Muhasebe ve Finansman Dergisi – 2025 Temmuz (107): 173-202

ISSN: 2146-3042
DOI: 10.25095/mufad.1642395

Dijital Çağda Muhasebe Güvenliği: Kişisel Verilerin Korunması Kanunu İhlallerinin Anatomisi*

Hakkı KIYMIK**

ÖZET

Bu çalışmanın amacı, Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında 2018-2024 yılları arasında Kişisel Verileri Koruma Kurumu veri ihlali bildirimi platformuna bildirilen 259 adet veri ihlal vakasını analiz ederek, özellikle mali müşavirlik sektörü başta olmak üzere muhasebe sistemlerini hedef alan ihlallerin nedenlerini, etkilerini ve çözüm önerilerini ortaya koymayı amaçlamaktadır. Bu amaç doğrultusunda, elde edilen veriler Excel programında sistematik olarak düzenlenerek veri ihlallerinin sektörel dağılımı, sıklığı, etkileri ve muhasebe sistemleri üzerindeki riskleri içerik analizi yöntemiyle incelenmiştir. Çalışmanın sonucunda, ihlallerin büyük çoğunluğunun siber saldırılar ve yetkisiz erişimler sonucu gerçekleştiği, fatura bilgileri, borç-alacak bakiyeleri ve resmi defterler gibi finansal verilerin de bu ihlallerden etkilendiği tespit edilmiştir. Bu durum, kurumların siber güvenlik altyapılarını güçlendirmesi, siber saldırıların erken tespitinin sağlanması, müdahale mekanizmaları geliştirmesi ve çalışan eğitimleri ile iç kaynaklı zafiyetleri en aza indirmesi gerektiğini ortaya koymaktadır.

Anahtar Kelimeler: *Muhasebe Sistemleri, Kişisel verilerin Korunması, Veri İhlali*

JEL Sınıflandırması: *K38, M40, M49*

Accounting Security in the Digital Age: Anatomy of PDPL Breaches

ABSTRACT

The purpose of this study is to analyze 259 data breach cases reported to the PDPL data breach notification platform between 2018 and 2024 within the scope of the Personal Data Protection Law (PDPL), and aims to reveal the causes, effects and solutions of breaches targeting accounting systems, especially the financial consultancy sector. For this purpose, the data obtained were systematically organized in Excel and the sectoral distribution, frequency, effects and risks of data breaches on accounting systems were examined by content analysis method. As a result of the study, it was determined that the vast majority of breaches occur as a result of cyber-attacks and unauthorized access, and financial data such as invoice information, debit-credit balances and official ledgers are also affected by these breaches. This situation reveals that organizations should strengthen their cyber security infrastructure, ensure early detection of cyber attacks, develop response mechanisms and minimize internal vulnerabilities through employee training.

Keywords: *Accounting Systems, Personal Data Protection, Data Breach*

Jel Classification: *K38, M40, M49*

Makale Gönderim Tarihi: 18.02.2025, **Makale Kabul Tarihi**: 13.05.2025, **Makale Türü:** Araştırma Makalesi

**Dr., Isparta Uygulamalı Bilimler Üniversitesi, Büyükkutlu Uygulamalı Bilimler Fakültesi, hakkikiymik12@gmail.com, ORCID:0000-0003-4695-1592

1. GİRİŞ

Günümüzde dijitalleşmenin hız kazanmasıyla birlikte kişisel verilerin korunması, işletmeler ve bireyler açısından kritik bir öneme sahip olmaktadır. Dijital dönüşüm sürecinde, işletmeler giderek daha fazla veriyi elektronik ortamda saklamakta ve işlemektedir. Özellikle muhasebe sistemleri, büyük miktarda kişisel ve finansal veri barındırmakta olup bu durum veri güvenliği risklerini artırmaktadır (Achar, 2018: 60-61). Kişisel verilerin kötüye kullanımı, siber saldırılar, veri sızıntıları ve yetkisiz erişimler, yalnızca bireylerin mahremiyetini ihlal etmekle kalmaz; aynı zamanda işletmeler için ciddi hukuki ve mali yükümlülükler doğurmakla birlikte kurumsal itibarın zedelenmesine de yol açmaktadır (Tao vd., 2019:661)

Kişisel verilerin korunmasına yönelik yasal düzenlemeler, bireylerin mahremiyet haklarını güvence altına alırken, veri sorumlularına da çeşitli yükümlülükler getirmektedir. Türkiye'de kişisel verilerin korunması ve işlenmesi konusundaki temel hukuki çerçeve, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile belirlenmiştir. 24 Mart 2016 tarihinde kabul edilen KVKK, Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR- General Data Protection Regulation) ile benzerlik göstermekte olup, veri sorumlularına ciddi yükümlülükler getirmektedir (Dilsiz, 2021:3-5). KVKK kapsamında, veri işleme faaliyetlerinin hukuka uygun olması, veri güvenliğinin sağlanması, veri ihlallerinin tespit edilmesi ve bildirim yükümlülüğünün yerine getirilmesi zorunluluğu bulunmaktadır (KVKK Faaliyet Raporu, 2023: 11).

