Geliş Tarihi:
13.12.2023
Kabul Tarihi:
29.03.2023
Yayımlanma Tarihi:
30.12.2023

Kaynakça Gösterimi: Yürük, Z. (2023). Veri sorumlusunun veri güvenliğine ilişkin idari ve teknik tedbirleri alma yükümlülüğü. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, *22*(48), 899-920. doi: 10.46928/iticusbe.1218693

VERİ SORUMLUSUNUN VERİ GÜVENLİĞİNE İLİŞKİN İDARİ VE TEKNİK TEDBİRLERİ ALMA YÜKÜMLÜLÜĞÜ

Derleme

Zehra Yürük
Sorumlu Yazar (Correspondence)
İstanbul Ticaret Üniversitesi
zehra.sen@istanbulticaret.edu.tr

Zehra YÜRÜK, Özel Hukuk alt bilim dalları ve Ceza Hukuku alanlarında Avukat olarak çalışmaktadır. Kişisel Verilerin Korunması Hukuku alanında lisansüstü çalışmalarına devam etmektedir.

VERİ SORUMLUSUNUN VERİ GÜVENLİĞİNE İLİŞKİN İDARİ VE TEKNİK TEDBİRLERİ ALMA YÜKÜMLÜLÜĞÜ

Zehra Yürük
zehra.sen@istanbulticaret.edu.tr

Özet

Teknolojik gelişmeler, hayatımızı kolaylaştıran birçok yenilik getirmekle birlikte yapay zekâ teknolojilerinin kullanıldığı uygulamalar ile bireylere ait verilerin toplanmasını ve bu verilerin birleşimi ile kişilerin özel ve sosyal hayatlarına ilişkin çıkarımlar üretilmesini sağlamaktadır. Bu çıkarımların oluşturulmasına kadar geçen süreç içerisinde toplanan, işlenen, aktarılan ve saklanan bu verilerin güvenliğinin sağlanamaması ise, ciddi hukuki sorunlara sebep olabilmektedir. Kişisel verilerin güvenliğinin sağlanabilmesi için 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile veri sorumlusu ve veri işleyenlere bazı yükümlülükler getirilmiştir. Bu yükümlülüklerin getirilmesinin temel sebebi, ilgili kişilerin mahremiyetlerinin korunması ve veri işleme faaliyetinin hukuka uygun olarak yerine getirilmesinin sağlanmasıdır. Bu kapsamda, ilgili kişinin hak kaybına uğramasının engellenmesi için KVKK ile veri sorumlularına getirilen gerekli idari ve teknik tedbirleri alma yükümlülüğü incelenmiştir.

Amaç: Bu çalışmada, kişisel verilerin korunması için veri sorumlusuna getirilen teknik ve idari tedbirleri alma yükümlüğü kapsamında yapılması gereken faaliyetler ve veri ihlallerinin engellenmesine ilişkin genel çözümler üretilmesi amaçlanmıştır.

Metodoloji: Araştırma yazılı kaynakların ve veri tabanlarının taranması ile hazırlanmıştır.

Bulgular: Kişisel verilerin korunması, bireyin mahremiyetinin ve temel haklarının da korunmasını sağlamaktadır. Bu sebeple veri dolaşımı etkilenmeden kişisel verilerin hukuka uygun olarak işlenmesi, hukuka aykırı erişimin önlenmesi ve bu süreçte verilerin muhafazasının sağlanması büyük önem arz etmektedir. Nitekim veri sorumlularına getirilmiş olan yükümlülükler kapsamında veri güvenliğine ilişkin risk ve tehditlerin azaltılması mümkün olsa da ihlallerin tamamen engellenmesini sağlamak mümkün değildir.

Özgünlük: Kişisel verilerin korunmasına ilişkin yayımlanmış eserler ve yapılan çalışmalar değerlendirilerek kişilerin mahremiyetinin korunmasının önemi, veri güvenliği sorunu ve alınabilecek tedbirleri inceleyen çalışma özgün niteliktedir.

Anahtar Kelimeler: Veri, Kişisel Veri, Kişisel Veri Güvenliği, Teknik ve İdari Tedbirler.

JEL Sınıflandırması: K29

LIABILITY OF THE DATA CONTROLLER TO TAKE ADMINISTRATIVE AND TECHNICAL MEASURES REGARDİNG DATA SECURITY

Abstract

Technological developments bring many innovations that make our lives easier, as well as the collection of data belonging to individuals with applications using artificial intelligence technologies and the production of inferences about the private and social lives of individuals with the combination of these data. Failure to ensure the security of these data, which is collected, processed, transferred and stored until the formation of these inferences, may cause serious legal problems. In order to ensure the security of personal data, some obligations have been imposed on data controllers and data processors with the Law on the Protection of Personal Data No. 6698. The main reason for these obligations is to protect the privacy of the data subjects and to ensure that the data processing activities are carried out in accordance with the law. In this context, the obligation to take the necessary administrative and technical measures brought to data controllers by KVKK in order to prevent the person concerned from losing their rights has been examined.

Purpose: In this study, the aim is to determine the activities to be done within the scope of the obligation to take technical and administrative measures brought to the data controller for the protection of personal data and to produce general solutions for preventing data breaches.

Method: The research was prepared by scanning written sources and databases.

Findings: The protection of personal data also ensures the protection of the privacy and fundamental rights of the individual. For this reason, it is of great importance to process personal data by the law without affecting the data circulation, to prevent unlawful access and to protect the data in this process. As a matter of fact, although it is possible to reduce risks and threats to data security within the scope of obligations imposed on data controllers, it is not possible to completely prevent violations.

Originality: This is an original study that examines the importance of protecting the privacy of individuals, the problem of data security, the measures that can be taken by evaluating the published works and studies on the protection of personal data.

Keywords: Data, Personal Data, Personal Data Security, Technical and Administrative Measures.

JEL Classification: K29

GİRİŞ

Her bireyin, günlük hayatı içerisinde sürekli oluşturduğu ve bilinçsizse çevresine yaydığı farklı türde birçok verisi bulunmaktadır. Bu veriler tek başına bir anlam ifade etmese de birleşimleriyle elde edilen bilgiler neticesinde, kişilerin hayatına ilişkin önemli detaylar ortaya çıkabilmektedir. Kişilerin yaşam tarzına, sosyal ve ekonomik hayatına, mensup olduğu dine, geçirdiği hastalıklara veya aile hayatına ilişkin bu bilgilerin, depo edildiği kişiler tarafından muhafaza edilmesi gerekmektedir.

Günümüz teknolojisinin yakıtı olan verileri elinde bulunduran kişi, ticari pazarda güçlü hale gelmektedir. Bu sebeple devletler ve özel sektör, rekabet için oldukça önemli olan verileri toplamak ve hedef kitleyi etkilemek için bu güce sahip olmak isterler. Zira bu sayede sundukları hizmetin kalitesini arttırabilir, seçimlere yön verebilir, bilgileri tehdit ve şantaj amaçlı kullanabilir veya satarak ticari kazanç elde edebilirler. Bu durum, kişilerin mahremiyetlerinin ihlali ile birlikte farklı birçok soruna da sebep olmaktadır.

Veri ihlallerinin engellenmesi ve yeni yaşam stillerinin de devam etmesi için gerekli olan veri akışının sağlanabilmesi adına, veri sorumlularına belirli yükümlülükler getirilmiştir. Bu sebeple veri sorumlularının, bilgileri hukuka aykırı olarak işlememesi ve bu bilgilere erişimi sınırlandırarak veya önleyerek iç ve dış tehditlere karşı koruması gerekmektedir.

I. VERİNİN TANIMI VE VERİ GÜVENLİĞİNİN SAĞLANMASI

A. Veri Nedir?

Veri, Latince "datum" olarak ifade edilen, İngilizce "data" sözcüğünden dilimize çevrilmiş ve orijinal karşılığı "verilen veya verilmiş şeyler" anlamına gelen bir kavramdır. Dilimizde de "verilen şey" veya "bir şey" olarak kullanılan verinin, sözlükte bilişim hukuku açısından "*olgu, kavram veya komutların, iletişim, yorumlama ve işlem yapmaya elverişli şekilde gösterimi*" olarak tanımlandığı görülmektedir (Türk Dil Kurumu (TDK), 2022). Bu doğrultuda veri kavramı; çeşitli harf, rakam, işaret ve sembollerle temsil edilebilen, birbiriyle bağlantısı henüz kurulmamış ve işlemeye hazır şekilde bulunan sinyal veya bit dizeleri olarak ifade edilebilir (Aksoy, 2010, s. 11, dn. 2; Canbek ve Sağıroğlu, 2006, s. 166).

