünün aksine tatmin edici ve idareyi tekrar sorumluluk doğuracak eylemden uzaklaştırıcı nitelikte caydırıcı olması gerektiği ileri sürülmüştür bkz. Altındağ (n 73) 395.

86 Altındağ (n 73) 395.

87 Danıştay 15 D, 2015/10101-2016/664, 08.02.2016.

durumlarında idarenin, risk ilkesi gereği kusursuz sorumluluğuna gidilebileceği de ileri sürülmektedir.[88]

İdarenin sorumluluğunun doğabilmesi için zararın gerçekleşmiş ve kesinleşmiş olması aranan nitelikler arasındadır.[89] Zararın kesinliği, güncel yani mevcut zarar ile gelecekte gerçekleşmesi kesin olan zararları ifade etmektedir.[90] Gerçekleşmiş zarar ise zararın bilfiil ortaya çıktığını belirtmektedir.[91] Burada belirtmek gerekir ki gelecekte oluşacak zararın kesin olması hali bunun tek istisnasını teşkil etmektedir.[92] Bu kapsamda, tıbbi bir hata sonucu sakat doğan çocuğun gelecek hayatındaki performans düşüklüğü nedeniyle zararı, kesin bir nitelik arz ediyorsa mahrum kalınan kârın tazmini buna örnek verilmektedir.[93] Ancak burada dikkat edilmesi gereken nokta zararın gerçekleşmesinin kesin ve kaçınılmaz olmasıdır. Dijital hizmet kusuru açısından ise bu kriterler önem arz etmektedir. Bu noktada kanaatimizce ele alınması gereken soru, kişisel verilerin ele geçirilmesi ve ardından dark web gibi sistemler üzerinden satışa çıkarılması durumunda geleceğe yönelik korku duyulması halinde zararın gerçekleşmediğinden ve kesinleşmediğinden bahsedebilir miyiz? Avrupa Birliği Adalet Divanı (ABAD)'ın bu konuda önüne gelen bir olayı aktarmak yorum yapmak açısından yön gösterici olabilecektir. Bulgaristan Yüksek İdare Mahkemesi (Varhoven administrativen sad) ön karar talebi ile ABAD'dan talepte bulunduğu olayda[94], Bulgaristan Maliye Bakanlığına bağlı bir idare olan Ulusal Gelir İdaresi'nin bilişim sistemine siber saldırı gerçekleşmiş, sistemde yer alan 6 milyondan fazla gerçek kişinin kişisel verileri internette yayınlanmış ve bu vakıa medya tarafından ortaya çıkarılmıştır. Mağdurlardan biri tarafından, rızası olmadan yayınlanan kişisel verilerinin gelecekte kötüye kullanılabileceği veya kendisine şantaj yapılabileceği, saldırıya uğrayabileceği ve hatta kaçırılabileceği korkusuyla manevi zarara uğrandığı iddiası ile dava açılmıştır. Bu davada ilk derece mahkemesi, saldırının üçüncü kişiler tarafından ger-

88 Altındağ (n 73) 396.

89 Gözler (n 2) 1323-1328, Sarsıkoğlu (n 25) 2412; Danıştay 13 D, 2015/4515-2021/1150, 31.03.2021 sayılı temyizen inceleme yaptığı kararında ilk derece mahkemesinin *"tazmini istenilen maddi zararın gerçekleştiğine ilişkin somut bir delil bulunmaması ve idare hukukuna hakim ilkelerden olan idarenin mali sorumluluğunun koşullarından birisi olan zararın, gerçekleşmiş, kesin ve belirli bir zarar niteliğinde olması gerektiği, henüz doğmamış ve doğması muhtemel zararlar ile doğmuş olması kuvvetle muhtemel olmakla birlikte belli bir miktar olarak ispatlanamayan zararların idare tarafından tazminine karar verilemeyeceği ilkeleri uyarınca olayda bu şartların gerçekleşmediği açık olduğundan (...) tazminat isteminin reddine"* karar verdiği kararı onamıştır; zarar açısından aranan diğer nitelikler için bkz. Gözler (n 2) 1320-1338, Sarsıkoğlu (n 25) 2411-2417.

90 Gözler (n 2) 1324.

91 ibid 1324.

92 Ender Ethem Atay and Hasan Odabaşı, *Teori ve Yargı Kararları Işığında İdarenin Sorumluluğu ve Tazminat Davaları* (2nd edn, Seçkin 2010) 183.

93 Atay and Odabaşı (n 92) 183; ancak bununla beraber örneğin Danıştay *"Davacıya ait arazinin yanından geçirilen kanalın iyi bir şekilde inşa edilmemesi sebebiyle araziye su sızdığı ve 1969 yaz mevsimi için ektiği çeltiğe %50 zarar vereceğinin mahkeme kararıyla tespit edildiğini belirtilerek, bu zararın tazmini istemiyle açılan davada Danıştay ihtimale dayalı olan tazmin isteminin daava konusu edilemeyeceği gerekçesiyle davayı reddetmiştir"* karar için bkz. Danıştay 12 D, 1969/1774-1971/2479, 06.11.1971 aktaran ibid 183.

94 Case C-340/21 *VB v Natsionalna agentsia za prihodite* [2023] OJ C2024/1065; Norveç'te gerçekleşen ve korkudan kaynaklanan zarara ilişkin başka bir örnek için ayrıca bakınız Mona Naomi Lintvedt, 'Putting a price on data protection infringement' (2022) 12(1) International Data Privacy Law 14 < https://doi.org/10.1093/idpl/ipab024 > Erişim Tarihi 06.06.2024.

çekleşmesi, yani zarara yol açan eylemin üçüncü kişiden kaynaklanması ve Ulusal Gelir İdaresi'nin güvenlik tedbirleri almadığının kanıtlanamaması sebebiyle davayı reddetmiştir. Uyuşmazlık temyizen Bulgaristan Yüksek İdare Mahkemesi'nin önüne gelmiş, Mahkeme General Data Protection Regulation (GDPR)[95] 82'nci maddesinin birinci fıkrası kapsamında bir kişinin kişisel verilerinin gelecekte kötüye kullanılabileceği korkusunun kendi başına manevi zarar teşkil edip etmeyeceğini, eğer ediyorsa tazminat talebinden önce üçüncü tarafın bu verileri kötüye kullanması gerekip gerekmediğini sorarak ön karar için ABAD'a başvurmuştur. ABAD, söz konusu düzenlemenin ihlal edilmesi sonucunda kişisel verilerinin üçüncü taraflarca kötüye kullanılması ihtimaline ilişkin olarak bir veri sahibinin yaşadığı korkunun, GDPR kapsamında 'maddi olmayan zarar' teşkil edebileceği yönünde karar vermiştir.[96] Bu da demek oluyor ki kişisel verilerin çalınması ancak henüz kötüye kullanılmaması halinde, yani verinin kötüye kullanımının potansiyel olması durumunda, veri sahibinin yaşadığı korkunun bir zarar oluşturması mümkündür. Ancak belirtilmelidir ki burada korku duygusu 'potansiyel' nitelikte değildir. İleride yaşanacak olan verilerin kötüye kullanılması potansiyel niteliktedir ve bu potansiyele bağı yaşanan korku duygusu kesin ve gerçekleşmiş bir duygudur. ABAD da bu duygunun, bir zarar teşkil edebileceğini kabul etmektedir. Elbette bu zarar manevi zarar kapsamında değerlendirilecektir. Ancak manevi zararlardan kaynaklanan tazminat taleplerinde Türk idari yargı yerleri, tazminatı bir zenginleşme aracı olarak görmemektedir.[97] Ayrıca tam yargı davalarında hükmedilecek manevi tazminat tutarının zarara uğrayan tarafın beklentilerini karşılamaması da ihtimal dahilindedir.[98] Ancak dijital veriler konusunda özellikle idarenin kusurunun ağırlığını ortaya koyacak oranda[99] tazminat belirlenmesi yaklaşımının benimsenmesi idarenin ileriye yönelik olarak siber alanda güvenlik önlemlerini arttırmasını ve bu alanda uzman personel istihdamını genişletmesini sağlayabilecektir. Aksi durumda, kusurun karşılıksız kalması nedeniyle önlem alınmaması ve siber saldırıların yoğunlaşması gibi sonuçların doğması da muhtemeldir.

---

[95] 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) [2016] OJ L 119/1.

[96] Case C-340/21 *VB v Natsionalna agentsia za prihodite* [2023] OJ C2024/1065, paras 75-84, para 82: *"Ana davadaki koşullara benzer durumlarda, kişisel verilerin kötüye kullanımının fiili değil, sadece potansiyel olması, GDPR'ın ihlali nedeniyle veri sahibinin manevi zarara uğramış olabileceği kabulü için yeterlidir. Ancak bu kabul, veri sahibinin, böyle bir kötüye kullanım korkusunun kendisinde gerçekten ve belirli bir şekilde fiili ve kesin duygusal zarara yol açtığını ispatlaması şartına bağlıdır."*

[97] Danıştay 8 D, 2021/1834-2023/5043, 20.10.2023: *"yaşanan olayın niteliği, davacılar üzerinde bıraktığı etki ile tedavi süreci, idarenin olay kapsamındaki sorumluluğu birlikte değerlendirilerek zenginleşmeye sebep olmayacak nitelikte ancak takdir edilecek miktarın aynı zamanda duyulan elem ve ızdırabı giderecek bir oranda manevi tazminat ödenmesine karar verilmesi gerektiği"*; aynı yönde bkz. Danıştay 5 D, 2017/15391-2020/3172, 07.07.2020.

[98] Ülkemizdeki manevi tazminat miktarlarının düşük olduğuna yönelik bkz. Eroğlu Durkal, (n 28) 203-205; ayrıca manevi tazminatın bir tazmin aracı değil tatmin aracı olarak öngörülmesi anlayışı nedeniyle hükmedilen tutarların sembolik olduğuna yönelik eleştiriler için bkz. Gözler (n 2) 1309; diğer yandan manen duyulan bu korkunun manevi bir zarar olarak nitelendirilmemesi ihtimali de bulunmakta olup bu durumda idare hukukuna özgü tazmin nedenleri bulunmaması gerekçesiyle idarenin tazmin yükümlülüğünün ortadan kalktığı ileri sürülebilecektir bkz. Danıştay 8 D, 2021/7933-2023/4151, 27.09.2023; ayrıca bkz. Oğuz Sancakdar, 'İdare Hukukuna Özgü Tazmin Nedenlerinin Bulunmaması Kavramı' (1999) Manisa Barosu Dergisi 20-31.

[99] Danıştay 10 D, 2001/323-2003/703, 25.02.2003.

Ayrıca değinmek gerekir ki mer'i hukukta benimsenen esas çerçevesinde hukuk kurallarının ihlali tek başına tazminat için yeterli olmamaktadır. Diğer bir ifadeyle ihlal ve zarar farklı kavramlardır ve farklı anlamlara sahiptirler. ABAD, ön karar talebi prosedürü kapsamında önüne gelen başka bir olayda kişisel verilerin korunmasına yönelik düzenlemelerin ihlal edilmesinin GDPR 82'nci maddesi anlamında tazminat talepleri için yeterli olmayacağına ve ortaya bir zarar çıkmasının tazminat talepleri açısından bir şart olduğuna vurgu yapmıştır.[100] Bu karar esasında ABAD önünde GDPR 82'nci maddesi açısından ön karar için bekleyen birçok kararın ilki niteliğindedir. Karar kapsamında sadece 82'nci maddenin ihlalinin yeterli olmadığı belirtilmekle yetinilmemekte, tazminat hakkının söz konusu olabilmesi için; 1-GDPR'ye yönelik bir ihlalin varlığı, 2-Uğranılan bir zararın varlığı, 3-Zarar ile ihlal arasında illiyet bağı olması şartlarının sağlanması gerektiği vurgulanmaktadır.[101] Mezkûr kararda ayrıca sorulan sorulardan biri zararın belirli bir ciddiyet eşiğine ulaşmış olmasının aranıp aranamayacağı meselesidir. Bu kapsamda ABAD, böyle bir kriter aranmasının uygulama birliğini sağlamayacağını ve AB yasama organının geniş kapsamlı zarar anlayışı tercihine ters düşeceğini belirterek ihlalin zarara yol açmış olmasının yeterli olacağını belirtmektedir.[102] Ayrıca bu karardan anlaşılabileceği üzere ABAD, GDPR 82'nci maddesinden kaynaklanan zararların tazmini için verilerin korunmasına yönelik bir ihlalin gerçekleşmesini aramaktadır.[103]

Tüm bu açıklamalarla birlikte gelecekte oluşması kesin olan zararlar dışında sorumluluk hukuku teorisinde potansiyel zararların tazmin edilebileceğine yönelik bir kabul bulunmamaktadır. Özellikle kişisel verilerin çalınması durumunda bu verilerin gelecekte ne şekilde kullanılabileceğine ilişkin bir belirleme yapabilmek çok mümkün değildir. Keza gelecekte kötüye kullanılsa bile bu verilerin nereden elde edildiğini tespit etmek, zarar ile davranış arasında illiyet bağı kurabilmek de çok mümkün değildir. Bununla birlikte mevcut sistemimizde, geleceğe yönelik bu zarar ihtimalinin gerçekleşmesini beklemek gerekecektir. Bir öneri olarak, potansiyel zarara bağlı 'kesinleştirilebilen' hususların tazmini mümkün kılınabilir. Yukarıda örnek verilen ABAD'ın C-340/21 sayılı kararında gelecekte olabileceklere ilişkin duyulan korku bunun bir örneğidir. Başka bir öneri ise genel, soyut, objektif ve kişilik dışı düzenlemelerle eğer verilere önceden bir fiyat biçilirse, örneğin emtialar sigortalanırken rayiç değerinin belirlendiği gibi kişisel verilere de bir maddi değer biçilirse, bu durumda verinin çalınması/sızması halinde zararın kesinleştiği ve gerçekleştiği, maddi bir zararın meydana geldiği ileri sürülebilecektir. Burada dikkat çekilmek istenen

[100] Case C-300/21 *UI v Österreichische Post AG* [2023] EU:C:2023:370, paras 33-42.