Muhasebe süreçleri, doğası gereği büyük miktarda kişisel ve finansal veri içermektedir. İşletmelerin mali kayıtları, çalışan maaş bilgileri, müşteri ve tedarikçi bilgileri gibi unsurlar, muhasebe kayıtlarında yer almakta ve bu nedenle verilerin korunması büyük önem arz etmektedir (Perwej vd., 2021; Lois vd., 2021). Ayrıca bu verilerin güvenliğinin sağlanması hem mesleki bir sorumluluk hem de yasal bir zorunluluk meydana getirmektedir. (Civelek ve Durukan, 1998:132).

Müşteriler ve paydaşlar, finansal verilerinin gizliliği, bütünlüğü ve doğruluğu konusunda muhasebe sistemlerine güven duymaktadır. Ancak giderek daha karmaşık ve sofistike hale gelen veri ihlal vakalarına neden olan siber tehditler, muhasebe alanında güçlü veri güvenliği önlemlerinin uygulanmasını zorunlu kılmaktadır. Bu nedenle, muhasebede veri

ihlal vakalarının önlenmesi sadece bir tedbir değil, aynı zamanda finansal bilgilerin güvenilirliğini ve sürdürülebilirliğini sağlamak için de kritik bir gereklilik haline gelmiştir (Smith ve Rupp, 2002:179).

Bu kapsamda çalışmanın amacı, KVKK'ya bildirilen veri ihlal vakalarını sistematik bir şekilde inceleyerek, özellikle mali müşavirlik sektörü odaklı olmak üzere, farklı endüstrilerdeki muhasebe sistemlerini hedef alan siber güvenlik ihlallerini analiz etmek ve bu tür ihlallerin önlenmesine yönelik stratejik çözüm önerileri geliştirmektir. Çalışmanın kapsamını, KVKK'nın resmi internet sitesinden temin edilen veri ihlali bildirimleri oluşturmaktadır. Bu veriler Excel programında kronolojik olarak düzenlenmiş ve kurum bilgisi, sektör, ihlal kaynağı, ihlal türü, etkilenen kişi sayısı gibi kategoriler altında sınıflandırılarak içerik analizi yöntemiyle incelenmiştir. Bu analizler, veri ihlallerinin sektörel dağılımı, sıklığı ve muhasebe sistemleri üzerindeki etkilerini ortaya koymayı hedeflemektedir. Türkiye'de muhasebe sektöründeki veri güvenliği sorunlarını kapsamlı ve metodolojik bir yaklaşımla ele alan bu araştırma, alanında öncü nitelik taşımaktadır.

2. VERİ İHLAL TÜRLERİ

Kişisel verilerin güvenliğinin sağlanamaması durumunda ortaya çıkan ihlaller, niteliğine göre farklı kategorilerde değerlendirilmektedir. Bu kategoriler, ihlalin kaynağına, yöntemine ve veri üzerindeki etkisine göre sınıflandırılmaktadır (KVKK, 2023:11). En yaygın ihlal türlerinden biri olan siber saldırılar, dış kaynaklı tehditler arasında yer almakta ve genellikle kötü amaçlı yazılım, fidye yazılımı ya da hizmet reddi (DDoS) gibi tekniklerle gerçekleştirilmektedir (Perwej vd., 2021: 670; Smith ve Rupp, 2002:179). Bu tür saldırılar sonucunda sistemler kilitlenmekte, veriler şifrelenmekte ya da tamamen yok edilmektedir. Yetkisiz erişim, kurum içinden veya dışından gelen aktörlerin uygun erişim yetkisi olmadan veri sistemlerine giriş yaparak kişisel verilere ulaşması durumudur. Bu durum sıklıkla zayıf parola politikaları ya da açık güvenlik protokolleri nedeniyle meydana gelmektedir (Lois vd., 2021:27).

Yetkisiz ifşa, kişisel verilerin veri sorumlusunun bilgisi dahilinde olmadan, üçüncü kişilere açıklanması veya paylaşılmasıdır. Bu durum, genellikle kurum içi dikkatsizlik veya yetersiz prosedürlerden kaynaklanmaktadır (Kutlu ve Kahraman, 2017:52). Veri kaybı ve

silinme, sistem arızaları, siber saldırılar ya da kullanıcı hataları sonucunda verilerin tamamen veya kısmen ortadan kalkmasıyla sonuçlanmaktadır. Bu durum yalnızca operasyonel işleyişi aksatmakla kalmaz, aynı zamanda hukuki ve finansal riskleri de beraberinde getirir (Świetla, 2019:63). Veri bütünlüğünün bozulması ise verilerin kasıtlı ya da kasıtsız şekilde değiştirilmesiyle, doğruluğu ve güvenilirliğinin zedelenmesi anlamına gelmektedir. Bu tür ihlaller, özellikle muhasebe sistemleri gibi verinin kesinliğine dayalı alanlarda büyük risk oluşturmaktadır (Achar, 2018:61).