Günümüzde veri ve bilgi kavramları, aynı anlamda kullanılmakla birlikte, bu kavramların eş anlamlı olmadığı yönünde eleştiriler mevcuttur. Esasen bilgi, temel hammaddesi olan verilerin, anlamlı bir biçime getirilerek işlenmesi sonucunda elde edilmektedir (Aksoy, 2010, s. 11; Dülger, 2020, s. 153). Dolayısıyla bağımsız değişkenlerden oluşan verinin, tek başına bir anlamı ve işlevi bulunmamaktadır. Verinin, bilgiden daha geniş bir kapsama sahip olduğu, ancak sadece anlamlı hale getirilen verilerin bir bilgi olarak kabul edilebileceği söylenebilir.

B. Kişisel Veri Nedir?

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) m. 3/1-d bendinde kişisel veri: *"Kimliği belirli veya belirlenebilir gerçek bir kişiye ilişkin her türlü bilgi"* olarak tanımlanmıştır. Kişisel verilere ilişkin bu tanım, birçok uluslararası metinde de benzer şekilde yer almaktadır. Tüzel kişilerin kapsam dışında bırakılmasının sebebi ise, veri güvenliğinin, kişinin temel ve hak özgürlüklerinin korunması ile sağlanmasıdır (Ayözger Öngün, 2019, s. 5).

Bu çerçevede gerçek bir kişinin adı, soyadı gibi bilgilerinin dışında; fotoğrafı, aile verileri, telefon numarası, sağlık verileri, etnik kökeni, sosyal ve ekonomik faaliyetleri, siyasi düşüncesi, inançları gibi kim olduğunun doğrudan veya dolaylı olarak belirlenmesini sağlayan her türlü verisi, kişisel veri olarak kabul edilmektedir. (Küzeci, 2019, s. 9; Başalp, 2004, s. 22; Çekin, 2019, s. 34; Beytar, 2018, s. 48; Anayasa Mahkemesi'nin, 12.11.2015 tarih ve E. 2015/32, K. 2015/102 sayılı kararı, s. 2, par. 9). Bu bilgilerin doğru veya yanlış olması da önem arz etmemektedir. Bir kişiyi belirli veya belirlenebilir kılan yanlış bilgi de kişisel veridir (Beytar, 2018, s. 51; Dülger, 2020, s. 156). Bu kapsamda, "kişisel veri" kavramına ilişkin sınırlı sayma ilkesi benimsenmeyerek genel bir tanım tercih edilmiştir. Böylece teknolojik gelişmeler ile ortaya çıkabilecek yeni veri kategorilerinin de korunması amaçlanmıştır.

Diğer taraftan bu kavramın sınırlarının tamamen belirsiz bırakılması halinde korunmasının da mümkün olmayacağı düşüncesiyle doktrin ve yargı içtihatları çerçevesinde, kişisel veri kavramına ilişkin dört temel unsur belirlendiği söylenebilir (Develioğlu, 2017, s. 30; Dülger, 2020, s. 152). Bunlar:

- Bir bilginin bulunması,
- Bilginin kişiyi belirli veya belirlenebilir kılması,
- Bilginin kişi ile ilişkili olması,
- Gerçek kişiye ait olması.

Ulusal ve uluslararası mevzuatta kişisel veriler, genel ve özel nitelikli (hassas) veri olarak ikiye ayrılmaktadır (Kaya, 2011, s. 317). Hassas kişisel verilerin ihlali, ilgili kişinin, ağır nitelikte zarar görmesine ve mağduriyete uğramasına sebep olabilmektedir. Bu nedenle hassas kişisel verilerin daha yüksek bir koruma altına alınması gerektiği kabul edilmektedir (Aksoy, 2010, s. 30; Dülger, 2020, s. 176). Bu doğrultuda kişisel veri güvenliğinin sağlanabilmesi için; kişisel verinin ne olduğunun, sınırlarının ve çeşidinin belirlenmesi, verilerin güvenli şekilde tutulması ve işlenmesi gerekmektedir.

C. Veri Güvenliği Nedir?

Veri güvenliği kavramı, "veriyi; ürünler, kişiler ve prosedürler aracılığıyla depolayan, işleyen ve ileten cihazlarda bilgilerin bütünlüğünü, gizliliğini ve kullanılabilirliğini koruma" şeklinde tanımlanmaktadır (Civan Kemiksiz, 2022, s. 73). Bu verilerin; izinsiz ya da yetkisiz kullanımı, hasar

verilerek bozulması, kazara yok edilmesi, ifşa edilmesi vb. zararlara uğraması hali ise, güvenlik zafiyeti olarak kabul edilmektedir (Civan Kemiksiz, 2022, s. 73; Develioğlu, 2017, s. 107).

Bu çerçevede teknolojik gelişmeler ile birlikte artan veri yığınlarının; CD, hard disk vb. fiziki ortamlar yerine, bulut bilişim sistemlerinde depolanmaya başlanması, uzaktan çalışmanın ve sosyal medya kullanımının yaygınlaşması gibi veri güvenliğinin sağlanmasını zorlaştıran koşullar, ciddi tehditler oluşturmaktadır (Korucu, 2021, s. 16). Kişisel veriler, aynı zaman dilimi içerisinde farklı fonksiyonlara sahip birçok uygulama tarafından; saklamak, kaydetmek ve paylaşmak gibi amaçlarla işlenmektedir. Bu sebeple veri sorumlusu, kişisel verilerin elde edildiği ilk andan itibaren her aşamada gerekli teknik ve idari önlemleri alarak veri güvenliğini ve gizliliğini sağlamakla yükümlüdür (Ayözger Öngün, 2019, s. 45 vd.; Dülger, 2020, s. 537; Zor, 2020, s. 91). Birçok düzenlemede yer alan bu yükümlülük, veri güvenliği ilkesi olarak kabul edilmektedir (Akdağ, 2015, s. 42; Gürbüz Erel, 2021, s. 119).

Kişisel verilerin korunması ile veri güvenliği birbirinden farklı kavramlardır (Küzeci, 2019, s. 253; Gündüz, 2022, s. 28; Çekin, 2019, s. 104). Kişisel verilerin korunmasında bireyin hak ve özgürlüklerinin korunması amaçlanır iken veri güvenliğinde korunan, bizzat verinin kendisidir (Akdağ, 2015, s. 29; Beytar, 2018, s. 213). Bu doğrultuda verinin güvenliğinin sağlanması, ilgili kişinin kişisel verilerinin korunmasına da hizmet etmektedir.

Veri güvenliğinin nasıl sağlanması gerektiğine ilişkin tüm teknolojiler için geçerli bir düzenleme olması mümkün değilse de genel kabul gören bazı kriterler bulunmaktadır (Dülger, 2020, s. 305-306; Gündüz, 2022, s. 30; Develioğlu, 2017, s. 50; Zor, 2020, s. 81-82; Korucu, 2021, s. 18-20). Bunlar aşağıdaki şekilde sayılabilir:

1- Bilginin yetkisiz ve kötü niyetli kişilerin eline geçmesini engellemeyi amaçlayan gizlilik kriteri (GDPR m. 5/1-f),
2- Verinin bozulmasını, silinmesini veya değiştirilmesini engellemeyi ve verinin doğruluğunun korunmasını sağlamayı amaçlayan veri bütünlüğü kriteri (GDPR m. 5/1-f),
3- Verinin işlendiği sistemlerin kesintisiz olarak çalışmasını, bilginin her an tam ve eksiksiz olarak ulaşılabilir ve kullanılabilir şekilde bulunmasını amaçlayan erişilebilirlik kriteri,
4- Veri sahibinin veya verilerin, kayıt altına alındığı mekanizmaları kullanmaya yetkili kişinin kimliğinin, doğru olup olmadığını kontrol etmeyi hedefleyen kimlik doğrulama kriteri,
5- Kullanılan sistemin, eksiksiz ve tutarlı şekilde çalışmasını amaçlayan güvenilirlik kriteri.

Veri güvenliğinin sağlanmasına yönelik olarak benimsenen bu ilkeler doğrultusunda, teknolojik ve kurumsal önlemler alınması, iç ve dış tehditlere karşı kişisel verilerin korunması gerekmektedir.

Bununla birlikte veri sorumlusunun kasıtlı bir eylemi bulunmasa dahi bazı *"sistemsel ve/veya yöntemsel hatalar"* sebebiyle maddi ve manevi zararlar meydana gelebilmektedir. Bu zararların, sonradan alınan önlemler ile engellenmesi ise mümkün değildir. Bu sebeple bu alandaki en güncel

düzenleme olan 2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) m. 25'te düzenlenen *"tasarlanmış ve önceden tanımlanmış veri koruma (data protection by design and by default)"* kuralının, hukukumuz açısından da kabul edilmesi gerektiği belirtilmektedir (Develioğlu, 2017, s. 101-102, 205; Çekin, 2016, s. 642). Zira *"tasarlanmış ve önceden tanımlanmış veri koruma"* kuralı ile verilerin; hukukî, teknik ve organizasyonel açıdan henüz tasarlama/gelişim aşamasında iken veri işleme ilkeleri ve şartları da göz önünde bulundurularak işleme faaliyetlerine dahil edilmesi ve böylece korunmasının sağlanması hedeflenmektedir. Buna, kişisel verilere erişim yetkisi olacak kişilerin önceden belirlenmesi örnek olarak verilebilir.