[101] Case C-300/21 *UI v Österreichische Post AG* [2023] EU:C:2023:370, paras 36.

[102] Case C-300/21 *UI v Österreichische Post AG* [2023] EU:C:2023:370, paras 43-51; zararın ciddiyet eşiğine ilişkin olarak kararın incelenmesine ilişkin bkz. Václav Janeček and Cristiana Teixeira Santos, 'The autonomous concept of "damage" according to the GDPR and its unfortunate implications: Österreichische Post' (2024) 61(2) Common Market Law Review 540-543 < https://doi.org/10.54648/cola2024031 > Erişim Tarihi 17.06.2024; idarenin kusursuz sorumluluğunda ise zararın anormal olması gerekliliğine ilişkin bkz. Gözler (n 2) 1337.

[103] Ayrıca bkz. 'Kusur' başlığı.

nokta yukarıdaki örneklerde de belirtildiği üzere dijital alandaki zararların potansiyel zarar niteliğinde olması oldukça yaygın görülebilmektedir. Öneri ise potansiyel olma durumunu, veriye fiyat biçilmesi gibi çözümler üreterek önceden kesinleştirilmesidir.

Diğer yandan zararın hesaplanması da özellik arz edecektir. Denial-of-Service gibi siber saldırılar neticesinde sisteme erişimin kısmen veya tamamen kesilmesi durumunda faaliyetlerin aksaması zarara yol açabilecektir. Örneğin gelir kaybı, sözleşme ihlali, erişim sağlayıcısına yapılan ek giderler, dava giderleri, sistemin onarım giderleri, olaya müdahale için yapılan giderler somut zararlar; üçüncü tarafın zararı, manevi kayıplar, üretkenlik kaybı, marka zararı, güvenilirlik kayıpları soyut zararlar kapsamında değerlendirilebilecektir.[104] Mer'i hukuk kriterleri açısından idari bir faaliyet, faaliyetten kaynaklanan zarar ve kusurun bulunması durumunda zararın tazmin edilmesi gerekmektedir. Ancak dijital ortamda gerçekleşen yahut dijital ortamda gerçekleşip maddi dünyaya yansıyan zararların tespiti o kadar da kolay görünmemektedir. Bu nedenle dijital varlıkların değerlemesine yönelik yöntemler geliştirilmesine ihtiyaç vardır. Dijital varlıklarda varlığın değerinin büyük bir kısmının maddi olmaması sebebiyle geleneksel zarar değerlemesinin zararı gerçek anlamıyla yansıtması mümkün olmadığından, siber saldırılar nedeniyle uğranılan zararlarda binom ağaçlarını kullanan reel opsiyon analizi yöntemi esas alınarak zararın hesaplanması önerilmiştir.[105] Böylelikle dijital varlıkların değerini ve potansiyel kaybını daha doğru bir şekilde ölçmek mümkün olabilecektir.[106] Türkiye uygulaması açısından da özellikle ticari işletmelere ve kamu iktisadi teşebbüslerine yönelik gerçekleşen siber saldırılara ilişkin uyuşmazlıklarda yapılacak bilirkişi hesaplamalarında gerçek zararın tespitine yaklaşan bu yöntemin kullanılması dijital varlıkların maddi olmayan değerini de hesaplayabilmek açısından hakkaniyetli bir yaklaşım olabilecektir. Vakıaya uygun düştüğü ölçüde dijital hizmet kusurundan kaynaklanan uyuşmazlıklarda da bu yöntemin benimsenmesi mümkün olmalıdır. Ancak buradaki temel sorun potansiyel kayba yargı yerinin yaklaşımının ne olacağı meselesidir. Özellikle dijital ortamdaki zararlarda potansiyel zarar meselesinin çok daha dikkatli ele alınması gerekmekte olup ileriye yönelik zararın kesinleşmesi açısından maddi dünyadaki gibi bir kesinliğin aranması hakkaniyete aykırı sonuçlar doğurabilecektir. Ya da başka bir öneri olarak idari yargıda dijital hizmet kusuru açısından munzam zarar anlayışı kabul edilip potansiyel zarar gerçekleştikten sonra ilgililerin kayıplarının ilk davayla birlikte yeniden ele alınarak hızlı bir şekilde giderilebilmesine yönelik hızlı tazmin imkânı öngören usuli yöntemler geliştirilebilir.

---

[104] Sharon Christensen, William J. Caelli, William D. Duncan and Eugenia Georgiades, 'An Achilles heel: denial of service attacks on Australian critical information infrastructures' (2010) 19(1) Information & Communications Technology Law 64 < https://doi.org/10.1080/13600831003708059 > Erişim Tarihi 17.06.2024.

[105] Bu hesaplama teknik uzmanlık gerektirip genel kapsamıyla siber saldırılardan kaynaklanan kayıplar, 1. Reel opsiyon değerindeki azalma, 2. Saldırı nedeniyle kaçırılan fırsatların maliyeti, 3. Saldırı nedeniyle yeniden yapılandırma maliyeti unsurlarından oluştuğu belirtilmekte olup öneri ve teknik hesaplama metoduna yönelik bkz. Smith and Amoruso (n 79) 158-159;

[106] ibid 160.

C. Faaliyet ve Zarar Arasında İlliyet Bağı

Dijital hizmet kusurunun meydana gelebilmesi için idarenin dijital alandaki faaliyeti ile meydana gelen zarar arasında illiyet bağı bulunması gerekecektir. İlliyet bağı idarenin sorumluluğunun doğması için ortaya çıkan zararın, idarenin eylem ya da işleminin bir sonucu olmasını yani idarenin eylem ya da işlemi ile zarar arasında neden-sonuç ilişkisinin bulunmasını ifade etmektedir.[107] Zarar görenin veya üçüncü kişinin eylemi, illiyet bağını ve dolayısıyla sorumluluğu etkileyen bir husus olup zarar tamamen zarar görenden veya üçüncü kişiden kaynaklanıyorsa illiyet bağı kesileceğinden idarenin sorumluluğu da normal şartlarda doğmayacaktır. İlliyet bağı konusu dijital hizmet kusurunda hassas meselelerden biridir. Nitekim dijital hizmet kusuru, zarar görenin veya üçüncü kişinin eyleminden kaynaklanabilecektir. Örneğin phishing gibi sosyal mühendislik yöntemlerinde zarar görenin; DoS, DDoS, trojan gibi siber saldırılarda üçüncü kişinin yani bilgisayar korsanının (hacker) eylemi söz konusudur. İlliyet bağının kesilip kesilmediğine ilişkin olarak bu noktada idarenin hizmetin yürütülmesi sürecinde hizmetle ilgili yükümlülüklerinin zararın ortaya çıkmasında etkili olup olmadığına[108] bakmak gerekecektir. Kural olarak üçüncü kişinin eyleminin ağırlığı idarenin kusurunu arka plana atacak yoğunlukta ise illiyet bağı kesilmektedir.[109] Ancak siber alandaki kusurlarda bu meseleyi maddi dünyadaki gibi ele almak doğru sonuçlar vermeyebilir. Zira aksi halde ilgililerin, tazminat taleplerini üçüncü kişi olan bilgisayar korsan(lar)ına yöneltmesi beklenecek[110] olup bunun da fiilen mümkün olmaması nedeniyle, zararlarını giderecek başkaca bir hukuki imkan kalmayacaktır. Nitekim idarenin, *dijital kamusal alana* yani yer sağlayıcı olduğu ve/veya kamu hizmetini gördüğü dijital alana yönelik olarak siber saldırıları önleme yükümlülüğü bulunmaktadır. Bu kapsamda gerekli teknolojik donanımı sağlamak, yeterli sayıda ve uzmanlığa sahip siber güvenlik personelini istihdam etmek, yeterli düzeyde güvenli sunucu sertifikasına sahip olmak, intranet sistemlerde dışsal müdahaleleri önleyecek yöntemler geliştirmek, sunucuların fiziki ve dijital ortamdaki güvenliği sağlamak gibi siber güvenliği temin etmeye yönelik önlemlerin idare tarafından alınması gerekmektedir.

Öte yandan zarar görenin davranışının ağır kusur teşkil etmesi halinde illiyet bağının kesildiği kabul edilmektedir.[111] Dijital alanda zarar görenin eyleminin zararın

---

[107] Bahtiyar Akyılmaz, Murat Sezginer and Cemil Kaya, *Açıklamalı-İçtihatlı Türk İdari Yargılama Hukuku* (Savaş 2019) 1281.

[108] Akyılmaz, Sezginer and Kaya *Açıklamalı-İçtihatlı Türk İdari Yargılama Hukuku* (n 107) 1282.

[109] ibid 1294.

[110] Örneğin yapay zekâ sistemlerinin idare tarafından konuşlandırılması (kullanılması) ve sisteme siber saldırı düzenlenmesi durumunda üçüncü kişinin sorumlu olacağına yönelik bkz. Çolpan Mücahit Küçük, 'Yapay Zekâ Tarafından Gerçekleştirilen İdari İşlemde Sorumluluk' (2024) 10(1) Başkent Üniversitesi Hukuk Fakültesi Dergisi 199.

[111] Ramazan Çağlayan, *İdarî Yargılama Hukuku* (10th edn, Seçkin 2018) 692; Kaplan (n 35) 325; Danıştay 10 D, 2021/6103-2022/774, 16.02.2022, *"Zarar görenin kusurunun ağır kusur kapsamında olduğunun tespit edildiği durumlar ise illiyet bağını kesen sebepler kapsamında olduğundan illiyet unsuru gerçekleşmediği için sorumluluk da söz konusu olmayacaktır."*

oluşmasına yol açtığı ileri sürülebilecek olan sosyal mühendislik[112] yöntemlerinin kullanılması durumunda illiyet bağının kesilip kesilmediği meselesi tartışılabilir. Nitekim sosyal mühendislik yöntemlerinde kişinin güveni kazanılarak sisteme erişim için gereken bilgiler elde edilmektedir. Elbette ilk bakışta burada idarenin sistem güvenliğini sağlaması yükümlülüğü ile zarar arasında illiyet bağı yokmuş gibi gözükmektedir. Ancak esasında idarenin sisteme giriş için iki aşamalı kimlik doğrulama sistemini zorunlu hale getirmesi gerekliliği de bu yükümlülük kapsamında değerlendirilebilir. Böylelikle sosyal mühendislik yöntemini kullanan kişinin, ikinci aşamadaki güvenlik sistemini de aşması gerekecektir. Bu yönüyle sistemin güvenliği daha sağlam temellerde temin edilmiş olacaktır. Örneğin Norveç'te, çeşitli güvenlik derecelendirmelerine sahip elektronik kimlik ve elektronik kimlik doğrulama sistemleri bulunmaktadır. Bu kapsamda en çok kullanılan dijital kimliklerden[113] MinID 3. derece, BankID ise 4. ve en üst derece güvenlik sistemine sahiptir. Sözleşmeler, bankacılık işlemleri, dijital kamu hizmetleri gibi birçok özel ve kamu hukuku muameleleri, işlemin güvenlik gereksinimine göre bu sistemler aracılığıyla gerçekleştirilmektedir. İkinci bir güvenlik katmanı niteliğinde olan bu sistemler sosyal mühendislik yöntemlerini oldukça zorlaştırmakta olup sistemin kullanıcılarına bu sistemlerin şifrelerinin kimseyle paylaşılmaması gerektiği en başından yazılı olarak bildirilmektedir. Nitekim bu bilgilere sahip olmayan bilgisayar korsanları, sisteme giriş için bilgileri elde etseler bile ikinci aşamada gereken sistem onayını uzaktan gerçekleştirebilmeleri mümkün olmamaktadır. Farklı ülkelerdeki çeşitli uygulamalar incelenerek güvenilirliği kanıtlanmış çift katmanlı güvenlik yöntemlerinin Türkiye'deki dijital kamu sistemleri açısından hayata geçirilmesinin idarenin dijital alandaki bir yükümlülüğü olduğu belirtilebilir. Nitekim zarar görenin zararının ortaya çıkmasını engelleyebilmesine rağmen böyle bir güvenlik önleminin alınmaması durumunda zarar ile faaliyet arasındaki illiyet bağının kesilmediği ileri sürülebilecektir.

D. Kusur

Dijital hizmet kusuru, idarenin kusura dayanan sorumluluğunun bir türü olduğundan idarenin bu alandaki sorumluluğunun doğabilmesi için kusurun varlığı aranacaktır. Sorumluluk hukuku açısından özel hukuk boyutuyla kusur, kast ve ihmal olmak üzere iki türden ibarettir.[114] Buna karşılık idarenin sorumluluğunun bir şartı olarak kusur, özel hukuktan bağımsızlaşarak kendine özgü bir karaktere sahip olmuştur.[115]

---

[112] *"Bir kişiyi kendi çıkarına olabilecek ya da olmayabilecek bir eylemde bulunması için etkileyen her türlü eylem"* olarak tanımlanan sosyal mühendislik, kişinin güvenini kazanarak sisteme giriş bilgileri gibi verileri elde etmeyi sağlayan bir yöntemdir bkz. Christopher Hadnagy, *Social Engineering: The Science of Human Hacking* (2nd edn, Wiley 2018) 7.