3. VERİ İHLALLERİNİN NEDENLERİ VE ÇÖZÜM YOLLARI

Veri ihlalleri, kuruluşların ve bireylerin güvenliğini tehdit eden ciddi bir sorundur. Veri ihlalleri genellikle teknik zafiyetler, insan hataları ve kötü niyetli saldırılar gibi çeşitli nedenlerden kaynaklanır. Teknik zafiyetler arasında yetersiz şifreleme, güncellenmemiş yazılımlar veya zayıf ağ güvenliği yer almaktadır. Nitekim Verizon'un 2023 Veri İhlali Raporu'na göre, ihlallerin %49'u sistemlerin gerekli güvenlik güncellemelerinin zamanında yapılmamasından kaynaklanmıştır (Verizon, www.verizon.com,2023). Öte yandan, insan kaynaklı hatalar da önemli bir risk unsurudur. Özellikle çalışanların kimlik avı (phishing) saldırılarına karşı savunmasız olması ve zayıf şifre tercihleri, IBM Security'nin 2023 yılı raporuna göre ihlallerin %74'ünde etkili olmuştur (IBM Security, www.ibm.com, 2023). Bu durum, hem teknik hem de insan kaynaklı risklerin birleştiğinde nasıl büyük tehditler oluşturabileceğini gösterir.

Dış kaynaklı tehditler, özellikle siber suçlular tarafından gerçekleştirilen hedefe yönelik saldırılar, veri ihlallerinin başlıca nedenlerinden biridir. Fidye yazılımları ve veri sızıntısı gibi saldırı türleri, özellikle finans ve sağlık gibi hassas verilerin yoğun şekilde işlendiği sektörlerde sıkça görülmektedir. ENISA'nın 2023 Tehdit Görünümü Raporu'na göre, kötü niyetli saldırılar veri ihlallerinin %50'sinden fazlasını oluştururken, bu saldırıların çoğu kimlik avı ve sosyal mühendislik teknikleriyle gerçekleştirilmektedir. Bununla birlikte, iç kaynaklı tehditler de önemli bir risk unsuru oluşturmaktadır; çalışanların kasıtlı ya da farkında olmadan gerçekleştirdiği veri sızıntıları, ihlallerin %20'sinden fazlasına neden olmaktadır. Bu doğrultuda, kuruluşların hem ileri düzey teknolojik çözümlerden faydalanmaları hem de çalışanlara yönelik sürekli eğitim ve farkındalık programları uygulamaları, veri güvenliğini sağlamak açısından kritik önem taşımaktadır (ENISA, www.enisa.europa. 2023).

Veri ihlallerinin etkin bir biçimde önlenmesi, teknik, organizasyonel ve insan faktörüne dayalı çözümlerin bütüncül bir şekilde uygulanmasını gerektirmektedir. Teknik önlemler kapsamında; güçlü şifreleme algoritmalarının kullanımı, sistemlerin düzenli olarak güncellenmesi ve çok faktörlü kimlik doğrulama (MFA- multi-factor authentication)) gibi güvenlik katmanlarının entegre edilmesi önem arz etmektedir. Kişisel Verileri Koruma Kurumu'nun 2023 yılı Teknik Rehberi'nde de belirtildiği üzere, veri güvenliğinin sağlanmasında şifreleme teknolojileri ve erişim kontrol mekanizmalarının etkin bir şekilde uygulanması zorunlu görülmektedir. Bunun yanı sıra, çalışanların siber güvenlik konusundaki farkındalık düzeylerinin artırılması da ihlallerin önlenmesinde kritik bir rol oynamaktadır.