Nitekim Kişisel Verileri Koruma Kurulu; 26.07.2018 Tarihli ve 2018/91 Sayılı Kararı ile alışveriş işlemleri için girilen kişisel verilerin, sistemden kaynaklanan bir hata sebebiyle diğer müşterilerin alışveriş işlemleri esnasında görülebilir hale gelmesini, veri sorumlusunun *"kişisel verilerin muhafaza edilmesi ve kişisel verilere hukuka aykırı erişilmesini önleme amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri alma"* yükümlülüğünün ihlali olarak değerlendirmiş ve idari para cezası uygulanmasına karar vermiştir. Bu doğrultuda GDPR ile uyum sağlayan Kurul kararları da dikkate alınarak *"tasarlanmış ve önceden tanımlanmış veri koruma"* kuralının hukukumuz tarafından da kabul edilmesi ve uygulanması gerekmektedir (Dülger, 2021, s. 1, 5-6; Çekin, 2016, s. 642).

II. VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLER

Kişisel verilerin güvenliğinin sağlanabilmesi için veri sorumlusu ve veri işleyenlerin alması gereken belirli bazı teknik ve idari tedbirler bulunmaktadır. Bu hususa ilişkin olarak GDPR m. 32'de alınabilecek teknik ve idari tedbirler düzenlenmiş ve gerekçesinin 83. maddesinde ayrıntılı olarak açıklanmıştır (Dülger, 2020, s. 537). Bu doğrultuda uygun teknik ve idari tedbirlere; "Kişisel verilerde takma ad kullanılması ve şifreleme; işleme sistemleri ve hizmetlerinin sürekli gizliliği, bütünlüğü, kullanılabilirliği ve esnekliğinin sürekli olarak sağlanması; fiziksel veya teknik bir müdahale durumunda kişisel verilere zamanında erişim ve geri yükleme olanağının sağlanması; veri işlemenin güvenliğini sağlamak için teknik ve organizasyonel önlemlerin etkinliğini düzenli olarak test etme ve değerlendirme imkânının sağlanması" gibi yöntemler örnek olarak sayılmıştır (GDPR m. 32).

KVKK m. 12/1'de ise, veri sorumlusunun *"Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda"* olduğu hüküm altına alınmıştır. Ancak hükmün içeriğinde, teknik ve idari tedbirlere ilişkin herhangi bir ayrıntı ve açıklamaya yer verilmemiştir. Esasen bu hususun bir eksiklik değil, KVKK'nun genel kanun olma özelliğinin bir tezahürü olarak yorumlanması gerektiği kanaatindeyiz. Zira teknolojinin her gün gelişip değiştiği ve bu hızı takip etmenin dahi çok zor olduğu göz önünde bulundurulduğunda; kanun ile belirlenecek sınırlı sayıdaki tedbirlerin zaman içerisinde

yetersiz kalacağı ve yeni gelişmelere göre sürekli kanun değişikliği yapılması gerekeceği aşikardır (Develioğlu, 2017, s. 100; Hizarcı, 2019, s. 136-137; Çelikel, 2021, s. 123-124). Nitekim bu genel düzenlemenin uygulanabilirliğini sağlamak amacıyla da uluslararası standartlar göz önünde bulundurularak Kurum tarafından *"Kişisel Veri Güvenliği Rehberi"* yayımlanmıştır.

Bununla birlikte Kurul tarafından verilen 31.01.2018 tarihli ve 2018/10 sayılı karar ile *"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler"* belirlenmiştir. Buna göre;

> *"1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi, 2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik, a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi, b) Gizlilik sözleşmelerinin yapılması, c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması, ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi, d) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması, 3- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi, b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması, c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması, ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması, d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması, e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması, 4- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması, b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi, 5- Özel nitelikli kişisel veriler aktarılacaksa a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması, b) Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması, c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi, ç) Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi gerekir. 6- Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır."*

Bu tedbirler, özel nitelikli veriler için belirlenmiş olsa da tüm kişisel veriler açısından veri sorumlusunun alacağı teknik ve idari tedbirlere yol gösterici niteliktedir (Eraslan Türkmen, 2019, s. 134 vd.).

Veri sorumlusu ve veri işleyen tarafından kullanılan teknolojinin değişmesi veya veri güvenliği uygulamalarının gelişmesi durumunda, alınan önlemler yeniden belirlenerek güncellenmeli ve gerektiği taktirde değiştirilmelidir. Tedbirlerin sürekli uygulanması halinde de mutlak bir veri güvenliğinin sağlanması söz konusu değildir (Dülger, 2020, s. 537; Zor, 2020, s. 93; Çekin, 2019, s. 145). Zira gerçek veri güvenliğinin sağlanması; ancak kişisel verilerin elde tutulmaması ve işlenmemesi ile mümkün olabilir. Bu sebeple veri sorumlusu tarafından gerçekten işlenmesi gerekli olan verilerin tespiti ve bu verilerin ihlaline ilişkin riskler belirlendikten sonra en uygun ve orantılı tedbirlerin alınması gerekir (Çekin, 2019, s. 146). Bu belirlemede esas olan veri sorumlusunun; faaliyet alanı, büyüklüğü, işlediği verilerin niteliği, altyapısı, uygulama maliyeti vb. unsurları dikkate almasıdır (Taştan, 2017, s. 74). Bu unsurları dikkate almayan ve yeterli seviyede veri güvenlik sistemi oluşturmayan veri sorumluları, doğan zararlardan sorumlu olacaktır.

Bu çerçevede genellikle kurumlarda veri güvenliğinin sağlanması amacıyla kullanılan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) Standardı önem arz etmektedir (Altındere, 2020, s. 180; Korucu, 2021, s. 65). Zira bu sistem ile kurumların, verileri; mevzuata uygun şekilde işlemesi ve koruması, doğru politika ve prosedürler oluşturması, risklerin önceden belirlenerek yönetilmesi, uygun yazılım ve donanımlardan yararlanarak dışarıdan veya içeriden yetkisiz erişimin engellenmesi sağlanmaktadır. Örneğin belirlenen politikalar kapsamında şirkete ait mail adreslerinin phishing (oltalama) sisteminden korunmasını sağlayan güvenli yazılımlar yerleştirilmesi, veri güvenliğinin korunmasına hizmet etmektedir.

Bu çerçevede Kurul, 09.10.2020 tarihli ve 2020/787 sayılı kararı ile veri sorumlusunun; "çalışanlarının ISO27001 sertifikalı eğitimler almasını zorunlu tutması ve her yıl güncellenen içerikleriyle eğitimleri tekrarlamasını, sızma testi uygulamasını, mevcut risk ve tehditleri belirleyerek ağ güvenliğini sağlaması ve güvenlik duvarı kullanmasını, kurumsal politikalar hazırlamış ve uygulamaya başlamış olmasını, kurum içerisinde periyodik/rastgele denetimler yapmasını/yaptırmasını, yetkisiz erişim denemelerinin bilgi teknolojileri birimi tarafından tespit edildiği an üst yönetime ve Şirket Kişisel Verilerin Korunması Komitesine raporlanması ve derhal veri güvenliği ekibinin kurulması" gibi önlemleri almış olmasını, veri güvenliğine ilişkin *"makul teknik ve idari tedbirleri almış olduğu"* şeklinde değerlendirmiştir.

Bu doğrultuda veri sorumlusu tarafından alınması gereken teknik ve idari tedbirler aşağıda detaylı olarak incelenmiştir.

A. Kişisel Veri Güvenliğine İlişkin Alınması Gereken İdari Tedbirler

Kişisel Veri Güvenliği Rehberi ile veri sorumlularının alabileceği gerekli idari tedbirler; "mevcut risk ve tehditlerin belirlenmesi, veri işleme politikalarının ve prosedürlerinin oluşturulması, veri minimizasyonu ilkesi çerçevesinde elde edilen verilerin mümkün olduğunca azaltılması, veri işleyenlerle ve müşterek veri sorumlularıyla sözleşme yapılması, çalışanlara yönelik eğitim ve farkındalık çalışmaları, çalışanlara yönelik tedbirler (iş sözleşmeleri, disiplin yönetmeliği, gizlilik taahhütnameleri), kurum içi periyodik ve/veya rastgele denetimler, kurumsal iletişim (Kurul ve ilgili kişiyi bilgilendirme süreçleri, kriz ve itibar yönetimi vb.) ve Veri Sorumluları Sicil Bilgi Sistemine bildirim yapılması" şeklinde belirlenmiştir (KVK Kurumu, Kişisel Veri Güvenliği Rehberi, 2018, s. 9-13, 29; Çekin, 2019, s. 105-106; Altındere, s. 82; Dülger, Kişisel Verilerin Korunması, s. 540-543; Günbey, 2020, s. 120-121).