[113] Bunlar dışında sunulduğu şirketler tarafından isimlendirilen Buypass ID 4. seviye, Commfides 4. seviye güvenlik katmanına sahip olup sisteme giriş yöntemleri tercih edilen cihazlara (usb, cep telefonu gibi) göre farklılık göstermektedir bkz. The Norwegian Digitalisation Agency (Digdir), 'How to obtain an electronic ID', (ID-porten) < https://eid.difi.no/en/id-porten/how-obtain-electronic-id > Erişim Tarihi: 18.06.2024.

[114] Fikret Eren, *Borçlar Hukuku Genel Hükümler* (25th edn, Yetkin 2020) 648.

[115] Duran, *Türkiye İdaresinin Sorumluluğu* (n 4) 24; Onar (n 7) 1695; Sarıca (n 5) 859; Özay (n 7) 207; A. Şeref Gözübüyük and Turgut Tan, *İdare Hukuku Cilt II: İdari Yargılama Hukuku* (8th edn, Turhan 2016) 636.

Bilgi ve iletişim teknolojileri sistemleri beraberinde getirdikleri yeniliklerle birlikte bünyesinde riskleri de ihtiva etmektedirler. Sorumluluk meselesi ise riskin yönetilemediği ve akabinde riskin gerçekleştiği andan itibaren gündeme gelmeye başlayacaktır. İdarenin öncelikle risk yönetimi meselesini tüm yönleriyle ele alması ve risk analizi yapması önem arz etmekte olup riskin gerçekleşmesi halinde buradaki ihmalinin boyutu hesaplanarak kusurunun bulunup bulunmadığı değerlendirmesi yapılabilecektir. Nitekim bilgi güvenliğine ilişkin tehditlerin tanımlanması için yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketlerin Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği'nin 10'uncu maddesine istinaden yılda en az bir defa risk değerlendirmesi yapma yükümlülüğü bulunmaktadır. Ancak risk yönetimi kavramı içerisinde yalnızca sistemsel riski değil hukuki riski de barındırdığından, riskin gerçekleşmesinin önlenmesine yönelik hukuki tedbirler öngörülmesi de gerekmektedir.[116] Bu nedenle hukuki risk yönetiminin de gereği gibi yahut hiç yapılmaması ya da geç yapılması kusurun varlığını gündeme getirebilecektir.

Dijital sistemler bünyesinde riski barındırdıklarından, kusur açısından belirli bir ağırlık aranıp aranmayacağı konusunun[117] ele alınması gerekmektedir. Nitekim kapalı ağ sistemleri dışındaki sistemler herkesin erişimine açık olduklarından sistemin her zaman saldırıya uğraması ihtimal dahilindedir. Bu nedenle hafif kusur derecesinden idarenin sorumluluğunun doğup doğmayacağı meselesi üzerinde durulmalıdır. Hafif kusur, ağır hizmet kusurundan daha hafif bir kusur derecesi olup iyi bir idarenin yapmayacağı kusuru ifade etmektedir.[118] Buna karşılık ağır kusur ise vasat veya kötü bir idarenin bile yapmayacağı bir kusur olarak tanımlanmaktadır.[119] Mevzuatımızda dijital ortamdaki kusurlar nedeniyle sorumluluk doğması için herhangi bir kusur derecesi öngörülmemiştir. Hatta idarenin sorumluluğunun Anayasal dayanağı olan Anayasa'nın 125'inci maddesinde basit kusurlardan dolayı idarenin sorumlu olmayacağı anlayışı da benimsenmediğinden basit kusurlarda dahi idarenin sorumlu olabileceği görüşü ileri sürülmektedir.[120] 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun[121] 14'üncü maddesinin üçüncü fıkrasında da kişilik hakları ihlal edilenlerin genel hükümlere göre tazminat hakkının saklı olduğu ifade edilmekle yetinilmiştir. GDPR 82'nci maddesi bağlamında ise zararın tazmini noktasında

[116] Risk yönetimi kavramının hukuki yönden neyi ifade ettiğine ve hukuki risk yönetimi kavramına ilişkin bkz. Jon Bing and Tobias Mahler, 'Contractual Risk Management in an ICT Context - Searching for a Possible Interface between Legal Methods and Risk Analysis' (2006) 49(0) Scandinavian studies in law-A proactive approach 339-342; Tobias Mahler, 'Tool-Supported Legal Risk Management: A Roadmap' (2010) 2(3) European Journal of Legal Studies 147-158.

[117] Duran, *Türkiye İdaresinin Sorumluluğu* (n 4) 34-37.

[118] Sancakdar, Önüt, Us Doğan, Kasapoğlu Turhan and Seyhan (n 5) 851.

[119] ibid 851.

[120] Yıldırım, Yasin, Kaman, Özdemir, Üstün and Okay Tekinsoy (n 7) 838; ancak eskiden idarenin sorumlu tutulabilmesi için ağır hizmet kusuru şartı arandığına yönelik bkz. Lütfi Duran, 'İdari İşlemden Sorumluluk: İptal – Tam Yargı Davası' (1967) 33(3-4) İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 9 < https://dergipark.org.tr/tr/download/article-file/96216 > Erişim Tarihi: 09.10.2024; Gözübüyük and Tan (n 115) 637.

[121] Kişisel Verilerin Korunması Kanunu, Kanun Numarası: 6698, Kabul Tarihi: 24.03.2016, RG: 07.04.2016/29677.

veri sorumlusu ve veri işleyenler yönünden kusur şartı öngörülmemiştir.[122] Maddenin üye devletlerin iç hukuklarında doğrudan uygulanması halinde de sorumluluk değerlendirmesi açısından kusur kriteri aranmayacaktır.[123] Ancak üye devletlerin iç hukuk sistemlerinde aksi öngörülmesi halinde kusur şartı aranabilecektir.[124] Yukarıda da belirttiğimiz üzere dijital hizmet kusuru yalnızca kişisel verilerin ihlalinden kaynaklanan zararlardan ibaret olmayıp idarenin dijital ortamdaki kusurlarını kapsayan bir anlama sahiptir. Bu nedenle konunun siber zafiyetleri de içine alacak şekilde geniş değerlendirilmesinde fayda bulunmaktadır.

Bu çerçevede ilk olarak kusurun derecelendirmesinin esasen doğru olup olmadığını tartışmak gerekecektir. Özellikle siber saldırılar açısından yaklaşıldığında kolluk faaliyeti niteliğinde olan saldırıları önleme yükümlülüğü açısından basit-hafif kusur derecesinde idareyi sorumlu tutmanın hakkaniyetli olmayacağı düşünülebilir. Ancak anayasal olarak bir kusur yoğunluğu ayrımı benimsenmediğinden kusurun yoğunluğu meselesini sorumluluğu etkileyecek bir kriter olarak ele almak hukuki bir yaklaşım olmayacaktır. Belki pragmatik bir çözüm yolu olarak kusur yoğunluğu, kusuru değil ancak tazminat miktarını etkileyebilecek bir mesele olarak öne sürülebilir ancak bu da hukuki bir temele oturmadığından eleştirileri beraberinde getirebilecektir. Dikkat çekilmesi gereken bir nokta olarak teknolojinin her geçen an gelişmesi çerçevesinde idarenin sistemlerini buna uyarlaması aynı hızda gerçekleşemeyebilir. Ancak bunun önüne geçebilmek adına siber güvenlik yatırımlarına yönelik bürokratik muafiyetler tanınması vesilesiyle hızlı aksiyon alınması sağlanabilir. Böylelikle idarenin bu alana yönelik kusurunun ortaya çıkmasının önüne geçilebilir.

İdarelerin özellikle bilişim sistemlerine yönelik olarak siber güvenlik risk değerlendirmesi yapması, zafiyet bulunan noktalarda riskin ortaya çıkmasını önleyecek aşamalardan biri olduğundan risk değerlendirmesi yapılıp yapılmadığının, yapılmış ise önlem alınıp alınmadığının kusur değerlendirmesinde ele alınmasında fayda bulunmaktadır. Bu noktada her somut olay özelinde konunun incelenmesi[125] ve siber güvenlik prosedürlerinin uygulanıp uygulanmadığının ele alınması gerekmektedir. Ülkemiz açısından konu ele alındığında Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ[126] yayınlanmış olup bu kapsamda idareler bünyesinde (m. 4) Siber Olaylara Müdahale Ekipleri (SOME) kurulması öngörülmektedir. Mezkûr düzenlemenin 5'inci maddesinde de SOME'lerin görev ve sorumluluklarına yer verilmiştir. Bununla beraber siber saldı-

[122] Gabriela Zanfir-Fortuna, 'Article 82. Right to compensation and liability' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford 2020) 1176.

[123] Zanfir-Fortuna (n 122) 1176.

[124] ibid 1176.

[125] Hizmet kusuru olaylara göre farklı karakter arz ettiğinden her somut olay açısından risk meselesinin ayrıca değerlendirilerek kusurun yoğunluğunun ele alınması doğru bir yaklaşım olabilecektir. Ayrıca bkz. Onar (n 7) 1697, 1698.

[126] Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, RG: 11.11.2013/28818.

rılara yönelik tedbirlere mevzuatımızda Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği'nin 35'inci maddesi kapsamında yer verilmektedir. Ancak genel olarak baktığımızda mevzuatımızın siber güvenlik tedbirleri yönünden oldukça zayıf olduğu görülmektedir. Özellikle idarelerin bilişim sistemlerine yönelik olarak bir siber güvenlik düzenlemesi yapılması ve bu düzenlemede yükümlülüklerin ortaya konulması, bu alanda yaşanabilecek uyuşmazlıkların önüne geçilmesini sağlayabileceği gibi her somut olaydaki hatanın yargı yerleri tarafından kusur olarak nitelendirilmesinin de önüne geçebilecektir. Bir öneri olarak, bilgi güvenliği ve siber güvenlikten kaynaklanan uyuşmazlıklar açısından ISO/IEC 27001:2022 standardı[127] kusur yönünden değerlendirmelerde olaya uygun düştüğü ölçüde dikkate alınabilir.[128]

Dijital kamu hizmetlerine yönelik faaliyetler açısından ise siber saldırılardan ari olarak sistemin kuruluş ve işleyişinin idare tarafından temin edilmesi gerekmektedir. Bu kapsamda dijital kamu hizmetlerine ilişkin sistemlerin özel hayatın gizliliği, kişisel veriler, kişi ve bilgi güvenliği gibi konular da göz önüne alınarak kurulması anayasal bir gerekliliktir. Bu kapsamdaki uyuşmazlıkların uluslararası işletim standartları ve mer'i mevzuattaki gereklilikler çerçevesinde ele alınması doğru bir yaklaşım olabilecektir.

Gelecek zaman diliminde 'siber güvenlik' anlayışındansa, 'siber dayanıklılık (cyber resilience)' anlayışının benimsenmesiyle birlikte siber tehditlerin bir istisna değil de kural olduğunun kabul edilmesi gündeme gelecek, idarenin de ilerleyen süreçte sorumluluk sahası genişleyecek ve faaliyetteki kusur anlayışı yerini kusursuz sorumluluğa bırakabilecektir[129].

E. Dijital Hizmet Kusurunun İdarenin Kusursuz Sorumluluğuna Sirayet Etmesi

İdarenin asli sorumluluk sebebi olarak kabul edilen kusur sorumluluğu, çalışmadaki kullanımıyla hizmet kusuru, idarenin mali sorumluluğuna ilişkin uyuşmazlıklarında öncelikle incelenmektedir. Kusurun bulunmaması durumunda ise somut olayın kusursuz sorumluluk ilkeleriyle bağdaşıp bağdaşmadığının yargı yerleri tarafından

[127] International Organization for Standardization (ISO), *Information security, cybersecurity and privacy protection — Information security management systems – Requirements* (ISO No. ISO/IEC 27001:2022) (2022) < https://www.iso.org/standard/27001 > Erişim Tarihi 20.06.2024.

[128] Nitekim Türk Standardları Enstitüsü (TSE) de ISO/IEC 27001:2022 standardı yönünden TS EN ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi belgelendirme hizmeti vermektedir bkz. Türk Standardları Enstitüsü, 'TS ISO/IEC 27001:2022 Standardı İçin Geçiş Şartları' (TSE, 16.02.2023) < https://www.tse.org.tr/duyuru/ts-iso-iec-270012022-standardi-icin-gecis-sartlari/?asp_highlight=siber+g%C3%BCvenlik&p_asid=1 > Erişim Tarihi 10.10.2024. Bu nedenle ISO/IEC 27001:2022 standardı uluslararası bir standart olduğundan ve ülkemizde de esas alındığından, uyuşmazlıklarda kusur değerlendirmesi yönünden dikkate alınabilir.