Kişisel veri güvenliğinin sağlanması için hem idari hem de teknik düzeyde bütüncül önlemler alınması gerekmektedir. İdari tedbirler kapsamında mevcut risk ve tehditlerin belirlenmesi, çalışanların siber güvenlik farkındalığının artırılması, veri güvenliği politikalarının oluşturulması ve yalnızca gerekli verilerin işlenmesine özen gösterilmesi önem arz etmektedir. Ayrıca, veri işleyen üçüncü taraflarla ilişkilerin dikkatle yönetilmesi de veri güvenliğinin bir diğer temel unsurudur. Teknik tedbirler ise siber güvenliğin sağlanması, verilerin güvenli ortamlarda saklanması, erişim kontrollerinin uygulanması ve sistemlerin düzenli yedeklenmesini kapsamaktadır. Bulut sistemlerinin güvenli kullanımı ve bilgi teknolojilerinin güvenli şekilde tedarik edilip yönetilmesi de bu önlemler arasındadır. Bu idari ve teknik uygulamaların uyum içinde yürütülmesi, Kişisel Verileri Koruma Kurumu kapsamındaki yükümlülüklerin yerine getirilmesi ve veri ihlallerinin önlenmesi açısından hayati önemdedir (Kişisel Verileri Koruma Kurumu, 2023).

4. LİTERATÜR TARAMASI

Kişisel verilerin korunmasına ilişkin literatürde çeşitli akademik çalışmalar mevcut olmakla birlikte, özellikle KVKK kapsamında gerçekleştirilen veri ihlali bildirimlerinin sistematik analizini konu alan çalışmalara rastlanmamıştır. Kişisel verilerin korunması kapsamında yapılan bazı akademik çalışmalar aşağıda verilmiştir.

Kauffman, vd. (2011) çalışmasında, muhasebe bilgi sistemleri (AIS-Accounting Information System) perspektifinden tüketici bilgi gizliliğini incelemeyi amaçlamaktadır. Çalışmada, bilgi gizliliğiyle ilgili mevcut literatür analiz edilerek, tüketicilerin kişisel

verilerinin nasıl işlendiğini, korunduğunu ve bu süreçlerin muhasebe bilgi sistemleriyle nasıl ilişkili olduğu değerlendirmektedir. Çalışmanın sonucunda, tüketici bilgi gizliliğini sağlamaya yönelik etkili muhasebe ve güvenlik politikalarının geliştirilmesi gerektiği belirtilmiş ve veri koruma süreçlerinin hem etik hem de yasal açıdan muhasebe uygulamaları üzerindeki etkileri tartışılmıştır.

Kılınç (2012) çalışmasında, kişisel verilerin korunmasını anayasal bir hak olarak ele almış ve bu çerçevede hukuki düzenlemeleri incelemiştir. Çalışmada, ulusal ve uluslararası mevzuat çerçevesinde konuya dair karşılaştırmalı bir analiz yapılmıştır. Çalışmanın sonucunda, kişisel verilerin korunmasının sadece bireysel mahremiyet açısından değil, aynı zamanda demokratik hukuk devletinin temel unsurlarından biri olarak ele alınması gerektiği de ortaya konmaktadır.

Çetin (2014) çalışmasında, bireylerin kişisel veri güvenliğine yönelik tutumları ve farkındalık seviyelerini değerlendirmiş ve çeşitli demografik faktörlerin bu farkındalık üzerindeki etkilerini analiz etmiştir. Araştırmanın sonucuna göre, kullanıcıların kişisel veri güvenliği konusunda yeterli bilgiye sahip olmadıkları, ancak bu konudaki bilinç düzeylerinin eğitim seviyesi ve teknoloji kullanım alışkanlıklarıyla ilişkili olduğu tespit edilmiştir.

Atasoy (2016) çalışmasında, sosyal medya platformlarında kişisel verilerin toplanması, işlenmesi ve paylaşılması süreçlerini ele alarak, bu süreçlerin bireylerin mahremiyet hakkı üzerindeki etkilerini incelemiştir. Ayrıca, veri sahibinin rızasının hukuki boyutunu, Avrupa Birliği ve Türk hukuku bağlamında karşılaştırmıştır. Çalışmanın sonucunda, kişisel verilerin korunmasına yönelik mevcut hukuki düzenlemelerin sosyal medya dinamikleri karşısında yetersiz kalabildiği, bu nedenle daha etkin yasal düzenlemelerin yapılması gerektiği ortaya konmuştur.

Kutlu ve Kahraman (2017) çalışmalarında, KVKK'nın uygulanma sürecini, yasal çerçevesini ve bu alandaki mevcut durum ile karşılaşılan sorunları inceleyerek Avrupa Birliği mevzuatıyla karşılaştırmalı olarak değerlendirmişlerdir. Çalışmanın sonucunda, Türkiye'de veri koruma politikalarının gelişmekte olduğu, ancak yasal düzenlemelerin etkinliğini artırmak için denetim mekanizmalarının güçlendirilmesi ve farkındalık çalışmalarının yapılması gerektiği tespit edilmiştir.