1. Risk Analizi

Veri sorumlusu, kişisel verilerin güvenliğinin sağlanması için elinde bulunan kişisel verilerin ne olduğuna, bu verilerin işlenmesi ile meydana gelebilecek risklerin gerçekleşme olasılığına ve gerçekleşmesi halinde yapacağı etkiye ilişkin belirlemelerde bulunarak doğru ve uygun tedbirleri almalıdır (Altındere, 2020, s. 164; Çekin, 2019, s. 147; KVK Kurumu, 2018, s. 8). Ortaya çıkabilecek ve mevcut olan risklerin belirlenmesinde; işlenen verinin özel nitelikli kişisel veri olup olmadığı, içeriği gereği hangi seviyede gizlilik gerektirdiği ve güvenlik ihlali halinde veri sorumlusu ve ilgili kişi açısından meydana gelebilecek zarar göz önünde bulundurulmalıdır (Altındere, 2020, s. 164-165; KVK Kurumu, 2018, s. 8). Bu sebeple risk kaynaklarının sistematik olarak belirlenmesi ve yüksek risk kaynaklarına karşı önlem alınması büyük önem arz etmektedir (Çekin, 2019, s. 147). Risk kaynaklarının belirlenmesinden sonra risklerin azaltılması veya ortadan kaldırılması için riskin tipine göre; personeli eğitmek, mimariyi değiştirmek, süreç veya prosedürü değiştirmek gibi farklı tekniklerin planlanarak uygulanması gerekmektedir (Korucu, 2021, s. 38; KVK Kurumu, 2018, s. 8). Bununla birlikte Kurum, yapılan risk analizine göre veri sorumlusunun, riski hafifletmek için gerekli tedbirleri almadığı ve veri işlemenin gerçek kişilerin hak ve özgürlükleri bakımından yüksek risk doğuracağının ortaya çıktığı durumlarda, veri işleme faaliyetinden önce Kurum'a danışılması gerektiğini belirtmektedir (KVK Kurumu, 2020, s. 16). Bu durum, Kurum'un uygulamalarında, KVKK'da yer almayan ancak GDPR kapsamında düzenlenmiş olan hesap verebilirlik ilkesine ve veri koruma etki analizi gibi uyum araçlarına paralel şekilde hareket ettiğini göstermektedir (Kaya, 2020, s. 1890).

2. Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Oluşturulması

KVKK, kişisel veri güvenliğinin sağlanmasına yönelik olarak veri güvenliği politikalarının belirlenmesi gerektiğine ilişkin açık bir düzenlenme getirmemiştir. Ancak sicile kayıt yükümlülüğü bulunan veri sorumlularına getirilmiş olan veri işleme envanteri hazırlama zorunluluğu, diğer veri sorumluları açısından da fayda sağlayacak niteliktedir. Zira veri güvenliğinin sağlanabilmesi için

işlenen verinin niteliğine göre; kişisel veri işleme envanterinin hazırlanması, bilgi güvenliği, erişim, saklama, imha vb. sürdürülebilir kurumsal politikaların oluşturulması ve uygulanması gerekir (Çekin, 2019, s. 147; Erarslan Türkmen, 2019, s. 142; KVK Kurumu, 2018, s. 11). Uygulamada, yönetim sistemine uygun politika ve prosedürlerin hazırlanmaması nedeniyle çalışanların üzerinde baskı oluşmakta ve yeterli güvenlik seviyesinin sağlanamadığı durumlar söz konusu olmaktadır. Bu hallerde kuruluşların ne yapacaklarını düşündükleri değil; veri sorumlusu ve veri işleyen tarafından gerçekte üstlenilen ve yapılan işleme faaliyetlerinin her aşamasına ilişkin alınacak olan tedbirlerin belirlendiği, örnek vaka çalışmaları üzerinden hazırlanacak prosedürlerin uygulanması gerekmektedir (Altındere, 2020, s. 167; Dülger, 2020, s. 831). Bu hususa ilişkin KVK Kurumu tarafından hazırlanmış olan *Kişisel Veri Saklama ve İmha Politikası*, veri sorumlularına da yol gösterici niteliktedir (KVKK, Kişisel Veri Saklama ve İmha Politikası).

Kurumlar tarafından belirlenen politika ve prosedürlerin, düzenli aralıklarla kontrol edilmesi ve sürekli değişen teknolojik gelişmeler doğrultusunda güncellenmesi gerekmektedir (Altındere, 2020, s. 167; Çekin, 2019, s. 148; Dülger, 2020, s. 537; Küzeci, 2019, s. 256; KVK Kurumu, 2018, s. 11). Güncellenen politika ve prosedürlerin önceki hallerinin de kayıt altına alınarak saklanması gerekir. Zira bu sayede veri sorumluları hem o tarihteki ihlal iddialarına karşı savunma yapabilir hem de veri güvenliği açısından ne derece geliştiklerini tespit edip gösterebilir (Dülger, 2020, s. 832). Bununla birlikte gizlilik içeren bilgiler hariç olmak üzere, veri koruma politikalarının, ilgili kişilerin ulaşabileceği şekilde internet sitesinde yayınlanmasına özen gösterilmelidir.

3. Çalışanların Eğitilmesi ve Farkındalık Çalışmaları

Kurumların, kişisel veri, veri güvenliği, verilerin korunması için kullanılan sistemler gibi konularda çalışanlarına eğitim vermesi şarttır. Bu eğitimlerin, işe yeni başlayanlar için zorunlu tutulması, çalışmakta olan personeller için 6 ay veya en geç 1 yıl içerisinde yenilenmesi gerekmektedir. Veri sorumlusu, çalışanlarını bilinçlendirmeye yönelik yaptığı paylaşım ve eğitimleri kayıt altına alarak saklamalıdır. Zira veri güvenliğinin, dışarıdan gelen saldırılar ile zedelenmesi mümkün olduğu gibi, veri sorumlusunun çalışanları tarafından yapılacak olan bilinçli veya bilinçsiz eylemler neticesinde ihlal edilmesi de mümkündür (Altındere, 2020, s. 165; KVK Kurumu, 2018, s. 9; Küzeci, 2019, s. 255). Buna, bir çalışanın tecrübesizliği ve dikkatsizliği ile birçok kişisel veri içeren evrakı yanlış alıcıya göndermesi veya içecek servisi yapan personelin, o anda masasında bulunmayan başka bir çalışanın, açık kalmış olan bilgisayar ekranından kişisel verileri hukuka aykırı olarak elde etmesi örnek olarak verilebilir.

Nitekim Kişisel Verileri Koruma Kurulu'nun 21.12.2017 Tarih, 2017/62 Sayılı Kararında, çalışanların bitişik düzende hizmet verdiği kamu ve özel sektör kurum ve kuruluşlarının *"banko/gişe/masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirlerine yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymasını, görmesini,*

öğrenmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirleri alması" gerektiği belirtilmiştir.

Veri sorumlusunun, ilgili kişinin onayı alınmadan, herhangi bir üçüncü kişiyle bilgi paylaşımı yapılmayacağına ilişkin çalışanları ile gizlilik sözleşmesi yapması yararlı olacaktır. Nitekim Kurul vermiş olduğu 31.01.2018 tarihli ve 2018/10 sayılı kararında, özel nitelikli kişisel verilerin işlenmesi sürecinde yer alan çalışanlar ile gizlilik sözleşmesi yapılmasını zorunlu tutmuştur (KVK Kurumu, 2018, s. 10).

Diğer taraftan veri sorumlusu, faaliyetleri kapsamında toplanan kişisel verilerin, işleme koşullarını ve işleme süresini net bir biçimde belirlemelidir. Bu bağlamda, bu verilere erişim yetkisi olan kişilerin de yetki kapsamları ve sürelerinin belirlenerek yetkisiz kişilerin verilere erişiminin engellenmesi gerekir (Çekin, 2019, s. 149; KVK Kurumu, 2018, s. 9). Bu sistemin korunabilmesi için de bu çalışanların yetkileri ve işlemlerinin hukuka uygunluğu belli periyotlarla denetlenmeli ve prosedürlere uyulmaması halinde disiplin süreci başlatılmalıdır (Altındere, 2020, s. 166; Çekin, 2019, s. 148; KVK Kurumu, 2018, s. 9; Dülger, 2020, s. 543). Zira ülkemizde cezası olmayan bir kurala uyulmasına gerek olmadığı anlayışı hâkim olduğu için, veri ihlali halinde hem kurumun hem de bireylerin hukuki ve cezai sorumluluklarının doğabileceğinin anlatılması büyük önem arz etmektedir.