[129] Siber güvenlik ve siber dayanıklılık arasında hukuki yönden farklılığa ilişkin bkz. Lee A. Bygrave, 'Cyber Resilience versus Cybersecurity as Legal Aspiration' in T. Jančárková, G. Visky, I. Winther (eds), *2022 14th International Conferance on Cyber Conflict: Keep Moving! (CyCon)* (NATO CCDCOE 2022) 27; ayrıca bkz. 'Dijital Hizmet Kusurunun İdarenin Kusursuz Sorumluluğuna Sirayet Etmesi' başlığı.

değerlendirilmesi gerektiği kabul edilmektedir.[130] Bundan dolayı dijital hizmet kusuruna ilişkin uyuşmazlıklarda da kusur unsuru bulunmaması halinde kusursuz sorumluluk yönünden değerlendirme yapılması gerekecektir. Bu nedenle mevcut çalışma kapsamında, idarenin dijital alandaki bir faaliyetinden kaynaklanan zararlara ilişkin uyuşmazlıklarda kusurun bulunmaması halinde kusursuz sorumluluk ilkeleri yönünden değerlendirme yapılıp yapılamayacağının da kısa da olsa ele alınması gerektiği düşünülmektedir.

İdarenin kusursuz sorumluluğu risk ve kamu külfetleri karşısında eşitlik olmak üzere iki temel ilkeye dayanmaktadır.[131] Dijital hizmet kusuruna ilişkin uyuşmazlıklarda genellikle kitlesel etkilenme potansiyeli bulunmaktadır. Diğer bir ifadeyle sistemin bozulması veya sistemden dolayı bir aksama yaşanması halinde, bundan o sistemi kullanan birçok kişi etkilenebilecektir. Bu nedenle kitlesel uyuşmazlıklar bakımından her bir davacıya kusuru ispat külfeti yüklemek yerine kusursuz sorumluluk esasının kabul edilmesi gerektiği bir öneri olarak sunulabilir. Ancak bununla beraber kitlesel zararın karşılanması noktasında, idareye kusuru bulunmasa dahi sorumluluk yüklemek devlete mali açıdan katlanılamaz yükler yüklemek anlamına da gelebilir. Bu noktada örneğin zarar görenin eylemine bağlanabilen, phishing yöntemiyle yapılan saldırılar gibi, zararlarda dahi idareyi kusuru olmasa da sorumlu tutmak makul bir yaklaşım olarak kabul görmeyebilir. Ancak bununla beraber dijital sistemlerin bünyesinde barındırdığı risk dolayısıyla, bu sistemlerde gerçekleşen zararların *risk sorumluluğu* kapsamında değerlendirilip değerlendirilemeyeceği de üzerinde düşünülebilir bir husustur. Nitekim dijital sistemlerin bünyesinde risk barındırması[132] risk sorumluluğu bağlamında konuyu kısa da olsa ele almayı gerektirmektedir. Esasında bilgi teknolojilerine ilişkin sistemlerde, sistem güvenliğine yönelik riskin değerlendirilerek buna ilişkin önlemler alınması beklenmektedir. Yani salt sistemin risk içermesi nedeniyle doğrudan idarenin kusursuz sorumluluğa gidilmesi mümkün

---

130 Danıştay 10 D, 2020/809-2024/2348, 03.06.2024: *"Tam yargı davalarında, öncelikle zarara yol açtığı öne sürülen idari işlem veya eylemin hukuka uygunluğunun denetlenmesi esas alındığından, olayın oluşumu ve zararın niteliği irdelenip, idarenin hizmet kusuru olup olmadığının araştırılması, hizmet kusuru yoksa kusursuz sorumluluk ilkelerinin uygulanıp uygulanmayacağının incelenmesi, tazminata hükmedilirken de her halde sorumluluk sebebinin açıkça belirtilmesi gerekmektedir."*; benzer yönde bkz. Danıştay 8 D, 2015/14519-2019/167, 17.01.2019; Danıştay 15 D, 2016/8172-2017/7132, 30.11.2017; Danıştay 8 D, 2004/784-4445, 23.11.2004.

131 Gözler (n 2) 1188, 1261; Günday (n 11) 379, 382; Ozansoy (n 11) 294; Yayla, *İdarenin Kusursuz Sorumluluğu* (n 11) 30.

132 Dijital unsur içeren ürünlere ve dijital platformlara ilişkin risk konusu çok kapsamlı bir mesele olup monografik bir çalışmanın kapsamını oluşturabilecek boyuta sahiptir. Bu siber alandaki risk mühendislik, ekonomik ve sosyal bilimler açısından da farklı anlamlara sahiptir bkz. Grzegorz Strupczewski, 'Defining Cyber Risk' (2021) 135 Safety Science 1-10 < https://doi.org/10.1016/j.ssci.2020.105143 > Erişim Tarihi 15.10.2024; Örneğin AB'nin Digital Services Act (DSA) düzenlemesinde çok büyük çevrimiçi platformlar ve çok büyük çevrimiçi arama motorları tarafından sistemik riskin değerlendirilmesine yönelik yükümlülükler öngörülmektedir bkz. DSA Recital 80; ayrıca DSA kapsamında platformlara ilişkin sistemik risk dört kategoriye ayrılmakta olup bunlar 1- Yasadışı içeriğin yayılması, 2- Temel hakların kullanılmasına yönelik olumsuz etkiler, 3- Sivil söylem ve seçim süreçleri ile kamu güvenliği üzerindeki olumsuz etkiler, 4- Cinsiyete dayalı şiddet, kamu sağlığının ve küçüklerin korunması ile ilgili olumsuz etkiler ve kişinin fiziksel ve ruhsal refahı üzerinde ciddi olumsuz sonuçlar olarak sınıflandırılmıştır bkz. Jason Peilemeier and David Sullivan, 'Unpacking "Systemic Risk" Under the EU's Digital Service Act' (Tech Policy, 19 July 2023) < https://www.techpolicy.press/unpacking-systemic-risk-under-the-eus-digital-service-act/ > Erişim Tarihi: 15.10.2024.

görünmemektedir.[133] Bununla birlikte sistemsel risk değerlendirmesi yapılıp bu risk değerlendirmesi doğrultusunda somut adımlar atılmış ve sistem güvenliğinin sağlanmasına yönelik yükümlülükler gerçekleştirilmiş ise bu durumda kusurdan bahsedilemeyecektir ve idarenin kusursuz sorumluluğunun doğup doğmayacağı ele alınacaktır. Risk ilkesi açısından bakıldığında idarenin dijital ortamdaki faaliyetlerini bir tehlikeli faaliyet olarak görmek çok mümkün görünmemektedir. Dijital unsur içeren araçları ise mevcut kusursuz sorumluluk teorisi açısından tehlikeli araç olarak kabul etmenin de doğru bir yaklaşım olmayacağı aksi takdirde bu alanda ortaya çıkan neredeyse her olay bakımından idareyi sorumlu tutmak yoluna gidilebileceği değerlendirilmektedir. Bununla birlikte, siber güvenlik anlayışından siber dayanıklılık anlayışına[134] geçilmesi halinde dijital unsur içeren sistemlerin bünyesindeki risk dolayısıyla, risk ilkesi çerçevesinde kusursuz sorumluluğun gündeme gelmesi daha da tartışılabilir hale gelecektir. Nitekim mevcut mali sorumluluk şartları açısından idarenin dijital alandaki faaliyetlerinde kusurun ispatının oldukça zor olması nedeniyle bu çalışma kapsamında dijital hizmet kusurundan kaynaklanan uyuşmazlıklarda ispat külfetinin idareye yüklenmesi önerilmektedir.[135] Bu bir geçiş adımı olarak da değerlendirilebilir. Nitekim bundan sonraki aşamada idarenin dijital faaliyetlerinden kaynaklanan sorumluluğu yönünden kusursuz sorumluluğa geçiş yapılabilir. Öncelikle kusurlu sorumluluğuna dayanılma sebebi ise idarenin asıl sorumluluğunun günümüzde kusura dayanıyor olmasıdır. Kusursuz sorumluluğun asıl olacağını ifade etmek hem günümüzde benimsenen idarenin kusura dayanan sorumluluğunun birincilliğiyle çelişecek hem de dijital ortamda doğan neredeyse hemen her zararı idareye atfetmeye yönlendirebilecektir. Bu nedenle dijital faaliyetlerden kaynaklanan zararların giderilmesi için öncelikle kusura dayanan sorumluluk anlayışının oluşturulması ve akabinde belirli durumlarda kusursuz sorumluluk anlayışının da geliştirilmesi önerilebilir.

Bir diğer mesele ise yine risk ilkesi bünyesinde, siber saldırılardan kaynaklanan zararların tıpkı terör eylemlerinden kaynaklanan zararlardaki gibi sosyal risk bağlamında değerlendirilip değerlendirilemeyeceği meselesidir. Sosyal risk ilkesi açısından, illiyet bağının daha geniş ele alınması ve devletin egemenlik alanında zararın gerçekleşmesi sebebiyle idarenin sorumluluğuna gidilebilmesi oldukça önemli bir noktadır. Dijital hizmet kusuruna ilişkin uyuşmazlıklarda da illiyet bağı unsuru yönünden özellikle dijital kamusal alan olarak nitelendirdiğimiz alanda meydana gelen zararların devletin egemenlik alanında meydana geldiği kabul edilerek kusurun varlığı halinde dijital hizmet kusurunun gündeme gelmesi önerilebilir. Keza kusursuz sorumluluk açısından da yine sosyal risk ilkesi bağlamında dijital kamusal alan değerlendirmesi

[133] Örneğin yapay zekaya ilişkin olarak da yapay zekâ sisteminin yazılımdan ibaret olması sebebiyle mevcut anlayış açısından bir tehlikeli araç vasfında değerlendirilemeyeceğine yönelik bkz. Yayla, *İdare Hukuku Bakımından Yapay Zeka* (n 32) 170; ayrıca bkz. Seyhan (n 32) 311-335.

[134] Nitekim ex ante denetim mekanizması esas alınarak hazırlanan siber dayanıklılık anlayışına Türkiye'nin 2024-2028 siber güvenlik strateji planında da yer verilmekte ve siber dayanıklılık bir hedef olarak belirlenmektedir bkz. T.C. Ulaştırma ve Altyapı Bakanlığı, *2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı* (n 64) 21.

[135] Bkz. 'Delil ve Zararın Tespiti' başlığı.

yapılarak burada gerçekleşen saldırılar nedeniyle meydana gelen zararlardan idarenin kusursuz da olsa sorumlu tutulması gerektiği yönünde bir öneride bulunulabilir. Bu tür eylemlerin terör eylemine benzerliği de oldukça dikkat çekicidir. Ayrıca konu açısından sosyal risk ilkesi ile bağlantı kurmayı da mümkün kılmaktadır.

Kamu külfetleri karşısında eşiklik ilkesi ise kusursuz sorumluluğun ana ilkesi olarak kabul edildiğinde risk ilkesini de kapsayacak[136] daha geniş bir kusursuz sorumluluk sebebi olarak idarenin dijital ortamdaki faaliyetlerinden kaynaklanan zararların karşılanmasında bir çözüm olarak gündeme gelebilecektir.

Tekrar belirtmek gerekir ki idarenin dijital alandaki faaliyetlerinden kaynaklanan kusursuz sorumluluğu ve buna yönelik bir anlayışın geliştirilmesi farklı bir çalışmanın konusunu oluşturabilecek kapsama sahiptir. Bu nedenle bu başlık kapsamında sadece dijital hizmet kusurunun mevcut olmaması halinde kusursuz sorumluluk yönünden de yargı yerlerince değerlendirme yapılması gerektiğine dikkat çekilmektedir.

III. İdarenin Dijital Alandaki Faaliyetlerinden Kaynaklanan Sorumluluğuna İlişkin Çeşitli Sorunlar Ve Öneriler

Dijital hizmet kusuru, idarenin dijital alandaki faaliyetlerinden kaynaklanan ve asli sorumluluk türü olan kusura dayanan sorumluluğu olarak önerilmektedir. Ancak bununla birlikte ilerleyen zamanlarda idarenin dijital ortamdaki faaliyetlerinden kaynaklanan sorumluluğunun kusursuz sorumluluğa dayanması ihtimali de gündeme gelebilir. Başlık kapsamında ileri sürülen bu sorunlar genel olarak yargılama aşamasında gündeme gelebilecek sorunlardır. Bu nedenle bu başlık kapsamında tespit edilen sorunlar ve bunlara ilişkin öneriler dijital hizmet kusurundan kaynaklanan uyuşmazlıklar açısından geçerli olabileceği gibi bahsedilen kusursuz sorumluluk esasının gelişmesi halinde de ortaya çıkabilir. Bu nedenle bu bölümün başlığında, *idarenin dijital alandaki faaliyetleri* ifadesi tercih edilmiştir.

A. Sorumluluk Alanının ve Hasmın Belirlenmesi

Dijital mecrada idarenin sorumluluğunun hangi alanla sınırlı olduğunu tespit edebilmek oldukça güçtür. İdarenin, kamu hizmetini sunduğu yani yer[137] ve/veya aynı zamanda içerik sağlayıcısı[138] olduğu ve doğal olarak alan adı sahibi olduğu alanda (domain) bir zararın ortaya çıkması ve şartların gerçekleşmesi halinde sorumluluğunun doğacağı belirtilebilir. E-Devlet, Dijital Vergi Dairesi, UYAP, e-SGK, e-Belediye platformları gibi kamu hizmetlerinin dijital ortamda emanet usulü ile sunulduğu ve idarelerin içerik ve/veya yer sağlayıcısı olduğu ortamların "*dijital kamusal alan*" ola-

[136] Yayla, *İdarenin Kusursuz Sorumluluğu* (n 11) 61; Yayla, *İdare Hukuku Bakımından Yapay Zeka* (n 32) 170.

[137] 5651 sayılı Kanun'un 2'nci maddesi kapsamında yer sağlayıcı *"Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler"* olarak tanımlanmaktadır.