Stanciu ve Rîndaşu (2018) çalışmalarında, Avrupa Birliği Genel Veri Koruma Yönetmeliği'nin (General Data Protection Regulation-GDPR) muhasebe mesleği üzerindeki etkilerini incelemişlerdir. Araştırmada, Romanya'daki muhasebe profesyonelleri açısından GDPR'nin getirdiği yükümlülükler ve karşılaşılan zorlukları ele alınmaktadır. Çalışmanın sonucunda, GDPR'nin muhasebe süreçlerinde veri koruma farkındalığını artırdığı, ancak işletmeler için ek maliyetler ve operasyonel zorluklar ortaya çıkardığı tespit edilmiştir.

Świetla (2019) çalışmasında, muhasebe süreçlerinde kişisel veri işleme uygulamalarını analiz ederek, GDPR'nin getirdiği yükümlülüklerin muhasebe sistemleri üzerindeki etkisini incelemiştir. Ayrıca, muhasebe meslek mensuplarının ve işletmelerin, veri koruma düzenlemelerine uyum sağlamak için karşılaştıkları zorlukları da ele almaktadır. Çalışmanın sonucunda, muhasebe alanında GDPR'ye uyum sağlamanın yalnızca hukuki bir gereklilik olmadığı, aynı zamanda veri güvenliğini artırarak işletmelerin itibarı ve operasyonel güvenliği için de kritik bir unsur olduğu ortaya konmuştur.

Deniz (2020) çalışmasında, KVKK ile arabuluculuk süreçlerinde gizliliğin nasıl bir arada işlediğini analiz ederek, bu iki yasal çerçevenin uyumunu ve karşılaşılan potansiyel sorunları incelemiştir. Çalışmanın sonucunda, arabuluculuk süreçlerinde kişisel verilerin korunmasına yönelik ilkelere uyum sağlamak için belirli düzenlemelerin ve pratik yaklaşımların geliştirilmesi gerektiği tespit edilmiştir.

Büyükarıkan, vd., (2021) çalışmalarında, muhasebe öğrencilerinin KVKK'ya yönelik bilgi ve bilinç seviyelerini yani farkındalık düzeylerini ölçmeyi hedeflemişlerdir. Ayrıca, bu farkındalık düzeyini çeşitli demografik faktörlere göre değerlendirilmiştir. Araştırmanın sonucunda, öğrencilerin KVKK hakkında genel bir bilgiye sahip oldukları ancak kanunun uygulama ve detayları hakkında eksiklikler bulunduğu görülmektedir.

Ertan (2022) çalışmasında, nesnelerin interneti (IoT-Internet of Things) cihazlarının veri toplama, işleme ve paylaşma süreçlerinin kişisel veri güvenliği açısından taşıdığı riskleri analiz etmiş ve bu teknolojilerin kullanıcıların mahremiyetini nasıl tehdit edebileceğine dair kapsamlı bir değerlendirmede bulunmuştur. Çalışmanın sonucunda, bu teknolojilerin kişisel verilerin korunması konusunda mevcut yasal düzenlemelerle uyumsuzluklar oluşturabileceği ve güvenlik açıklarını artırabileceği tespit edilmiştir.

Sevindi ve Ordu (2023) çalışmalarında, Avrupa Birliği (AB) ve Türk hukukunda veri ihlallerinin tespiti ve bildirim sürelerini karşılaştırmalı olarak analiz etmişlerdir. Çalışmanın sonucunda, AB ve Türk hukukundaki farklılıklar ortaya konmaktadır. Ayrıca çalışma, Türkiye'deki veri ihlali bildirim süreçlerinin AB standartlarına uyum sağlayabilmek adına bazı iyileştirmelere ihtiyaç duyduğu ortaya çıkmıştır.

Eralp (2023) çalışmasında, işyerlerinde kişisel sağlık verilerinin işlenmesi sürecinde sırrın saklanması yükümlülüğünün hukuki çerçevesini incelemiştir. Ayrıca, işverenlerin çalışanlarının sağlık verilerini işleme ve bu verilerin korunması hakkındaki yasal sorumluluklarını da ele almıştır. Çalışmanın sonucunda, işyerlerinde sağlık verilerinin korunmasına yönelik mevcut hukuki yükümlülüklerin ve uygulamaların güçlendirilmesi gerektiğini tespit edilmiştir.

Literatürde yer alan çalışmalar genellikle veri koruma mevzuatının hukuki boyutları, tüketici farkındalığı ve genel veri güvenliği gibi konulara odaklanırken, bu çalışma, muhasebe sistemlerindeki veri ihlallerinin nedenlerini, etkilerini ve yaygınlığını somut örneklerle ortaya koyarak sektörel bir perspektif sunmaktadır. Ayrıca, bu ihlallerin önlenmesi ve etkilerinin azaltılması için etkili çözüm önerileri sunmayı amaçlamaktadır. Bu bağlamda, çalışma, literatürdeki boşluğu doldurarak, veri ihlallerinin muhasebe sistemleri üzerindeki etkilerini anlamaya ve bu alanda etkili politikalar geliştirilmesine yönelik önemli bir adım teşkil etmektedir.