4. Kişisel Verilerin Azaltılması

KVKK m. 4/2-b ve d bentleri kapsamında "kişisel verilerin, doğru ve gerektiğinde güncel olarak; ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi" gerekmektedir. Bu nedenle veri sorumluları, topladığı verilerin kullanılmayan kısmını ya da işlediği verilerin doğru olmayan veya güncelliğini yitirmiş olanlarını, *"Kişisel Veri Saklama ve İmha Politikası"* ile *"Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Yönetmeliği"*ne uygun olarak imha etmelidir (Altındere, 2020, s. 168). Aksi halde verilerin korunması zor hale gelecek ve yetkisiz erişimin önüne geçilmesi mümkün olmayacaktır (KVK Kurumu, 2018, s. 12; Özkan, 2020, s. 173). Bu kapsamda internet sitelerine yapılan üyelikler esnasında, kişinin gerekli olmayan bilgilerinin istenmemesi (örneğin T.C. numarası), alınabilecek idari tedbire örnek olarak verilebilir. Uygulamada en sık karşılaşılan sorun, *"kalsın, lazım olur, zararı yok"* mantığı ile kişisel verilerin, ihtiyaç duyulan muhafaza süresinden daha uzun süre tutulmasıdır (Altındere, 2020, s. 167; Dülger, 2020, s. 828). Buna bir şirketin, kuruluşundan itibaren çalışanlarına ilişkin tüm verileri saklaması ve imha etmemesi örnek olarak verilebilir. Bu durumda kişisel veriler hukukunda uzman bir danışmanın yardımıyla sadece işleme amacıyla orantılı olan verilerin saklanması ve bu verilere ilişkin en makul saklama sürelerinin tespit edilmesi gerekir.

5. Veri İşleyenler ile İlişkilerin Yönetimi

KVKK m. 12/2'de *"kişisel verilerin veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda veri sorumlusunun da bu*

kişilerle birlikte müştereken sorumlu olduğu" hüküm altına alınmıştır. Bu doğrultuda bilgi teknolojilerine ilişkin ihtiyaçlarını karşılamak için veri işleyenlerden hizmet alan veri sorumlularının, en az kendilerinin sağladığı seviyede veri güvenliğinin sağlandığından emin olmaları gerekir (KVK Kurumu, 2018, s. 12-13). Veri işleyenin, hangi niteliklere sahip olması gerektiği konusunda, Kanun'da açık bir düzenleme bulunmamaktadır. Bu sebeple veri sorumlusunun, ilgili kişi ve kuruluş hakkında araştırma yapması, yeterli tedbirleri aldığına ve alacağına ilişkin kanaat getirmesi önemlidir. Diğer taraftan Kanun'da öngörülmeyen ancak GDPR'da açıkça düzenlenmiş olan yazılı sözleşme ilkesi kapsamında veri sorumlusunun, veri işleyen ile bağlayıcı nitelikte yazılı bir sözleşme imzalaması gereklidir (Altındere, 2020, s. 168; Dülger, 2020, s. 621, 822; KVK Kurumu, 2018, s. 13; Develioğlu, 2017, s. 103).

Veri işleyen ile imzalanan sözleşmede; "veri işleyenin, kişisel verileri koruma mevzuatı ile uyumlu şekilde, sadece veri sorumlusunun talimatları doğrultusunda ve sözleşmede belirtilen veri işleme amaç ve kapsamına uygun olarak hareket edebileceği" hükmü yer almalıdır. Bununla birlikte veri işleyenin, "süresiz sır saklama yükümlülüğü olduğu" ve "veri ihlali halinde, veri sorumlusuna derhal bildirimde bulunması gerektiği" de sözleşmede düzenlenmelidir (GDPR, m. 33/1-2; Altındere, 2020, s. 168-169; KVKK m. 12/4-5; KVK Kurumu, 2018, s. 13; Taştan, 2017, s. 117-154). Zira Kanun'un açık lafzı ile bildirim yükümlülüğünün, veri sorumlusuna verilmiş olması göz önüne alındığında veri işleyenin, geç bildirimde bulunması halinde meydana gelecek gecikmeden veri sorumlusu sorumlu tutulacaktır (KVKK m. 12/5). Bununla birlikte veri sorumlusu, veri işleyen ile yapılan sözleşmede belirlenen hükümlere uyulup uyulmadığını ve kişisel verilerin işlenmesinden sonra, tüm kişisel verilerin ortadan kaldırılıp kaldırılmadığını da denetlemelidir.

Veri İhlali Bildirimi yapılmasındaki amaç ise, ihlal nedeniyle ilgililer nezdinde ortaya çıkabilecek olumsuz sonuçların engellenmesinin ya da en aza indirilerek gerekli önlemlerin alınmasının sağlanmasıdır (KVK Kurulu'nun 18.09.2019 tarih ve 2019/271 sayılı kararı). Nitekim KVK Kurulu'nun 04.01.2019 tarih ve 2019/10 sayılı kararı ile Kurul'a yapılacak olan bildirimin en geç 72 saat olarak yorumlanması gerektiği belirtilmiştir. Buna göre:

> *"…Kanunun 12 nci maddesinin (5) numaralı fıkrasının "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir…." hükmünde yer alan "en kısa sürede" ifadesinin 72 saat olarak yorumlanmasına ve bu kapsamda veri sorumlusunun bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine, veri sorumlusunca söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına…"*

Kararda dikkat çeken bir diğer husus ise; GDPR'da sadece ilgili kişinin hak ve menfaat kaybına uğraması ihtimalinde yapılması öngörülen bildirimin, KVKK açısından yapılmasının zorunlu tutulmuş olmasıdır (Dülger, 2020, s. 559). GDPR, düşük riskli veri işleme faaliyetlerinde bulunan veri sorumlularına; veri sahiplerine bildirim yapılması, veri koruma etki analizi yapılması, veri koruma otoritesine başvuru gibi bazı yükümlülükleri yerine getirme zorunluluğu getirmemiştir (GDPR m. 34). Bunun nedeni GDPR'ın, "veri sorumlularının, veri işleme eyleminin doğuracağı risklerle doğru orantılı olarak gerekli teknik ve idari tedbirleri alma yükümlülüğü" olarak tanımlanan *"risk temelli yaklaşımı"* benimsemiş olmasıdır (GDPR m. 32). Bu yaklaşım doğrultusunda veri sorumlusunun, veri işleme faaliyetindeki risk seviyesi yükseldikçe hesap verilebilirliğe ilişkin yükümlülükleri de ağırlaşmaktadır (Keser, 2018, s. 20). Ancak KVKK'nda böyle bir risk değerlendirmesi ayrımına gidilmemiş ve ihlalin önlemesine yönelik değil, ihlalin gerçekleşmesi sonucunda yaptırım uygulanmasına yönelik bir tutum izlenmiştir. Bununla birlikte ilgili kişilere yapılacak olan bildirimin süresi de belirtilmemiştir.

Bu çerçevede veri sorumlularının yapmış oldukları risk ölçümleri kapsamında, veri işleme faaliyetinin risk seviyesine göre, ilgililere bildirim değerlendirmesi yapılması ve konuya ilişkin verilen kararlarda (KVK Kurulu'nun 16.05.2019 tarih ve 2019/143 sayılı; 16.05.2019 tarih ve 2019/141 sayılı; 08.03.2019 tarih ve 2019/67 sayılı; 01.09.2022 tarih ve 2022/882 sayılı kararları) yer alan sürelere ilişkin çelişkilerin giderilerek ilgililere yapılacak olan bildirim için makul bir sürenin belirlenmesi gerekmektedir (Dülger, 2020, s. 559; Keser, 2018, s. 20).

B. Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler

Kişisel verilerin özel nitelikli olup olmamasına göre, farklı teknik tedbirlerin alınması gerekmektedir. Bilindiği üzere riskin boyutu arttıkça alınması gereken önlemlerin de arttırılması ve farklı önlemler alınması zorunludur (Küzeci, 2019, s. 256). Bu doğrultuda veri sorumluları, teknolojik gelişmeler ile doğru orantılı olarak sistem güncelleme ve yenileme işlemlerini dikkatli şekilde yerine getirmelidir.

Veri sorumlusu tarafından alınabilecek teknik tedbirler, Kişisel Veri Güvenliği Rehberinde; "siber güvenliğin sağlanması (ağ güvenliği, uygulama güvenliği, veri maskeleme, şifreleme, kriptografi, veri kaybı önleme yazılımları, yedekleme güvenlik duvarları vb.), kişisel veri güvenliğinin takibi (sızma testi, erişim logları, saldırı tespit ve önleme sistemleri, kullanıcı hesap yönetimi, log kayıtları), kişisel veri içeren ortamların güvenliğinin sağlanması (veri kaybı önleme yazılımları, güncel anti-virüs sistemleri vb.), kişisel verilerin bulutta depolanması, sistemlerin tedariği, geliştirilmesi ve bakımı ile kişisel verilerin yedeklenmesi" şeklinde belirtilmiştir (KVK Kurumu, 2018, s. 28).