[138] 5651 sayılı Kanun'un 2'nci maddesi kapsamında içerik sağlayıcı *"İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler"* olarak tanımlanmaktadır.

rak nitelendirilmesinin, sorumluluk alanı açısından daha belirleyici olacağı düşüncesiyle bu alanları dijital kamusal alan olarak adlandıracağız.[139] Bu alanları tanımlamak için mevzuatta henüz herhangi bir tanım bulunmaması nedeniyle bu tanımlama sorumluluk alanı açısından yol gösterici olabilecektir.

Alan adı sahipliği ve Top-Level Domain'ler (TLDs) baz alınarak uyuşmazlıklardaki hasım tespitinin yapılabileceği ileri sürülebilir. Alan adında ".gov, .edu, .bel,..." gibi kamusal idarelere özgü sponsored-TLDs veya second-level domain kullanan kamu tüzel kişilerinin alan adı sahibi olduğu dijital alanda meydana gelen zarar nedeniyle husumetin kendisine yöneltilebilmesi mümkün diye düşünülebilir. Ancak bu yöntemi kullanmak her zaman doğru sonuç vermeyebilir. Türkiye'de birçok kamu idaresi ve kamu kurumunun hizmetleri, e-Devlet entegrasyonu çerçevesinde e-Devlet üzerinden sağlanıyormuş gibi görünse de sistem kapsamındaki içerik ilgili idare tarafından temin edilmektedir. Örneğin yükseköğretim belgelendirme hizmetleri açısından birçok içerik e-Devlet üzerinden ilgili yükseköğretim kurumu tarafından sağlanmaktadır. Bu kapsamda yalnızca TLDs ve alan adı sahibi esas alınarak sorumluluk açısından belirleme yapıldığında sanki husumetin "turkiye.gov.tr" alan adı esas alınarak tespit edilmesi gerektiği anlaşılacak ve bu anlayış doğrultusunda husumetin, alan adı sahibi olan ve müstakil bir kamu tüzel kişiliğini haiz Cumhurbaşkanlığı Dijital Dönüşüm Ofisine yöneltilmesi gerekecektir. Ancak esasında alan adıyla birlikte dijital kamu hizmetinin içeriğinin kimin tarafından sağlandığına da bakmak doğru sonuç verecektir. Yani alan adı sahipliği tek başına, sorumluluğun kime ait olduğunun bir belirleyicisi değil hizmetin kim tarafından yerine getirildiğiyle birlikte dikkate alınacak olan yardımcı bir unsur olacaktır.[140]

Böylelikle önce idarenin sorumluluk alanının belirlenmesi ve ardından idarenin sorumluluk alanında kaldığı düşünülen durumlarda husumetin hangi idareye yöneltileceği meselesinin ele alınması gerekecektir. Bu nedenle öncelikle idarenin sorumluluğunun şartları açısından ortada dijital bir idari faaliyet olup olmadığı konusu ele alınacaktır. Bu kapsamda dijital kamu hizmetinin sağlandığı ortam, 'dijital kamusal alan' olarak nitelendirilecek ve hizmeti sağlayan kamu tüzel kişisi tespit edilerek husumet yöneltilebilecektir. Böylelikle emanet usulü ile dijital ortamda yani dijital kamusal alanda sunulan kamu hizmetlerinden kaynaklanan zararlarda husumetin yöneltileceği kamu tüzel kişisinin tespitinde çok zorluk yaşanmayacaktır.

İkinci bir soru olarak, kamu hizmetinin özel kişilerce dijital ortamda sunulması halinde nasıl bir belirleme yapılacaktır? Örneğin elektronik sertifikasyon hizmeti sağlayıcılarının sağladığı e-imza hizmetinde bir aksama ve dolayısıyla bir zarar meydana

[139] Dijital ortamdaki kamusal alan kavramının, idarenin otomatik karar alma sürecinin etik boyutu bakımından değerlendirilmesine ilişkin olarak bkz. Dag Wiese Schartum, 'Law and alghorithms in the public domain' (2016) 1(0) Etikk i praksis 15-26.

[140] Bu fikrin geliştirilmesine katkı sağlayan Prof. Lee Andrew Bygrave'e teşekkür ederim.

gelmesi halinde bu hizmet bir kamu hizmeti olarak mı değerlendirilecek, eğer öyle ise sorumluluk kime ait olacak, uyuşmazlık nedeniyle hangi yargı koluna gidilecek gibi sorular akıllara gelmektedir. Bir diğer örnek olarak 5369 sayılı Evrensel Hizmet Kanununa istinaden evrensel hizmet (m. 2) ve dolayısıyla kamu hizmeti (m. 1) olarak kabul edilen internet erişim hizmetindeki aksama nedeniyle, idarenin sorumluluğu doğacak mıdır? Bu noktada hizmet sağlayan ile hizmetten yararlananlar arasındaki ilişkinin ve sözleşmenin niteliğine bakmak gerekecektir. Özellikle internet erişimi hizmetinde, abonelik sözleşmesi ilişkisinden dolayı burada meydana gelen aksamalarda kişiler ile internet servis sağlayıcısı arasında sorumluluk ilişkisinin cereyan edeceği[141] ve bunun özel hukuk hükümleri çerçevesinde adli yargıda giderileceği belirtilebilir. Ancak abonelik sözleşmesi bulunsa bile ulusal yahut bölgesel çapta bir servis sunumundan kaynaklanabilecek aksamalarda idarenin de servis sağlama yönünden yükümlülükleri belirlenerek idarenin de sorumluluğunun gündeme gelebilmesinin ihtimal dahilinde olduğu belirtilmelidir. Nitekim hizmetin asli sahibi idaredir. Bunlar dışında kalan diğer durumlarda kamu hizmetinin özel kişilere gördürülmesi rejimindeki esaslar dikkate alınacak, hizmetten yararlananlar ve üçüncü kişilerin gördükleri zararlar nedeniyle idarenin sözleşme dışı sorumluluğu gündeme gelecektir.[142]

Üçüncü soru ise dijital kamusal alan dışında kalan dijital idari kolluk faaliyetleri nedeniyle meydana gelen zararlarda idarenin sorumluluk alanı genişleyecek midir? Öncelikle dijital kamusal alan kapsamındaki kolluk faaliyetlerinden kaynaklanan zararlarda bir kusur bulunması ve faaliyetten kaynaklanan bir zararın meydana gelmesi halinde dijital hizmet kusurundan kaynaklanan zarar nedeniyle idareye husumet yöneltilebilecektir. Bu kapsamda kanımızca husumetin alan adı sahibi idareye yöneltilmesi daha doğru olacaktır. Nitekim aksi düşüncede siber güvenliği sağlama yönünden hizmet alımı usulü uygulanması halinde husumetin özel hukuk kişisine yöneltilmesi gerekeceği sonucu çıkabilir. Böyle bir karışıklığa mahal vermemek adına alanın korunmasına yönelik yükümlülüğü alan adı sahibine yüklemek suretiyle husumetin dijital kamusal alandaki alan adı sahibi idareye yöneltilmesinin daha doğru sonuç vereceği ileri sürülebilir. Ancak esas soru idarenin kamusal dijital alan dışında

[141] Aynı yönde bkz. Turgut Kaya, *İnternet Servis Sağlayıcısının Hukuki ve Cezai Sorumluluğu* (Seçkin 2019) 104-107.

[142] Ezgi Palas Dağlı, *Kamu-Özel İşbirliği Modeli ve İdarenin Sorumluluğu (Sağlık Hizmetlerinde)* (Seçkin 2024) 220.

yani özel platformlarda gerçekleştirdiği sanal devriye, erişimin engellenmesi[143], bant genişliğinin daraltılması gibi önleme faaliyetlerinden kaynaklanan zararlarda ne olacağıdır. Böyle bir durumda artık alan adı sahibinin yahut yer sağlayıcının değil, dijital idari kolluk faaliyeti yapan idarenin sorumluluğunun doğacağını belirtebiliriz. Bu noktada zararın ortaya çıkmasına neden olan idare olduğundan sorumluluğa yönelik talebin idareye yöneltilmesi gerekecektir. Özellikle tartışmalı nitelikte olan derin paket analizi, sanal devriye, erişimin engellenmesi, bant genişliğinin daraltılması gibi dijital idari kolluk faaliyetleri kamusal dijital alan dışında vücut bulduğundan, bu faaliyetlerin Anayasa'nın 13'üncü maddesindeki sınırlama sebepleri de dikkate alınarak gerçekleştirilmesi gerektiği izahtan varestedir. Bu nedenle anayasal ölçütlere uymayan kolluk işlemlerinden kaynaklanan zararlarda, idarenin sorumluluğu gündeme gelebilecektir.

B. Tespitinin Uzmanlık Gerektirmesi

Dijital alandaki olaylara ilişkin tespitler, teknik bir konu olduğundan dolayı uzmanlık gerektirmektedir. Bilgi ve iletişim teknolojilerine ilişkin çeşitli uzmanlık konuları olduğundan her somut olay bağlamında özel değerlendirme yapılmasına yönelik konuyla ilgili uzman kişilerin desteğini almak doğru sonuçlar verebilecektir. Bu husus davanın açılmasından sonuçlanmasına kadar birçok aşamayı içermektedir. Dava dilekçesinin hazırlığı aşamasında davacının, savunma aşamasında idarenin ve yargılama aşamasında mahkemenin konuyla ilgili uzman kişilerden destek alması hukuki savlarını ve gerekçelerini oluşturabilmesi açısından önem arz edecektir.

Yargılama aşamasına geçilmeden önce siber zafiyetleri önlemek adına "bu konuyla ilgili bir regülasyon faaliyeti, sertifikasyonu ve uzman bir kurum üzerine düşünülebilir mi?" sorusunu değerlendirmek gerekmektedir. Avrupa Birliği açısından konu ele alındığında, European Union Agency for Cybersecurity-Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) bu konuda uzman bir kurum olarak karşımıza çıkmaktadır.

[143] Erişimin engellenmesinin tazminat boyutu ayrı bir çalışmanın konusunu oluşturabilecek nitelikte geniş olduğundan çalışmanın bütünlüğünü bozmamak adına burada yalnızca ilgili görüşleri paylaşacağız. Erişimin engellenmesi kararının uygulandığı maddeye göre değişen hem bir koruma tedbiri hem de bir idari tedbir niteliği olduğundan konunun iki yönü bulunmaktadır. Koruma tedbiri açısından; bir görüşe göre koruma tedbiri niteliğinde verilen erişimin engellenmesi kararı, 5271 sayılı Ceza Muhakemesi Kanunu (CMK) 141'inci maddesi kapsamında sayılmadığından tazminat istenemeyeceği ileri sürülmektedir (bkz. İsmail Çınar, '5651 sayılı Kanun Çerçevesinde Koruma Tedbiri Olarak İnternet Ortamında Yapılan Yayınlarda İçeriğin Çıkarılması ve/veya Erişimin Engellenmesi' (2021) 8(1) İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 85). Ancak diğer görüş uyarınca CMK'nın 141'inci maddesinin üçüncü fıkrasına istinaden sayılanlar dışındaki koruma tedbirlerinden kaynaklanan zararlarda da ağır ceza mahkemelerinde CMK hükümlerine istinaden tazminat davası açılabilecektir ve nitekim Yargıtay da bu görüşü benimsemektedir (bkz. Yargıtay 12 CD, 13049/17584, 11.11.2015; Uğur Demiral, *Bir Koruma Tedbiri Olarak Şirket Yönetimi İçin Kayyım Tayini (CMK m. 133)* (Seçkin 2021) 158, Mehmet Taştan, *Koruma Tedbirleri Nedeniyle Tazminat Davaları* (Adalet 2019) 116). Diğer yandan 5651 sayılı Kanun 8/A maddesi ile 9/A maddeleri kapsamında öngörülen ve idari tedbir niteliğinde olan erişimin engellenmesi kararından kaynaklanan uyuşmazlıklarda bir idari kolluk faaliyeti söz konusu olduğundan bu karar nedeniyle bir zararın ortaya çıkması ve idarenin kusurunun bulunması halinde idarenin sorumluluğu yoluna gidilebilecektir.

2004 yılında kurulan[144] ENISA'nın, 2019 yılında yayımlanan Cybersecurity Act[145] ile yetkilerinde önemli değişikliklere gidilmiş ve Kurum'a siber güvenlik ile ilgili konularda önemli yetkiler verilmiştir. Günümüz itibariyle ENISA, siber güvenlik konusunda uzman bir merkez olup (Cybersecurity Act m. 4), dijital unsur içeren ürünlerin siber güvenlik yönünden sertifikasyonuna (Cybersecurity Act m. 8) yönelik çeşitli görevleri bulunmaktadır. Ülkemizdeki uygulama açısından bakıldığında konunun BTK yönünden yürütülmesi ilk aşamada akla gelebilir. Ancak BTK'nın artan iş yükü ve uğraş alanına gün geçtikçe birçok bilgi ve iletişim teknolojisi meselesi girmesi nedeniyle siber güvenlik alanında uzman müstakil bir regülasyon ve ürün sertifikasyon kurumu öngörülmesi amaca uygun bir yaklaşım olabilecektir. Nitekim bilgi ve iletişim teknolojileri alanına ilişkin olarak tüm iş yükünü tek bir kuruma bırakmak hizmette aksamaya yola açma potansiyeline sahip olduğu gibi bu alana ilişkin tek bir kurum öngörmek yapay zekâ, siber güvenlik, iletişim teknolojileri, bilgi teknolojileri gibi çok farklı ve sürekli gelişen alanlarda ve uzmanlık isteyen konularda uzmanlaşmayı da engelleyebilecektir. ENISA gibi yalnızca siber güvenlik tedbirleri ve ürünlerin siber güvenlik yönünden sertifikalandırılması konularıyla ilgilenen bağımsız ve tarafsız nitelikleri haiz milli siber güvenlik kurumunun kurulması uzmanlaşma konusunda oldukça büyük destek sağlayacaktır. Ayrıca belirtmek gerekir ki siber güvenlik konusunda özel sektörün de işin içine dahil edilmesi daha hızlı ve efektif davranmayı sağlayabilecektir. Nitekim ENISA'da siber tehditlere karşı kamu-özel iş birliği modelinin oluşturulmasına yönelik çalışmalar yürütmektedir.[146] Bu konuya ilişkin bir ek olarak, bilgi ve iletişim teknolojileri alanlarında AB regülasyonlarıyla uyum sağlayacak düzenlemeler yapılması, bu alanda üretim ve AB'ye ihracat yapanlar açısından da kolaylaştırıcı olacak, mevzuatlar arasındaki uyumsuzluk nedeniyle ilgililerin üretimlerinde iç pazar ve dış pazar arasında kalmasının önüne geçilebilecektir.