5. ARAŞTIRMANIN AMACI, YÖNTEMİ VE KAPSAMI

Bu çalışmanın temel amacı, Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında bildirilen veri ihlali vakalarını sistematik bir şekilde inceleyerek, özellikle mali müşavirlik sektörü başta olmak üzere çeşitli sektörlerde muhasebe sistemlerini hedef alan siber saldırıların ve veri ihlallerinin analizini yapmaktır. Bu analizler ışığında, söz konusu ihlallerin nedenleri, etkileri ve yaygınlığını ortaya koyarak, bu tür vakaların önlenmesine ve azaltılmasına yönelik etkili çözüm önerilerinin sunulması hedeflenmiştir.

Bu amaç doğrultusunda çalışmanın kapsamını, Kişisel Verileri Koruma Kurumu resmi internet sitesinde yer alan https://www.kvkk.gov.tr/veri-ihlali-bildirimi/ adresinden temin

edilen ve 2018-2024 yılları arasında bildirilmiş olan 259 veri ihlali vakası oluşturmaktadır. Bu vakaların 25 tanesi muhasebe sistemleri ve mali müşavirlik sektörü ile doğrudan ilişkili olup, çalışmada bu 25 vakaya ayrıca odaklanılmıştır.

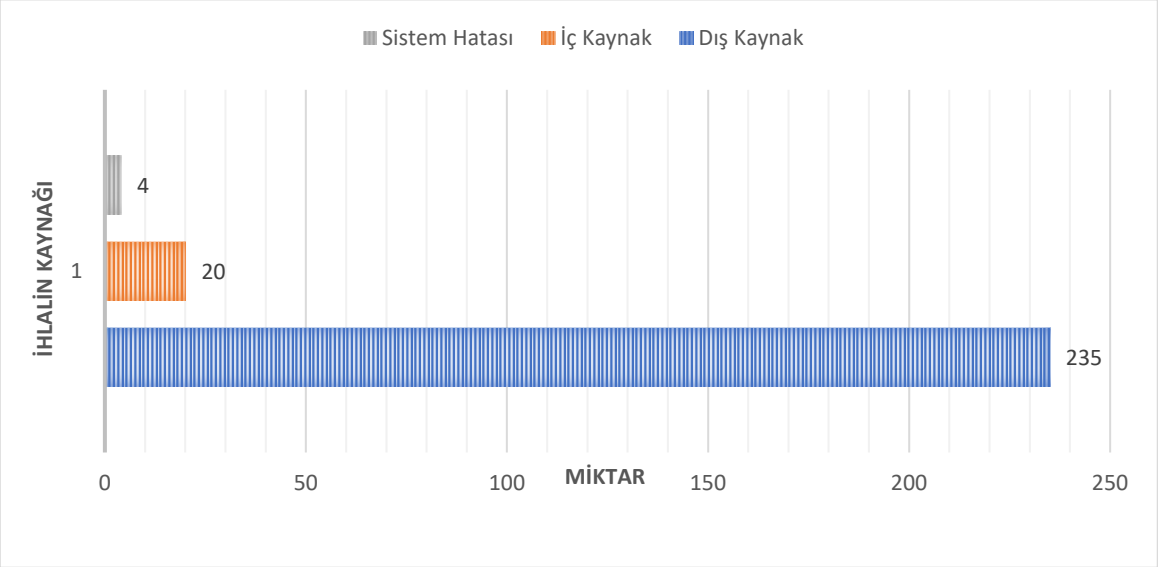
Çalışmanın yöntemi kapsamında, Kişisel Verileri Koruma Kurumu tarafından sağlanan veri ihlali bildirimleri, Excel programı üzerinde sistematik bir şekilde düzenlenmiş ve içerik analizi yöntemiyle analiz edilmiştir. Veriler, kronolojik bir sırayla tasniflenerek aşağıdaki kategoriler altında sınıflandırılmıştır:

- **Veri Sorumlusu Bilgisi**: İhlalin gerçekleştiği kurumun adı,
- **Veri Sorumlusu Türü**: Kurumun özel sektör, kamu veya vakıf olma durumu,
- **Sektör**: Kurumun faaliyet gösterdiği sektör,
- **Bildirim Tarihi**: İhlalin bildirildiği tarih,
- **Etkilenen Kişi Sayısı**: İhlalden etkilenen bireylerin sayısı,
- **İhlalin Kaynağı**: İhlale neden olan kaynak (İç Kaynak, Dış Kaynak, Sistem Hatası),
- **İhlalin Türü**: Gerçekleşen ihlalin niteliği (Siber Saldırı, Yetkisiz Erişim, Yetkisiz İfşa, Veri kaybı ve Silinme, Veri Bütünlüğünün Bozulması),
- **Kişisel Verilere Etkisi**: İhlalin kişisel veriler üzerindeki etkisi,
- **Muhasebe Sistemlerine Etkisi**: İhlalin muhasebe sistemleri üzerindeki olası etkileri.