1. Siber Güvenliğin Sağlanması

Kişisel verilerin genellikle elektronik ortamda toplandığı ve işlendiği düşünüldüğünde; alınması gereken öncelikli tedbir, siber güvenliğin sağlanmasıdır (Altındere, 2020, s. 81). Bilgisayar sistemleri ve ağlara yönelik olarak programları bozma, değiştirme, yok etme veya parçalara ayırma şeklinde

kasten gerçekleştirilen siber saldırı eylemlerine karşı, elektronik sistemleri koruyan uygulamalara, siber güvenlik denilmektedir (Sarı, 2013, s. 16).

Siber güvenliğin sağlanabilmesi için tek bir güvenlik sisteminin değil, günün gerektirdiği sorunlara göre farklı sistemlerin de kullanılması ve düzenli kontroller neticesinde gereken önlemlerin alınması ve uygulanması gerekmektedir. Örneğin internet üzerinden gelen izinsiz erişim tehditlerine karşı koruma sağlayan güvenlik duvarı ve kişisel verilerin güvenliğini tehdit edebilecek internet sitelerine veya online servislere erişimi engelleyen internet ağ geçidi, saldırıları durduran ilk savunma mekanizmasıdır (Altındere, 2020, s. 82, 175-176; Küzeci, 2019, s. 255; KVK Kurumu, 2018, s. 16). Bu sistemlerin doğru şekilde çalışabilmesi için düzenli kontrollerin ve güncellemelerin yapılması, güvenlik açığı tespit edilmiş ve kullanılmayan eski sürümlerin, cihazlardan kaldırılması gerekir (Altındere, 2020, s. 82-83; Küzeci, 2019, s. 255-256; KVK Kurumu, 2018, s. 16-17). Ayrıca zararlı yazılımların önlenebilmesi için bilgi sistem ağını düzenli bir şekilde tarayan ve tehlikeleri tespit ederek önleyen güncel antivirüs, antispam gibi programların kullanılması gerekir (Küzeci, 2019, s. 255; KVK Kurumu, 2018, s. 18). Örneğin Kurul'un 27.08.2019 tarihli ve 2019/255 karar sayılı kararına göre: Bir turizm şirketinin "Local Area Network (LAN-Yerel Alan Ağı)" üzerinden elde edilen şifrelerinin kullanılması suretiyle yetkisiz şifre girişi ile siber saldırı yapılmıştır. Bu esnada güvenlik duvarının güncel olmaması ve şirket IT sistemlerinin, bilişim sistemlerinde gerçekleşen sızma veya olmaması gereken bir hareketi fark edememesi, Kurul tarafından "teknik eksiklik" olarak kabul edilmiştir. Söz konusu ihlalin, diğer çalışanlar tarafından bilgi işlem birimine bildirilmesi ise, "*Şirketin Bilgi İşlem Biriminin ve Bilgi Sistemlerinin düzgün olarak çalışmadığı ve işlemediğinin bir göstergesi olduğu"* şeklinde yorumlanmıştır.

Bu çerçevede kişisel veri bulunan sistemlerin; sınırlı erişimde tutulması, çalışanların kullanıcı adı ve şifre ile sistemlere giriş yapması, şifrelerin harf, rakam ve sembollerden oluşan kombinasyonlar ile oluşturulması, şifre denemelerinin sınırlandırılması, yetkisi sona eren personellerin girişlerinin engellenmesi vb. önlemler ile korunması önem arz etmektedir (Altındere, 2020, s. 176; KVK Kurumu, 2018, s. 17). Farklı internet sitelerinden kişisel veri temin edilmesi gerektiğinde ise, sunucu ile istemci arasında akan veri güvenliğini ve bütünlüğünü mümkün kılan SSL bağlantıları veya daha güvenli sertifikaların kullanılması kişisel veri güvenliğinin sağlanmasına hizmet etmektedir (KVK Kurumu, 2018, s. 18; Özkan, 2020, s. 173).

2. Kişisel Veri Güvenliğinin Takibi

Veri sorumlularının, sistemlerine içeriden veya dışarıdan gelen siber saldırıları ve zararlı yazılımları kısa sürede fark edip önleyebilmesi için; "bilişim ağlarında hangi yazılım ve servislerin çalıştığının tespiti, bilişim ağlarında herhangi bir sızma veya olağan dışı bir hareket olup olmadığının tespiti, tüm kullanıcılara ait işlem hareketlerinin (log kayıtları gibi) düzenli olarak tutulması, güvenlik ihlallerinin en hızlı şekilde raporlanması ile personellerin güvenlik açıklarını veya zafiyetleri kullanan tehditleri bildirilebilmesi için resmi raporlama prosedürü oluşturulması" gibi tedbirler alması gerekmektedir

(Altındere, 2020, s. 178-179; KVK Kurumu, 2018, s. 18; Zor, 2020, s. 100). Bu tedbirlerin, veri güvenliğini sağlayabilmesi için; sistemlerden gelen uyarıların dikkate alınması ve gerektiğinde hemen müdahale edilmesi, raporlama sistemlerinin düzenli olarak test edilmesi ve sonuçlarına göre değerlendirmelerde bulunularak güvenlik açıklarının yok edilmesi büyük önem arz etmektedir (KVK Kurumu, 2018, s. 19; GDPR m. 32/1-d). Bu hususa Kurul'un, log kayıtlarının kontrol edilmesi ile veri ihlalini kısa bir sürede fark eden Ficosa International Otomotiv San. ve Tic. A.Ş.'ye ilişkin 29.12.2020 tarihli ve 2020/1011 sayılı kararı örnek olarak verilebilir.

3. Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

Veri sorumlularının bünyesinde yer alan cihazlarda veya kâğıt ortamında saklanan kişisel verilerin; çalınma, kaybolma veya yangın, sel gibi dış risklere karşı güvenliğinin sağlanması için uygun yöntemlerle korunması, bu ortamlara giriş çıkışların kontrol altına alınması ve sadece yetkili kişilerin girmesine izin verilmesi, çalışanların şahsi cihazlarının sisteme erişiminin gerekli tedbirler alındıktan sonra sağlanması, şifreleme ve ağ bileşenleri arasında erişimin sınırlandırılması gibi önlemlerin alınması gerekmektedir (Altındere, 2020, s. 177-178; KVK Kurumu, 2018, s. 20; Küzeci, 2019, s. 255-256). Bununla birlikte kişisel veri içeren fiziki evraklar, sunucular, yedekleme cihazları, CD, USB ve DVD gibi cihazların ISO/IEC 27001 standartlarındaki korunaklı bir odada tutulması, kullanılmadıkları zaman sadece yetkili kişilerin girebileceği şekilde kilit altında bulundurulması, giriş ve çıkış kayıtlarının tutularak fiziksel güvenliğin sağlanması gerekir (Altındere, 2020, s. 179; KVK Kurumu, 2018, s. 21).

4. Kişisel Verilerin Bulutta Depolanması

Kişisel verilerin, sanal ortamda muhafaza edilmesini ve kaybolmamasını sağlayan alanlara bulut depolama sistemi denilmektedir. Veri sorumlusunun, kendi bilgi sistemi dışında bir bulut depolama sisteminde veri işlemesi, bazı riskleri de ortaya çıkarmaktadır. Bu risklerin en aza indirgenmesi için; depolanan kişisel verilerin detaylı bir envanterinin oluşturulması, yedeklenmesi, bu bilgilere erişim gerektiğinde iki kademeli kimlik doğrulama tedbirinin uygulanması, depolama esnasında bilginin güvende olmasını sağlayan özel kodlama (kriptografik) yöntemleriyle kişisel verilerin şifrelenmesi, her bulut için ayrı şifreleme anahtarı kullanılması ve hizmet ilişkisi sona erdiğinde şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekmektedir (Altındere, 2020, s. 172-173; KVK Kurumu, 2018, s. 22). Kurul 16.04.2020 tarihli ve 2020/286 sayılı kararında; *"Hackerların, şirketin bulut sistemlerine, belirli olmayan kaynaklardan temin ettikleri kimlik bilgileri kullanarak erişmiş olduğu, bir bulut sistemi bulunan veri tabanına saldırganlar tarafından erişim sağlanmasının yapılan zafiyet testlerin yetersiz olmasının ve gerekli önlemlerin alınmadığının göstergesi olduğu"* ve gerekli teknik tedbirleri almayan şirket hakkında 1.000.000 TL idari para cezası uygulanması gerektiğine karar vermiştir.

5. Bilgi Teknolojileri Sistemlerinin Tedariği, Geliştirilmesi ve Bakımı

Hızla değişen teknolojik gelişmeler, halihazırda kullanılan sistemlerin belli oranda yetersiz kalmasına sebep olabilmektedir. Bu sebeple veri sorumlusu, güvenlik ihtiyaçlarını belirlemeli ve buna göre en uygun ve güncel sistemi tercih etmelidir. Kullanılan cihazların düzenli kontrollerinin yapılması, bakım veya arıza sebebiyle üçüncü kişilerin teması gerektiğinde; cihazlardaki veri saklama ortamının sökülüp saklanması ya da sadece arızalı parçanın verilmesi, dışarıdan herhangi bir kopyalama işlemenin yapılmaması için gerekli önlemlerin alınması büyük önem arz etmektedir (KVK Kurumu, 2018, s. 23).