Yargılama aşamasında ise kusurun tespiti özellikle zorluk gösterebilecek konulardan biridir. Kusurun kime atfedileceği konusu, kusurun yoğunluğu meselesi gibi konular sübjektif olduğundan bu noktada objektif bir değerlendirme yapabilmek çok da kolay görünmemektedir. Bu nedenle uzman bilirkişilerden destek alınmak suretiyle muhakeme yapılması ilk aşamada hakkaniyetli sonuçlar ortaya çıkmasını destekleyebilecektir. İlerleyen süreçte, teknolojinin hayatımızdan ayrı olarak düşünülemeyeceği, yapay zekanın her alana yayılacağı ve hukuki uyuşmazlıkların teknolojilerden ayrışamayacağı noktaya gelindiğinde, belki de uzman bilişim mahkemelerinin kurulması gündeme gelecektir.

---

144 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77.

145 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151.

146 ENISA, *Public Private Partnerships (PPP): Cooperative models* (ENISA 2017) 7.

C. Hak Arama Yolu

Özellikle dijital idari sistemlere yapılan saldırılarda birçok kişinin zarar görmesi ihtimal dahilindedir. Örneğin, e-Devlet gibi bir sistem tüm vatandaşların verilerini içerdiğinden sistemin tamamında gerçekleşecek bir hatada milyonlarca kişinin zarar görmesi söz konusu olabilir. Böyle bir durumda her bir kişinin tek tek dava açma yoluna gitmesi halinde milyonlarca davanın açılması gündeme gelecektir. Bu durum, usul ekonomisiyle bağdaşmayacağı gibi yargının iş yükünü de olağanüstü derecede arttıracak ve adaletin tecellisinde gecikmeler yaşanabilecektir. Bu nedenle dijital hizmet kusurundan kaynaklanan uyuşmazlıklarda grup dava uygulamalarının kabul edilmesi öngörülebilirliği sağlayacak ve aynı konuda farklı kararlar verilmesinin de önüne geçebilecektir.[147] Grup dava uygulamalarından, yargısal görüş, grup başvurular ve topluluk davası imkanlarının[148] dijital hizmet kusuruna yönelik uyuşmazlıklarda yargılama usulü yönünden uygulanabilmesi kanaatimizce mümkündür. Bu kapsamda hak arama yollarına ilişkin sorun oluşturabilecek hususlar bertaraf edilmiş olacaktır. Elbette bu husus yargılama usulüne ilişkin bir mesele olduğundan öncelikle grup dava uygulamalarının kanuni temele oturtulması gerekecektir.

D. Delil ve Zararın Tespiti

Maddi dünyada cereyan eden idari ilişkilerde işlemler bir yazıya bağlandığından, eylemler de bir iz bıraktığından bu eylem ve işlemler esas alınarak yargılama yapılması nispeten daha kolay yürümektedir. Bu işleme yahut eyleme dayanak teşkil eden belgelerin idareden celbi talep edilerek yargılama safhasında muhakeme yapılmaktadır. Ancak dijital deliller nasıl elde edilecek ve idari yargıda nasıl değerlendirilecektir? Mahkemenin, Devletin ve idarenin sunucularına inceleme yaptırması belirli noktalarda milli güvenlik menfaatlerinin bulunması da göz önüne alındığında nasıl gerçekleşecektir? İşte bu gibi sorunlar delil elde edilebilmesinin ve nihayetinde kusurun idare atfedilebilmesinin önünde engeller oluşturacaktır. Nitekim dijital deliller iz bıraksa da isteyerek veya yanlışlıkla bu izler üzerinde oynama yapılabilmesi, delillerin bozulabilmesi ihtimal dahilindedir. Bu konuda yargı yerlerinin konusunda uzman adli bilişim alanında (digital and cyber forensics) çalışanlardan destek alması daha doğru sonuçlar verecektir. Ayrıca idarenin dijital delilleri sunmamasına yönelik yaklaşımını benimsemesinin de önüne geçici hukuki araçlar öngörülmesi uygun olabilecektir. Bu kapsamda ispat yükünün idareye çevrilmesi ihtimal dahilinde düşünülebilecek konulardandır. Zira dijital hizmet kusurunda davacı taraf, hangi delile dayanacağını da bilemiyor pozisyonda olabilir. Bilişim sisteminin işleyişini bilmeyen ve oldukça teknik nitelikte olan dijital hizmet kusuruna ilişkin uyuşmazlıklarda davacıya ispat külfetini yüklemek hakkaniyete aykırı sonuçlar meydana getirebilecek

147 Lale Burcu Önüt, *İdari Yargılama Hukukunda Adil Yargılanma İlkesi Çerçevesinde Grup Dava Uygulaması* (Seçkin 2018) 86.

148 Önüt (n 147) 87-136.

potansiyeldedir. Bu nedenle özellikle re'sen araştırma ilkesi gözetilerek gerektiği noktalarda delillerin re'sen ve bizzat yargı yerince araştırılması bu riski gidebilecektir. Yahut dijital hizmet kusuruna ilişkin uyuşmazlıklarda ispat külfetinin tersine çevrilerek idareye yükletilmesi ikinci bir öneri olarak sunulabilir.

Dijital hizmet kusurunda meydana gelen zararın tespiti, maddi dünyada meydana gelen zararın tespitine kıyasla daha zordur.[149] Nitekim dijital dünyadaki zararın hem dijital varlıklara etkisi söz konusu olabilecek hem de burada meydana gelen zarar maddi dünyaya da sirayet edebilecektir.[150] Dijital hizmet kusurunda özellikle manevi nitelikteki zararlar açısından belirleme yapmak oldukça güçtür. Nitekim veri kaybı, siber saldırı nedeniyle gelecekte olabileceklere yönelik korku yaşanması, özel hayatın gizliliğinin ihlali nedeniyle üzüntü duyulması gibi sübjektif, kişiden kişiye değişebilen duygular üzerinden bir zarar değerlendirmesi yapılması oldukça güçtür. Nitekim maddi nitelikteki dijital varlıklar açısından da durum bazen zorlaşabilmektedir. Örneğin, günümüzde maddi açıdan değersiz görülebilen bir alan adı, NFT veya kripto para birimleri gibi dijital varlıklar ileride çok büyük değerlere ulaşabilmektedir. Varlığın günümüz açısından maddi değerlemesinin yapılması halinde geleceğe yönelik çok büyük kayıplar yaşanması ihtimal dahilinde olabilecektir. Özellikle yapay zekâ sistemlerinin devreye girmesiyle birlikte bu tartışmalarda artış yaşanacaktır. Aynı özellikleri göstermese de destekten yoksun kalma tazminatında olduğu gibi bir ölçeklendirme metodu geliştirilmesi üzerinde düşünülebilir. Örneğin kimlik numarası, ad-soyad, adres, aile bilgileri gibi verilerin herkes açısından benzer derecede öneme sahip olması nedeniyle bu gibi verilere önceden bir değer biçilerek zararın değerlemesinin bu ölçeklendirmeye göre hesaplanması bir öneri olarak ileri sürülebilir. Elbette kamuoyunu ilgilendiren kişilerin bu gibi verileri daha önemli olarak düşünülecek ve uğradığı zararın tespiti yapılırken bu etken de göz önünde bulundurulacaktır. Bu gibi ölçeklendirme metodunun tüm veriler yahut dijital varlıklar açısından yapılması mümkün olmadığından herkesin sahip olduğu temel kişisel veriler yönünden ele alınması daha doğru bir yaklaşım olabilecektir. Nitekim böyle bir yöndem başlı başına maddi zararı tespit etmeyi sağlayacaktır. Bununla birlikte manevi zararın da şartlarının oluşması halinde talep edilmesi mümkün olacaktır. Ayrıca ABAD'ın, kişisel verilerin çalınmasından ve bu nedenle gelecekte kötüye kullanılması ihtimalinden dolayı ilgilinin yaşadığı korkuyu bir manevi zarar olarak kabul etmesi de oldukça önemlidir.[151] Öğretide, kişisel veriler nedeniyle idareye idari para cezası uygulandığında, elde edilen gelirin mağdurlara tazminat olarak dağıtılabileceğine yönelik önemli bir görüş de ileri sürülmüştür.[152] Nitekim bu görüş idareye uygulanan para cezasının diğer yandan yine idareye dönmesine yönelik anlayışı da bertaraf edebilecek

[149] Zarar ile ilgili olarak 'Zarar' başlığında açıklamalarda bulunulmuş olup ayrıca o başlığa da bakılması önerilmektedir.

[150] Sasha Romanosky and Zachary Goldman, 'Understanding Cyber Collateral Damage' (2017) 9(2) Journal of National Security Law&Policy 238.

[151] Bkz. 'Zarar' başlığı.

[152] Lintvedt (n 94) 15.

niteliktedir. Ancak yukarıda da belirttiğimiz üzere[153] mevzuatımız kapsamında kişisel verilerin ihlali nedeniyle idareye para cezası uygulanmasına cevaz verilmediğinden bu imkânın öngörülebilmesi için öncelikle mevcut düzenlemenin değiştirilmesi gerekmektedir. Farklı bir görüş tarafından ise veri ihlallerine ilişkin olarak zorunlu mali sorumluluk sigortası öngörülmesi önerilmiştir.[154] Özel hukuk ilişkileri bağlamında böyle bir sigorta sözleşmesi ilişkisi kurulabilse bile idarenin sorumluluğu açısından konu ele alındığında büyük çaplı sistemlerde gerçekleşen zararlarda, sigorta şirketlerinin milyonlarca insanın verisine ilişkin zararı karşılayabilmesi fiilen mümkün olamayabilir. Bunun yerine özellikle kişisel verilerin ihlalinden kaynaklanan dijital hizmet kusurlarında; zararlara ilişkin Devlet bünyesinde bir zarar fonu kurulması, idarelere verileri koruyamama nedeniyle para cezası uygulanabilmesinin mevzuat kapsamında mümkün kılınması, idarelere uygulanan cezaların bu zarar fonunda biriktirilmesi ve ilgililerin zararının bu fondan karşılanması önerilebilir.[155]

Sonuç

Teknolojik gelişmelerin ilerlemesi ile birlikte mevcut hukuki düzenlemelerin bunlara uygulanmakta yetersiz kalması aslında hukuk dilinin kullanımına da sirayet etmekte ve genel dil olarak ifade edilen ayrı bir otomasyon dili oluşturmaktadır.[156] Bu genel dil kamu hukuku ve özel hukuk fark etmeksizin her iki alana da uygulanmakta ve hukuk dilini zenginleştirmektedir.[157] Ancak mevzuatın bulunmaması ve dolayısıyla somut olaylara uygulanabilecek herhangi bir kavramın bulunmaması durumunda ne gibi bir yorum yapılabileceği ise belirsizliğini sürdürmektedir. İdare Hukuku'nun kendine özgü özelliklerinden esnek ve içtihadi bir hukuk dalı olması nedeniyle mevcut kavramların özelleştirilerek farklı durum ve olaylara uygulanması imkânı bulunmaktadır. Ancak mevcut kavramlardan ayrılan bu uygulamaların yine kendine özgü kelimelerle ifade edilmesi hem mevcut kavramın içeriğini değiştirmeyecek hem de bu kavramla bağını korumayı sürdürebilecektir. Bu doğrultuda hizmet kusuru teorisinden tamamıyla kopmadan, alanın kendine özgü özelliklerini de gözeterek idarenin dijital ortamdaki faaliyetlerinden meydana gelen kusurlu sorumluluğunu dijital hizmet kusuru olarak adlandırmayı önermekte ve bu alana özgülenmesini arzulamaktayız.

Elbette dijital hizmet kusurunun, hizmet kusurundan ayrı olarak isimlendirilmesinin bir sebebi olmalıdır. Aksi takdirde aynı kavramı farklı terimlerle ifade etmek hukuk dilini zenginleştiremeyeceği gibi kavram kargaşasına da yol açabilecektir. Bu

153 Bkz. 'Dijital Kolluk Faaliyeti' başlığı.

154 Gürpınar (n 72) 693.

155 Benzer yönde ancak fon kurulması önerisi hariç, idareye uygulanan cezaların doğrudan mağdurlara tazminat olarak dağıtılmasına ilişkin bkz. Lintvedt (n 94) 15.

156 Ida Koivisto, Riika Koulu and Stefan Larsson, 'User accounts: How technological concepts permeate public law through the EU's AI Act' (2024) 0(0) Maastricht Journal of European and Comparative Law 18 < https://doi.org/10.1177/1023263X241248469 > Erişim Tarihi 30 May 2024.