Bu kategoriler üzerinden yapılan analizler, veri ihlallerinin sektörel dağılımı, sıklığı, etkileri ve muhasebe sistemleri üzerindeki risklerin anlaşılmasına yönelik nicel ve nitel değerlendirmeler sunmayı amaçlamaktadır.

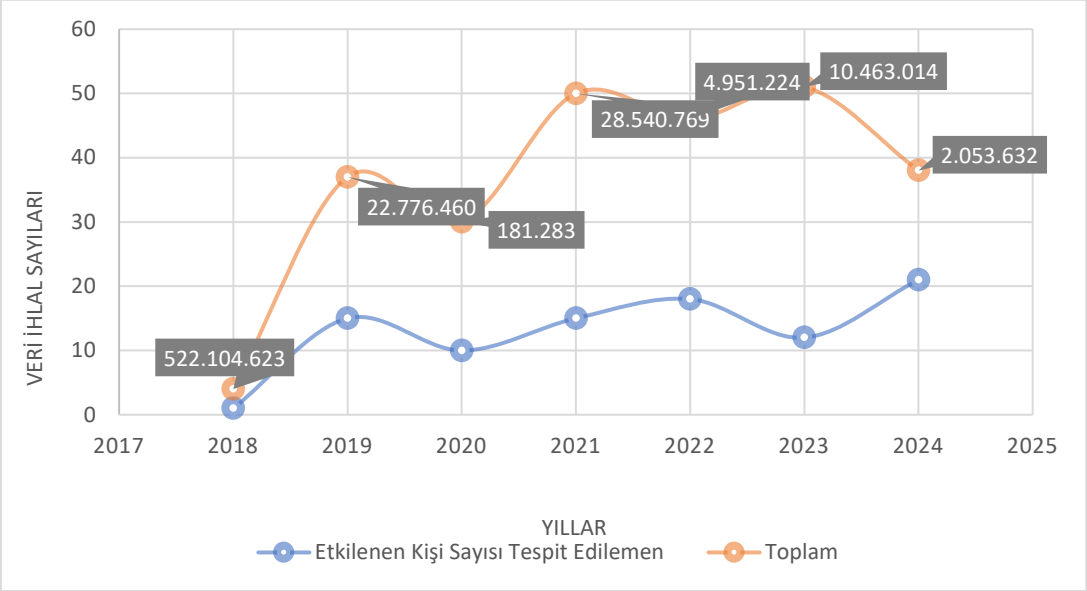
6. ARAŞTIRMANIN BULGULARI

Şekil 1'de, KVKK kapsamında gerçekleşen veri ihlallerinin kaynaklara göre dağılımı gösterilmektedir. Toplamda üç ana kaynak kategorisinde (dış kaynak, iç kaynak ve sistem hatası) 259 adet veri ihlali gerçekleşmiştir. Söz konusu veri ihlallerinin büyük çoğunluğu 235 adet olmak üzere dış kaynaklı unsurlardan kaynaklanmıştır. İç kaynaklardan ve sistem hatalarından kaynaklanan veri ihlalleri ise sırasıyla 20 ve 4 adet olarak gerçekleşmiştir.



Şekil 1. İhlalin Kaynağı

Analiz sonuçlarından da anlaşılacağı üzere veri ihlallerinin büyük çoğunluğu siber saldırılar, kötü amaçlı yazılımlar veya üçüncü tarafların yetkisiz erişimleri gibi dış kaynaklı unsurlardan meydana gelmektedir. Bu durum, kurumların siber güvenlik önlemlerini geliştirmesi ve dış unsurlardan kaynaklanan tehditlere karşı daha etkili savunma mekanizmaları geliştirmesi gerektiğini göstermektedir. İç unsurlardan kaynaklanan veri ihlalleri ise daha az sayıda olmakla birlikte kurum içi politika ve prosedürlerin gözden geçirilerek etkinleştirilmesi gerektiğini, çalışanların eğitim ve bilinçlendirilmesi gibi ek önlemlerin alınması gerektiğini göstermektedir. Teknik altyapı sorunları ve etkin olmayan sistem yönetimi gibi nedenlerden dolayı sistem hatalarından kaynaklanan veri ihlalleri ise altyapının ve sistem yönetimin sürekli güncellenerek iyileştirmeler yapılması gerektiğini göstermektedir.