6. Kişisel Verilerin Yedeklenmesi

Veri güvenliğine ilişkin alınan tüm tedbirlere rağmen veri sistemin; saldırı, kötü amaçlı yazılım, çalınma, doğal afet, kullanım hatası vb. sebeplerle zarar görmesi mümkündür. Bu hallerde veri sorumlusunun, yedeklenen verilere ulaşması ve en kısa sürede faaliyetlerine devam etmesi gerekmektedir (Altındere, 2020, s. 176; Çekin, 2019, s. 151; Kara, 2013, s. 29; KVK Kurumu, 2018, s. 24). Yedeklenen kişisel verilerin, mutlaka ağ dışında tutulmasına ve sadece sistem yöneticisi tarafından erişilebilir olmasına özen gösterilmelidir (KVK Kurumu, 2018, s. 24; Göksu, 2010, s. 23). Aksi halde, veri seti yedeklerinde yer alan verilerin de yok olması söz konusu olabilir.

Nitekim Kurul, 16.06.2020 tarihli ve 2020/463 sayılı kararında; "kritik öneme sahip tüm sunucu ve verilerinin ve bunlarla birlikte diğer sunucuların yedek dosyalarının depolandığı Data Domain Sunucusu verilerinin" silinmesinde veri sorumlusunun kusurlu olduğuna ve 125.000 TL idari para cezası uygulanması gerektiğine karar vermiştir.

III. VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLERİN UYGULANMASI VE DENETİM MEKANİZMASI

Kişisel verilerin güvenliğine ilişkin tedbirler alınması gerektiği yukarıda incelendiği üzere, KVKK m. 12'de düzenlenmiş ve alınması gereken tedbirler "*Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)"*nde belirlenmiştir. Ancak işleme faaliyetlerinin, getirilen düzenlemelere uygun şekilde gerçekleştirildiğini gösterme yükümlülüğü (GDPR m. 24), KVKK kapsamında düzenlenmemiştir (Kaya, 2020, s. 1892). Bu nedenle veri sorumlularının alması gereken bu tedbirler, çoğu zaman sadece teoride kalmakta ve uygulamaya geçirilmemektedir. Uygulamadaki bu sorunun başlıca kaynağı ise etkili bir denetim mekanizmasının bulunmamasıdır.

GDPR m. 37 hükmü ile veri sorumluları ve veri işleyenlerin, veri koruma kurallarına uygun faaliyet göstermesini sağlamak amacıyla veri sorumluları ve veri işleyenlere, bilgi ve tavsiye verecek "veri koruma görevlileri" atanması ve hatta bazı durumlarda zorunlu tutulması gerektiği düzenlenmiştir (Dülger, 2019, s. 126). KVKK'da böyle bir kavram bulunmamakla birlikte KVK Kurum'u tarafından *"Personel Belgelendirme Kuruluşları"*nın, Veri Koruma Görevlisi (VKG) sertifikasyon sınavları

düzenleyeceği yayınlanmıştır. Bu sınav sonucunda başarılı olan gerçek kişilerin, veri koruma görevlisi unvanını kullanabileceği belirtilmiş olsa da henüz görevleri açıklanmamıştır. Bununla birlikte KVK Kurum'u tarafından Veri Koruma Görevlisi tanımının, GDPR'da yer alan Veri Koruma Görevlisi (DPO) ile aynı anlamı ifade etmediğine ilişkin bir kamuoyu duyurusu da yapılmıştır. Bu açıklamalar neticesinde, hukuk sistemimize getirilecek olan yeni veri koruma görevlisi kavramının da uygulamadaki kişisel veri işleme süreçlerinin hukuka uygun şekilde sürdürülmesinin sağlanması sorununu çözemeyeceği kanaatindeyiz.

Bu çerçevede bağımsız olarak çalışan, veri sorumluları ve veri işleyenlerin KVKK ile uyumlu şekilde veri işleme faaliyetlerini yürütmesinin devamlılığını sağlayacak, kişisel verilerin korunmasına ilişkin alınan tedbirlerin uygulanabilirliğini denetleyecek ve ortaya çıkan sorunlara hızlı çözümler üreterek kişisel verilerin korunmasına doğrudan katkıda bulunacak bir görevlinin belirlenmesi gerekmektedir. Bununla birlikte veri işleme faaliyetlerinden önce ve veri işleme faaliyetleri esnasında, gerekli idari ve teknik tedbirlerin alınıp alınmadığının da düzenli olarak denetlenmesinin sağlanması gerekir. Ancak KVK Kurul'unun re'sen denetleyici görevi bulunmasına rağmen daha çok ilgili kişinin şikâyeti üzerine denetleme süreci başlatılmaktadır. Bu durum da veri sorumlularının gerekli önlemleri alma konusunda ihmalkâr davranmalarına ve veri ihlallerinin gerçekleşmesine sebep olabilmektedir. Bu noktada personeller kadar veri sorumlularının da yapılacak eğitimler ile bilinçlendirilmesi ve Kurul'un ihlal bildirimini veya ilgili kişi şikâyetlerini beklemeden düzenli denetim sağlayacak bir mekanizma kurması önem arz etmektedir.

Diğer taraftan ülkemizde henüz Kanun'u anlama ve uyum sağlama sürecinde olan veri sorumlularının, veri koruma kültürünü benimsemesini ve bu doğrultuda iç ilişkilerini düzenlemesini teşvik eden bir yaklaşım benimsenmelidir (Aşıkoğlu, 2018, s. 193). Bu çerçevede veri işleme faaliyetlerinin, gerçek kişilerin temel hak ve özgürlükleri açısından meydana getirebileceği riskler ve bunların önlenmesi için gerekli çalışmaların yapılmasının önemi hususunda veri sorumluları bilinçlendirilerek "tasarımdan itibaren veri koruma" ve "veri koruma etki analizi" kavramlarının hukukumuza kazandırılması büyük önem arz etmektedir (Bayram, 2022, s. 50). Zira tasarımdan itibaren veri koruma, sistemin kurulma anında ilkelere uygunluğunun gözetilmesini ve sonradan uyumlu hale getirme sorununu bertaraf ederken; veri koruma etki analizi, kurumların kendi kendini düzenlemesi (self regulation) için bir denetleme aracı olarak kullanılmakta ve oluşabilecek riskleri veri işleme süreci başlamadan önlemektedir (Aşıkoğlu, 2018, s. 192; Kartöz, 2020, s. 134). Kurum'un uygulama ve tavsiyelerinde, GDPR kapsamında düzenlenmiş olan şeffaflık ve hesap verebilirlik ilkeleri ile spesifik olarak veri koruma etki analizine benzer yapılara yer verilse de bu ilke ve yükümlülüklerin Kanun'unda da tanımlanması gerekmektedir (KVK Kurulu, 25.03.2019 tarihli ve 2019/78 sayılı kararı). Nitekim "Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı" tarafından düzenlenen 11. Kalkınma Planı (2019-2023) ile KVKK'nın, GDPR hükümleri doğrultusunda güncellenmesi hedeflenmektedir. Söz konusu reform çalışmaları kapsamında, Türk hukukunda da hesap verebilirlik ilkesine ve uyum araçlarına yer verilmesi beklenmektedir (Bayram,

2022, s. 49; Kaya, 2020, s. 1889). Bu kapsamda veri sorumluları tarafından, veri koruma etki analizi uygulamasının benimsenebilmesi için uzmanlardan destek alınması ve bu süreçten etkilenen kişilerin geri dönüşlerinin değerlendirilmesi yerinde olacaktır (Kartöz, 2020, s. 134).

SONUÇ

Teknolojik gelişmelerin hayatımıza sağladığı kolaylıkların yanı sıra, beraberinde getirdiği birtakım teknik problemler ve hukuki ihtilaflar da bulunmaktadır. Bunlardan biri olan kişisel verilerin korunması sorunu, bireyin temel hak ve özgürlüklerinin de zedelenmesine sebep olabilmektedir. Bu sebeple kişisel verilerin işlenmesinin belirli bir hukuki sistem ile korunması ve sınırlarının belirlenmesi gerekir.

Kişisel verilerin işlenmesi esnasında, veri güvenliğinin sağlanabilmesi için veri sorumlusu ve veri işleyenlere bazı yükümlülükler getirilmiştir. Bu yükümlülüklerden sadece biri olan veri güvenliğine ilişkin idari ve teknik tedbirleri alma yükümlülüğü, veri güvenliğinin sağlanabilmesi için büyük önem arz etmektedir. Zira kötü amaçlarla yapılan veri sızıntıları neticesinde, ciddi temel hak ihlalleri ve ekonomik kayıplar olması kaçınılmazdır. Bu sebeple veri sorumlusu, bireyin mahremiyetinin ve kişisel verilerin korunmasının sağlanması için gerekli teknik ve idari önlemleri almalıdır.