157 Koivisto, Koulu and Larsson (n 156) 18.

noktada çalışma kapsamında ortaya konulan temel gerekçe; dijital hizmet kusuru, idarenin mali sorumluluğunun şartları olan *idari bir davranış*, *zarar*, zarar ile davranış arasındaki *illiyet bağı* ve *kusurun* ele alınması açısından hizmet kusurundan farklılaşmalıdır.

Öncelikle *idari davranış*, hizmet kusuru ile dijital hizmet kusuru arasında 'ayrım yapmayı' sağlayacak ve bir belirleyici olarak rol alacaktır. Dijital hizmet kusurundan bahsedebilmek için idarenin dijital alanda gördüğü bir faaliyet olmalıdır. Çalışmamız kapsamında bu faaliyetler dijital kamu hizmetleri ve dijital kolluk faaliyetleri olarak belirtilmektedir.

Akabinde ise zarar, illiyet bağı ve kusur şartları, uyuşmazlıklarda yargı yerleri tarafından mevcut hizmet kusurundan ayrışarak farklı bir yöntemle değerlendirilmelidir.

Zarar, dijital varlıkların özelliklerine göre ele alınmalıdır. Özellikle kişisel veriler yönünden geleceğe yönelik tehlikeden kaynaklanan korku yargı yerleri tarafından manevi bir zarar olarak nitelendirilmelidir. Her ne kadar ilk bakışta bu korkunun kaynağı gelecekte yaşanacak bir olaya dayansa da yani 'potansiyel/muhtemel' nitelik arz etse de korku yaşanmaya başladığı için bu korku kesin ve gerçekleşmiş zarar kapsamında ele alınabilir ve dijital hizmet kusuru çerçevesinde tazmini mümkün kılınabilir. Ayrıca dijital ortamda gerçekleşen zararlar hesaplama yönünden de özellik arz edecektir. Bu nedenle örneğin siber saldırılardan kaynaklanan zararlarda, zararın hesaplanmasında belirsizlik yaratan durumların da tahmin yöntemiyle hesaplanabilmesine yarayan bilimsel hesaplama yöntemlerinden yararlanılabilir. Böylelikle sorumluluk şartı olan zararın, 'kesin ve gerçekleşmiş' olma niteliği dijital hizmet kusuru yönünden daha esnek ele alınmayı, yeri geldiğinde 'potansiyel/muhtemel' zararı da zarar olarak kabul etmeyi sağlayacaktır. Buna ek olarak dijital varlıkların gerçek değerinin belirlenmesinde rayiç belirleme modelinin kullanılması, kişisel verilere önceden belirlenmiş somut ve objektif düzenlemelerle fiyat biçilmesi veya buna yönelik ölçeklendirme metodu geliştirilmesi maddi yönden zararın belirlenmesine katkı sağlaması için önerilebilir.

İlliyet bağı açısından ise özellikle idarenin dijital ortamdaki faaliyetlerinden kaynaklanan zararlarda, bu zararın gerçekten de idarenin faaliyetinden kaynaklanıp kaynaklanmadığını kanıtlayabilmek davacı yönünden çok kolay sayılabilecek bir mesele değildir. Bu nedenle dijital hizmet kusurundan kaynaklanan uyuşmazlıklarda, özellikle dijital kamusal alanda gerçekleşen uyuşmazlıklarda, bu alanı sosyal risk ilkesinde olduğu gibi devletin egemenlik alanı kabul etmek suretiyle illiyet bağının daha esnek yorumlanması önerilebilir. İlliyet bağı ile ilgili bir diğer mesele ise özellikle siber saldırılarda üçüncü kişinin eylemi nedeniyle illiyet bağının kesildiğinin ileri sürülmesine imkân verilmemesi veya oldukça ihtiyatlı ele alınması önerilebilir.

Kusur açısından ise idarenin dijital ortamdaki faaliyetlerinden kaynaklanan uyuşmazlıklarda kusurun idarenin sisteminden kaynaklandığını ispat etmek davacı açısından oldukça güçtür. Özellikle dijital delillerin değişebilme, silinebilme özellikleri dikkate alındığında dijital hizmet kusuruna ilişkin uyuşmazlıklarda kusuru ispat külfeti tersine çevrilerek, idarenin ortaya çıkan zararın dijital ortamda görülen faaliyetin kuruluş ve işleyişinden kaynaklanmadığını kanıtlaması bir öneri olarak sunulabilir. Nitekim ilk bakışta bu menfi bir durumun ispatı gibi görünse de idare, sistem kayıtları ile bunun kendinden kaynaklanmadığını davacıya kıyasla çok daha kolay ispat edebilecektir.

Yeni bir kavram önerebilmek ve bunu temellendirebilmek kolay bir iş olmadığı gibi uygulama açısından benimsenmesini görebilmek de kolay beklenen bir sonuç değildir. Esasında bu çalışma idarenin sorumluluğuna yönelik özel ve farklı bir 'teori' geliştirmek amacıyla hazırlanmamıştır. Giriş bölümünde de belirtildiği üzere bu çalışma lex ferenda açısından dijital hizmet kusuru gibi idarenin dijital alandaki sorumluluğunu tanımlayacak ayrı bir kavrama ihtiyaç duyulduğuna ve mevcut sorumluluk şartlarının idarenin dijital ortamdaki faaliyetlerden kaynaklanan uyuşmazlıklar açısından yetersiz kaldığına dikkat çekmek için kaleme alınmıştır. Ancak bu çalışmanın bir karşılık bularak sonraki çalışmalarda eleştirilmesi ve kavramın zamanla gelişmesi neticesinde, dijital hizmet kusuru yahut bunun ötesinde idarenin dijital alandaki sorumluluğuna yönelik farklı ve yeni bir teori geliştirilmesi potansiyel dahilindedir. Çalışmada, mevcut hukuki temel olan hizmet kusurundan çok kopmadan ancak alanın kendine özgü niteliklerini de dikkate alarak idarenin dijital alandaki kusurlu davranışlarından kaynaklanan sorumluluğunun, sorumluluk şartları açısından daha farklı bir şekilde alınması gerekliliği ispatlanmaya çalışılmış ve buna istinaden bu sorumluluğun yeni bir kavramla ifade edilmesi ihtiyacına dikkat çekmek amaçlanmıştır. Ama bu önerideki gibi ama farklı bir şekilde olsun mevcut sistemin dijital ortama uygulanmasında yetersiz kalması, yakın bir gelecekte idarenin sanal ortamdaki faaliyetlerinden kaynaklanan zararlarda mevcut sorumluluk şartlarının bu ortamın özellikleri dikkate alınarak uyarlanmasını gerektirecektir.

Teşekkür: TÜBİTAK'a, University of Oslo ve NRCCL'e çalışma için sağladıkları imkanlardan dolayı teşekkür ederim. Çalışma hakkındaki görüşleriyle çalışmanın gelişmesine destek olan Mona Naomi Lintvedt, Lee Andrew Bygrave, Tobias Mahler, Dag Wiese Schartum'a ayrı ayrı teşekkür ederim.
Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.
Finansal Destek: Çalışma, TÜBİTAK 2214-A Yurtdışı Doktora Sırası Araştırma Burs Programı çerçevesinde University of Oslo, Faculty of Law, Norwegian Research Center Computers and Law (NRCCL) bünyesinde yürütülen araştırma esnasında toplanan kaynaklar ve sağlanan imkanlar ile desteklenmiştir.

Acknowledgments: I would like to thank TUBITAK, University of Oslo and NRCCL for the facilities provided for the study. I would like to thank Mona Naomi Lintvedt, Lee Andrew Bygrave, Tobias Mahler, Dag Wiese Schartum, Lee Andrew Bygrave, Tobias Mahler and Dag Wiese Schartum for their comments on the study.
Peer-review: Externally peer-reviewed.

Conflict of Interest: The author has no conflict of interest to declare.
Grant Support: The study was supported by the resources collected and facilities provided during the research conducted at the University of Oslo, Faculty of Law, Norwegian Research Center Computers and Law (NRCCL) within the framework of TUBITAK 2214-A Research Fellowship Programme.

Bibliyografya/Bibliography

Akyılmaz B, Sezginer M and Kaya C, *Açıklamalı-İçtihatlı Türk İdari Yargılama Hukuku* (Savaş 2019).

Akyılmaz B, Sezginer M and Kaya C, *Türk İdare Hukuku* (17th edn, Seçkin 2023).

Altındağ H, 'Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu' (2019) 18(2) İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi 387-401.

Atay EE, *İdari Yargılama Hukuku* (Seçkin 2021).

Atay EE and Odabaşı H, *Teori ve Yargı Kararları Işığında İdarenin Sorumluluğu ve Tazminat Davaları* (2nd edn, Seçkin 2010).

Başar C, *Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması* (On İki Levha 2020).

Beck C, Boumezoued A, Cherkaoui Y, Pradat E and Fleisher B, ' Modelling Financial Losses From a Ransomware Attack Using a Casual Approach' (Milliman, 2023) < https://www.milliman.com/-/media/milliman/pdfs/2023-articles/10-13-23_modeling-financial-losses-from-a-ransomware-attack.ashx > Erişim Tarihi: 15.10.2024.

British Broadcasting Corporation (BBC), '108 milyon kişinin verileri çalındı iddiası: Bakanlık ne açıkladı, tepkiler ne oldu?' (BBC, 12 September 2024) < https://www.bbc.com/turkce/articles/cn8789ez2q7o > Erişim Tarihi 02 October 2024.

Bhavsar V, Kadlak A and Sharma S, 'Study on Phishing Attacks' (2018) 183(33) International Journal of Computer Applications < https://www.ijcaonline.org/archives/volume182/number33/ > Erişim Tarihi 27 May 2024.

Bing J and Mahler T, 'Contractual Risk Management in an ICT Context - Searching for a Possible Interface between Legal Methods and Risk Analysis' (2006) 49 Scandinavian studies in law 339-358.

Bygrave LA, 'Cyber Resilience versus Cybersecurity as Legal Aspiration' in T. Jančárková, G. Visky, I. Winther (eds), *2022 14th International Conferance on Cyber Conflict: Keep Moving! (CyCon)* (NATO CCDCOE 2022) 27-43.

Christensen S, Caelli WJ, Duncan WD and Georgiades E, 'An Achilles heel: denial of service attacks on Australian critical information infrastructures' (2010) 19(1) Information & Communications Technology Law 64 < https://doi.org/10.1080/13600831003708059 > Erişim Tarihi 17.06.2024.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 'e-Devlet Kapısı Kullanıcı Hesaplarının Sızdırıldığı İddiaları Hakkında Basın Açıklaması' (CBDDO, 26 February 2023) < https://cbddo.gov.tr/duyurular/6627/-e-devlet-kapisi-kullanici-hesaplarinin-sizdirildigi-iddialari-hakkinda-basin-aciklamasi- > Erişim Tarihi 27 May 2024.

Çağlayan R, *İdarî Yargılama Hukuku* (10th edn, Seçkin 2018).

Çaptuğ M, 'Covid-19 Salgınının Kamu Hizmetlerinin Dijitalleşmesi Sürecine Etkisi ve Sonuçları' (2021) 23(2) Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 1309-1327.

Çınar İ, '5651 sayılı Kanun Çerçevesinde Koruma Tedbiri Olarak İnternet Ortamında Yapılan Yayınlarda İçeriğin Çıkarılması ve/veya Erişimin Engellenmesi' (2021) 8(1) İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 63-95.

Demir Bayram S, *Kamu Hizmetinde Dijital Dönüşüm ve E-İhale Süreci* (On İki Levha 2023).

Demiral U, *Bir Koruma Tedbiri Olarak Şirket Yönetimi İçin Kayyım Tayini (CMK m. 133)* (Seçkin 2021).

Dolma E, 'Uzmanlar yanıtladı: 10 soruda e-Devlet'ten veri sızıntısı' (Oksijen, 18 June 2023) < https://gazeteoksijen.com/turkiye/uzmanlar-yanitladi-10-soruda-e-devletten-veri-sizintisi-181501 > Erişim Tarihi 27 May 2024.

Duran L, 'İdari İşlemden Sorumluluk: İptal – Tam Yargı Davası' (1967) 33(3-4) İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 3-26 < https://dergipark.org.tr/tr/download/article-file/96216 > Erişim Tarihi: 09.10.2024.

Duran L, *Türkiye İdaresinin Sorumluluğu: Sorumluluğun Temeli ve Sebepleri, Sorumluluğa Yol Açan Olgular* (TODAİE 1974).

ENISA, *Public Private Partnerships (PPP): Cooperative models* (ENISA 2017).

Erdoğmuş T, 'Kişisel Verileri İhlal Eden İdareye Karşı İdari Para Cezası Uygulanamaması Sorunu', (2023) 10(1) İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 137-168.

Eren F, *Borçlar Hukuku Genel Hükümler* (25th edn, Yetkin 2020).

Erkal A, 'Kişisel Verilerin Önleyici ve Koruyucu Faaliyetler Kapsamında Otomatik Araçlarla Veri Analizi/Değerlendirilmesi Suretiyle İşlenmesi ve Alman Federal Anayasa Mahkemesi Yaklaşımı' Cemil Kaya (ed) *Kişisel Verilerin Korunması Hukuku ve Bilgi Edinme Hukuku: Çeşitli Açılardan Bakış* (On İki Levha 2023) 23-77.

Eroğlu Durkal M, 'Tam Yargı Davalarında Manevi Tazminat' (2017) 131 Türkiye Barolar Birliği Dergisi 179-210.

Erol ÖF, *Algoritmik Regülasyon: Yapay Zekâ ve İdarenin Regülasyon Faaliyeti* (On İki Levha 2023).

Gözler K, *İdare Hukuku Cilt 2* (3rd edn, Ekin 2019).

Gözübüyük AŞ and Tan T, *İdare Hukuku Cilt II: İdari Yargılama Hukuku* (8th edn, Turhan 2016).

Güçlütürk OG, 'Blokzincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinemezlik, Yok Edilemezlik Sorunu' (2019) 1(2) Kişisel Verileri Koruma Dergisi 30-40.

Gülan A, *İdare Hukuku Ders Notları* (İstanbul Üniversitesi Hukuk Fakültesi) < https://cdn.istanbul.edu.tr/FileHandler2.ashx?f=2015-2016-idare-hukuku-ders-notlari-teskilat-haric.pdf > Erişim Tarihi 20 May 2024.

Gülan A, 'Kamu Hizmeti Kavramı' (1988) 9(1-3) İdare Hukuku ve İlimleri Dergisi 147-159.

Günday M, *İdare Hukuku* (11th edn, İmaj 2017).

Gür NT, *İdarenin Özendirme ve Destekleme Faaliyeti* (On İki Levha 2019).

Gürpınar D, 'Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk' (2017) 18(2) Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi (Prof. Dr. Şeref Ertaş'a Armağan) 679-694.

Janeček V and Teixeira Santos C, 'The autonomous concept of "damage" according to the GDPR and its unfortunate implications: Österreichische Post' (2024) 61(2) Common Market Law Review 531-543 < https://doi.org/10.54648/cola2024031 > Erişim Tarihi 17.06.2024.

Kağıtçıoğlu M, 'Yapay Zekâ ve İdare Hukuku (Bugünden Geleceğe Yönelik Bir Değerlendirme)' (2021) 11(1) Hacettepe Üniversitesi Hukuk Fakültesi Dergisi 118-168.

Kalabalık H, *İdare Hukuku Dersleri Cilt: II* (6th edn, Seçkin 2024).

Kaplan G, *İdari Yargılama Hukuku* (7th edn, Ekin 2020).

Karakoyunlu Y, 'Türkiye'de e-Devlet Forumu Açılış Konuşması' (Hürriyet, Bilişim Zirvesi 2001).

Kaya MB, *Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi* (On İki Levha 2010).

Kaya MB, 'Türkiye'de İnternete Kim, Neden ve Nasıl Müdahale Ediyor?' (İnternet-Hukuk-Yetki-Kontrol, 25 August 2024) < https://mbkaya.com/internet-hukuk-yetki-kontrol/ > Erişim Tarihi: 08.10.2024.

Kaya T, *İnternet Servis Sağlayıcısının Hukuki ve Cezai Sorumluluğu* (Seçkin 2019)

Koivisto I, Koulu R and Larsson S, 'User accounts: How technological concepts permeate public law through the EU's AI Act' (2024) 0(0) Maastricht Journal of European and Comparative Law 1-21 < https://doi.org/10.1177/1023263X241248469 > Erişim Tarihi 30.05.2024.

Krimmer R, Kalvet T, Toots M, Cepilovs A and Tambouris E, 'Exploring and Demonstrating the Once-Only Principle: A European Perspective' (2017) dg.o '17: 18th Annual International Conference on Digital Government Research 546-551 < http://dx.doi.org/10.1145/3085228.3085235 > Erişim Tarihi 29 May 2024.

Küçük ÇM, 'Yapay Zekâ Tarafından Gerçekleştirilen İdari İşlemde Sorumluluk' (2024) 10(1) Başkent Üniversitesi Hukuk Fakültesi Dergisi 169-215.

Lee L, 'Examining the Legal Status of Digital Assets as Property: A Comparative Analysis of Jurisdictional Approaches' (2024) SSRN 1-16 < http://dx.doi.org/10.2139/ssrn.4807135 > Erişim Tarihi: 03.10.2024.

Lintvedt MN, 'Putting a price on data protection infringement' (2022) 12(1) International Data Privacy Law 1-15.

Mahler T, 'Tool-Supported Legal Risk Management: A Roadmap' (2010) 2(3) European Journal of Legal Studies 146-167.

Mecek M, 'E-Devlet ve E-Belediye: Kavramsal Çerçeve ve Türkiye'de Belediye Web Sitelerine Yönelik Yapılan Çalışmaların İncelenmesi' (2017) 22(15) SDÜİİBFD (Kayfor15 Özel Sayısı) 1815-1851.

Milakovich ME, *Digital Governance* (2nd edn, Routledge 2021).

Mozur P, 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority' (New York Times, 14 April 2019) <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> Erişim Tarihi 23 May 2024.

National Institute of Standards and Technology, 'Guide for Conducting Risk Assessments-Information Security' (2012) Rev. 1 800-30 NIST Special Publication Appendix-B < https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf > Erişim Tarihi: 08.10.2024.

Nebil FS, 'Depremde bant daraltma yapan BTK nedenini açıklasın' (*T24,* 21 March 2024) <https://t24.com.tr/yazarlar/fusun-sarp-nebil/depremde-bant-daraltma-yapan-btk-nedenini-aciklasin,44048#:~:text=%226.02.2023%20depreminin%20hemen%20sonras%C4%B1nda,tarihinde%20bant%20daraltma%20uygulamas%C4%B1na%20gidilmi%C5%9Ftir. > Erişim Tarihi 31 May 2024.

International Organization for Standardization (ISO), *Information security, cybersecurity and privacy protection — Information security management systems – Requirements* (ISO No. ISO/IEC 27001:2022) (2022) < https://www.iso.org/standard/27001 > Erişim Tarihi 20.06.2024.

Oğurlu Y, *İdare Hukukunda "e-Devlet" Dönüşümü ve Dijitalleşen Kamu Hizmeti* (On İki Levha 2010).

Onar SS, *İdare Hukukunun Umumî Esasları III. Cilt* (3rd edn, Hak 1966).

Ozansoy C, *Tarihsel ve Kuramsal Açıdan İdarenin Kusurdan Doğan Sorumluluğu* (Yayınlanmamış Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü 1989).

Önüt LB, *İdari Yargılama Hukukunda Adil Yargılanma İlkesi Çerçevesinde Grup Dava Uygulaması* (Seçkin 2018).

Özay İH, *Günışığında Yönetim II: Yargısal Korunma* (On İki Levha 2010).

Palas Dağlı E, *Kamu-Özel İşbirliği Modeli ve İdarenin Sorumluluğu (Sağlık Hizmetlerinde)* (Seçkin 2024).

Peilemeier J and Sullivan D, 'Unpacking "Systemic Risk" Under the EU's Digital Service Act' (Tech Policy, 19 July 2023) < https://www.techpolicy.press/unpacking-systemic-risk-under-the-eus-digital-service-act/ > Erişim Tarihi: 15.10.2024.

Prince II WN, Gerke S and Cohen IG, 'Potential Liability for Physicians Using Artificial Intelligence' (2019) 322(18) Journal of the American Medical Association 1765-1766 < https://jamanetwork.com/journals/jama/article-abstract/2752750 > Erişim Tarihi: 15.10.2024.

Romanosky S and Goldman Z, 'Understanding Cyber Collateral Damage' (2017) 9(2) Journal of National Security Law&Policy 233-257.

Sancakdar O, 'İdare Hukukuna Özgü Tazmin Nedenlerinin Bulunmaması Kavramı' (1999) Manisa Barosu Dergisi 20-31.

Sancakdar O, Önüt LB, Us Doğan E, Kasapoğlu Turhan M and Seyhan S, *İdare Hukuku Teorik Çalışma Kitabı* (11th edn, Seçkin 2022).

Sarıca M, 'Was Turkey's e-Government Hacked?' (Hack 4 Career, 21 June 2023) < https://www.mertsarica.com/was-turkeys-e-government-hacked/ > Erişim Tarihi 27 May 2024.

Sarıca R, 'Hizmet Kusuru ve Karakterleri' (1949) 15(4) İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 858-895.

Sarsıkoğlu Ş, 'İdarenin Mali Sorumluluğu Açısından Zarar Kavramı' (2016) 65(4) Ankara Üniversitesi Hukuk Fakültesi Dergisi 2389-2422.

Schartum DW, 'Law and alghorithms in the public domain' (2016) 1(0) Etikk i praksis 15-26.

Seskir Z, 'Hacklenmemek Elimizde mi?' (Medium, 18 October 2017) < https://medium.com/duzensiz/hacklenmemek-elimizde-mi-79bcefc08fbc > Erişim Tarihi 25 May 2024.

Seyhan S, *Yapay Zekâ Teknolojileri Kapsamında İdarenin Sorumluluğu* (On İki Levha 2023).

Smith GS and Amoruso AJ, 'Using real options to value losses from cyber attacks' (2006) 2(3-4) Journal of Digital Asset Management 151 < https://doi.org/10.1057/palgrave.dam.3650033 > Erişim Tarihi 01.06.2024.

Strupczewski G, 'Defining Cyber Risk' (2021) 135 Safety Science 1-10 < https://doi.org/10.1016/j.ssci.2020.105143 > Erişim Tarihi 15.10.2024.

Tan T, *İdare Hukuku* (9th edn, Turhan 2020).

Taştan M, *Koruma Tedbirleri Nedeniyle Tazminat Davaları* (Adalet 2019).

T.C. Kalkınma Bakanlığı, *On Birinci Kalkınma Planı (2019-2023) e-Devlet Hizmetlerinin Geliştirilmesi Çalışma Grubu Raporu* (T.C. Kalkınma Bakanlığı 2018) 23 < https://www.sbb.gov.tr/wp-content/uploads/2020/04/e-DevletCalismaGrubuRaporu.pdf > Erişim Tarihi 02.10.2024.

T.C. Ulaştırma ve Altyapı Bakanlığı, *2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı* (*Faaliyetler-Siber Güvenlik*, 2020) < https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf > Erişim Tarihi 29 May 2024.

T.C. Ulaştırma ve Altyapı Bakanlığı, *2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı* (UAB 2024) 27 < https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf > Erişim Tarihi: 08.10.2024.

The Federal Council of Switzerland, 'Digital public services' (*Federal Department of Finance-Digital Public Services Switzerland,* 26 February 2024) < https://www.efd.admin.ch/efd/en/home/digitalisation/digital-public-services.html > Erişim Tarihi 29 May 2024.

The Norwegian Digitalisation Agency (Digdir), 'How to obtain an electronic ID', (ID-porten) < https://eid.difi.no/en/id-porten/how-obtain-electronic-id > Erişim Tarihi: 18.06.2024.

Türk Mühendis ve Mimar Odaları Birliği Bilgisayar Mühendisleri Odası, *6 Şubat 2023 Kahramanmaraş Depremleri Raporu* (BMO, 6 August 2023) 4 < https://www.bmo.org.tr/wp-content/uploads/2023/10/BMO-Deprem-Raporu.pdf > Erişim Tarihi 02.10.2024.

Türk Standardları Enstitüsü, 'TS ISO/IEC 27001:2022 Standardı İçin Geçiş Şartları' (TSE, 16.02.2023) < https://www.tse.org.tr/duyuru/ts-iso-iec-270012022-standardi-icin-gecis-sartlari/?asp_highlight=siber+g%C3%BCvenlik&p_asid=1 > Erişim Tarihi 10.10.2024.

Ulusoy A, *Yeni Türk İdare Hukuku* (Yetkin 2019).

Walden I, *Computer Crimes and Digital Investigations* (2nd edn, Oxford 2016).

Webteknohaber, 'Sadece Telefon Numarasıyla Türkiye'deki Herkesin Tüm Kişisel Bilgilerini Gösteren Bir İnternet Sitesi Ortaya Çıktı' (WebTekno, 09 June 2023) < https://www.webtekno.com/turkiye-herkesin-kisisel-bilgilerini-gosteren-internet-sitesi-h135098.html > Erişim Tarihi 02 October 2024.

Wirth C and Kolain M, 'Privacy by BlockChain Design: A BlockChain-enabled GDPR-compliant Approach for Handling Personal Data' (2018) Proceedings of 1st ERCIM Blockchain Workshop 2018 < https://doi.org/10.18420/blockchain2018_03 > Erişim Tarihi 30 May 2024.

Yakar U, 'Facebook, Yemeksepeti, LinkedIn ve Clubhouse'dan Çalınan Bilgileriniz ile Neler Yapılabilir?' (WebTekno, 17 April 2021) < https://www.webtekno.com/facebook-calinan-bilgileriniz-ile-neler-yapilabilir-h108701.html > Erişim Tarihi 02 October 2024.

Yayla A, *İdare Hukuku Bakımından Yapay Zeka* (Seçkin 2023).

Yayla A, *İdarenin Kusursuz Sorumluluğu* (On İki Levha 2015).

Yerebasmaz Y, *Yargı Kararları Işığında Hizmet Kusuru Kişisel Kusur Ayrımı* (Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü 2012).

Yıldırım R and Çınarlı S, *Türk İdare Hukuku Dersleri Cilt: II* (Astana 2019).

Yıldırım T, Yasin M, Kaman N, Özdemir HE, Üstün G and Okay Tekinsoy Ö, *İdare Hukuku* (7th edn, On İki Levha 2018).

Zanfir-Fortuna G, 'Article 82. Right to compensation and liability' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford 2020) 1160-1179.