Belirtmek gerekir ki bu önlemler, "yeterli önlemler" niteliğindedir ve asgari düzeyde koruma sağlamaktadır. Veri sorumlusunun faaliyetlerinin daha yüksek koruma gerektirmesi halinde ise, veri sorumlusu işlediği verilerin niteliğine uygun olan üst düzey önlemler almalıdır. Peki üst düzey önlemler alınması, veri güvenliğinin tamamen korunmasını sağlar mı? İnsan faktörünün ve sistemsel hataların bulunduğu hiçbir koruma yöntemi, verilerin yüzde yüz korunmasını sağlayamaz. Bu çerçevede, verilerin en güvenli korunma şekli, kişisel verilerin toplanmaması ve işlenmemesi ile mümkün olabilir.

Sonuç olarak modern dünyada işlenmesi gereken birçok verinin bulunması ve bu durumun durdurulmasının mümkün olmaması sebebiyle veri sorumlularının, veri güvenliğini sağlayabilmek amacıyla gerekli tüm teknik ve idari tedbirleri alması, kişisel verilerin korunmasına ilişkin mevzuatlara uyması ve çalışanlarını bilinçlendirerek kurallara uyulmasını sağlayacak bir kültürün oluşması için tüm önlemleri alması gerekmektedir.

KAYNAKÇA

Akdağ, H. (2015). Türk ceza hukukunda kişisel verilerin korunması: Prof. Dr. Nevzat Toroslu'ya armağan, 27-48. https://www.academia.edu/

Aksoy, H. C. (2010). *Medeni hukuk ve özellikle kişilik hakkı yönünden kişisel verilerin korunması*. Ankara: Çakmak Yayınevi.

Altındere, M. (2020). *Kişisel verilerin korunması hukuku ve uygulanması*. Ankara: Adalet Yayınevi.

Aşıkoğlu, Ş. İ. (2018). *Avrupa birliği ve Türk hukukunda kişisel verilerin korunması ve büyük veri* [Yayınlanmamış yüksek lisans tezi]. İstanbul Üniversitesi.

Ayözger Öngün, A. Ç. (2019). *Kişisel verilerin korunması hukuku: Elektronik haberleşme sektörüne ilişkin özel düzenlemeler dahil*. İstanbul: Beta Basım Yayın.

Başalp, N. (2004). *Kişisel verilerin korunması ve saklanması*. Ankara: Yetkin Yayınları.

Bayram, Ö. B. (2022). Bir uyum aracı olarak veri koruma etki analizinin Türk hukuku bakımından değerlendirilmesi. *Kişisel Verileri Koruma Dergisi, 4*(1), 38-53.

Beytar, E. (2018). *İşçinin kişiliğinin ve kişisel verilerinin korunması*. İstanbul: On İki Levha Yayıncılık.

Canbek, G. & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi, 9*(3), 165-174.

Civan Kemiksiz, R. (2022). Büyük veri çağında kişisel veri güvenliği üzerine bir alan araştırması: Dijital yerliler ve dijital göçmenlerin güvenlik algıları. *Maltepe Üniversitesi İletişim Fakültesi Dergisi, 9*(1), 64-91.

Çelikel, S. (2021). *Kişisel verilerin korunması hukuku kapsamında veri sorumlusu ve veri sorumlusunun yükümlülükleri* [Yayınlanmamış doktora tezi]. Ankara Üniversitesi.

Çekin, M. S. (2019). *Avrupa birliği hukukuyla mukayeseli olarak 6698 sayılı kişisel verilerin korunması kanunu*. İstanbul: On İki Levha Yayıncılık.

Çekin, M. S. (2016). 6698 sayılı kişisel verilerin korunması hakkında kanun'un big data (büyük veri) ve irade serbestisi açısından değerlendirilmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 74*(2), 629-644.

Develioğlu, H. M. (2017). *6698 sayılı kişisel verilerin korunması kanunu ile karşılaştırmalı olarak avrupa birliği genel veri koruma tüzüğü uyarınca kişisel verilerin korunması hukuku*. İstanbul: On İki Levha Yayıncılık.

Dülger, M. V. (2019). Avrupa birliği genel veri koruma tüzüğü bağlamında kişisel verilerin korunması. *Yaşar Hukuk Dergisi,* 1(2), 71-174.

Dülger, M. V. (2020). *Kişisel verilerin korunması hukuku*. İstanbul: Hukuk Akademisi Yayıncılık.

Dülger, M. V. (2021, Şubat). Tasarlanmış ve önceden tanımlanmış veri koruma ile zarara karşı risk sorumluluğu: Kişisel verileri koruma kurulu'nun 18 şubat 2019 tarihinde yayınlanan kararları ne anlama geliyor?, 1-13. https://www.academia.edu/

Eraslan Türkmen, S. (2019). *Özel nitelikli kişisel verilerin işlenmesinde açık rızanın aranmadığı haller*. İstanbul: On İki Levha Yayıncılık.

Göksu, M. (2010). *Hukuk yargılamasında elektronik delil* [Yayınlanmamış doktora tezi]. Ankara Üniversitesi.

Günbey, O. (2020). *Kişisel verilerin korunması kanunu kapsamında veri sorumlusunun yükümlülükleri* [Yayınlanmamış yüksek lisans tezi]. İstanbul Bilgi Üniversitesi.

Gündüz, M. Ş. (2022). *Uluslararası insan hakları açısından kişisel veri güvenliği* [Yayınlanmamış yüksek lisans tezi]. Batman Üniversitesi.

Gürbüz Erel, İ. (2021). *Sağlık hukukunda kişisel verilerin korunması*. [Yayınlanmamış yüksek lisans tezi]. Kocaeli Üniversitesi.

Hizarcı, E. (2019). *6698 sayılı kişisel verilerin korunması kanununun ab veri koruma hukuku ışığında değerlendirilmesi*. [Yayınlanmamış yüksek lisans tezi]. Marmara Üniversitesi.

Kara, Ş. (2013). *Veri kurtarma yöntemlerinin başarımlarının değerlendirilmesi* [Yayınlanmamış yüksek lisans tezi]. Fırat Üniversitesi.

Kartöz, M. O. (2020). *Şeffaflık ve hesap verilebilirlik açısından kişisel verilerin korunması ve yapay zekâ*. [Yayınlanmamış yüksek lisans tezi]. İstanbul Üniversitesi.

Kaya, C. (2011). Avrupa birliği veri koruma direktifi ekseninde hassas (kişisel) veriler ve işlenmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, LXIX*(1-2), 317-334.

Kaya, M. B. (2020). Kişisel verilerin korunmasında yeni paradigma: Hesap verebilirlik ilkesi. *İstanbul Hukuk Fakültesi Mecmuası*, 78(4), 1859-1897. DOI: 10.26650/mecmua.2020.78.4.0005.

Keser, L. (2018). General data protection regulation (GDPR) ve uygulanması. İstanbul Bilgi Üniversitesi. https://cdn2.hubspot.net/hubfs/5089999/Mdsap_2019/PDF/SolutionPDF-1152018123643.pdf

Korucu, O. (2021). *Veri güvenliğinin iyileştirilmesi sürecinde risk tabanlı küresel standart, çerçeve ve en iyi uygulama yaklaşımları*. [Yayınlanmamış yüksek lisans tezi]. İstanbul Bilgi Üniversitesi.

Küzeci, E. (2019). *Kişisel verilerin korunması*, Ankara: Turhan Kitabevi.

KVK Kurumu. (2018). *Kişisel veri güvenliği rehberi (teknik ve idari tedbirler).* https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf.

KVK Kurumu. (2020). *Veri sorumluları için bağlayıcı şirket kurallarında bulunması gereken temel hususlara ilişkin yardımcı doküman*. https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU.

Özkan, O. (2020). *Kişisel verilerin korunması*. [Yayınlanmamış yüksek lisans tezi]. Ankara Üniversitesi.

Sarı, O. (2013). *Uluslararası hukuk ve Türk ceza hukuku bağlamında siber güvenlik ve bilişim sistemine yönelik suçlar*. [Yayınlanmamış yüksek lisans tezi]. Harp Akademileri Stratejik Araştırmalar Enstitüsü, İstanbul.

Taştan, F. G. (2017). *Türk sözleşme hukukunda kişisel verilerin korunması*, İstanbul: On İki Levha Yayıncılık.

Zor, A. (2020). *Veri sorumlusunun yükümlülükleri ve bu yükümlülüklerin ihlalinden doğan özel hukuk sorumluluğu.* [Yayınlanmamış yüksek lisans tezi]. İstanbul Üniversitesi.