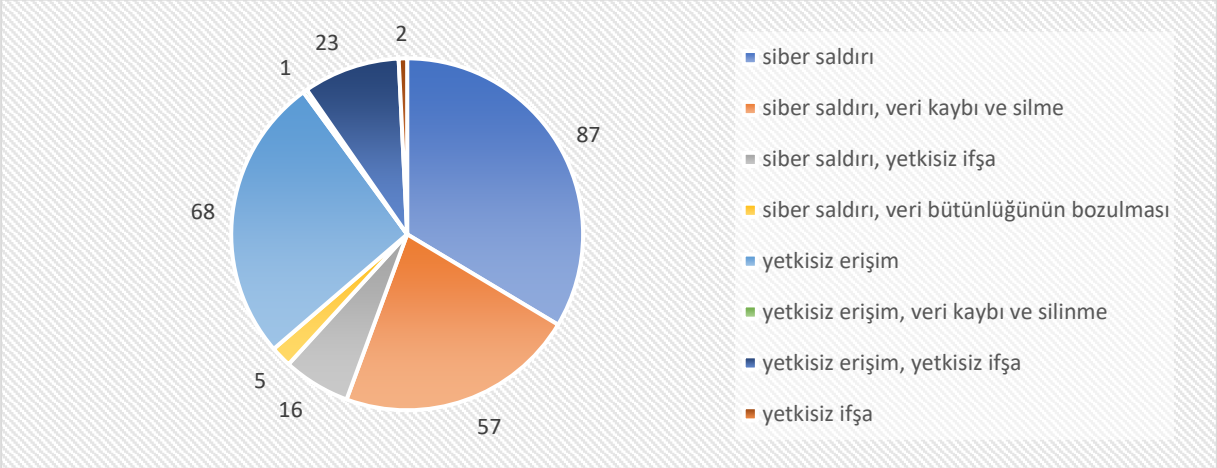


Şekil 2. Veri İhlalleri ve Etkilenen Kişi Sayıları

Şekil 2'de, KVKK kapsamında gerçekleşen veri ihlallerinin yıllara göre dağılımı, veri sorumlusu tarafından etkilenen kişi sayısı tespit edilemeyen ihlal sayıları, toplam ihlal sayıları ve bu ihlallerden etkilenen kişi sayıları gösterilmiştir. Şekil 2'de sunulan grafik, 2018-2024 arası dönemi kapsamakta olup veri ihlallerinin hem sayısal hem de etki boyutunu analiz etmek için önemli verileri sunmaktadır.

Bildirimi yapılan toplam ihlal sayılı 2018 yılında 4 iken bu sayı 2023 yılında 51 düzeyine kadar yükselerek önemli bir artış göstermiştir. 2024 yılında ise 38 adet ihlal bildirimi yapılmıştır. Siber güvenlik tehditlerinin dinamik yapısını sunan bu dalgalanmalar, dijitalleşmenin yaygınlaşması ve veri kullanımının artmasıyla birlikte siber saldırıların da arttığını ve dolayısıyla veri ihlal sayılarının arttığını göstermektedir. Veri ihlallerinden en fazla etkilenen kişi sayısı 2018 yılında kaydedilmiş olup, toplamda 522.104.623 kişi veri ihlallerinden etkilenmiştir. Sonraki yıllarda bu sayı azalmış olmasına rağmen yıllar itibariyle dalgalanmalar göstermiştir. Veri ihlallerinden etkilenen kişi sayısı 2020 yılında 181.283'e düşmüş, 2021 yılında 28.540.769'a yükselmiş ve 2024 yılında ise 2.053.632'ye düşerek kayıtlara geçmiştir. Veri ihlallerinden etkilenen kişi sayılarındaki dalgalanmalar, gerçekleşen veri ihlallerinin niteliğine ve boyutuna bağlı olarak değişiklik göstermektedir. Bazı veri ihlallerinde ise yetersiz raporlama, eksik kayıtlar veya saldırının geç tespit edilmesi gibi nedenlerden ötürü etkilenen kişi sayısı tespit edilememiştir. 2018 yılında veri ihlalinden

etkilenen kişi sayısının tespit edilemediği ihlal sayısı 1 iken, 2024 yılında bu sayı 21'e yükselmiştir. 2019, 2020, 2021, 2022 ve 2023 yıllarında ise etkilenen kişi sayısının tespit edilemediği ihlal sayıları sırasıyla 15, 10, 15, 18 ve 12 olarak kayda geçmiştir. Bu ihlallerde etkilenen kişi sayısının tespit edilememesi, ihlallerin gerçek boyutunu ve etkisini tam olarak anlamayı zorlaştırmaktadır. Bu durum, hem bireylerin kişisel verilerinin ne ölçüde risk altında olduğu konusunda belirsizliği artırmakta hem de kurumların ihlallerin etkisini değerlendirme ve gerekli önlemleri alma süreçlerini daha da zorlaştırmaktadır.



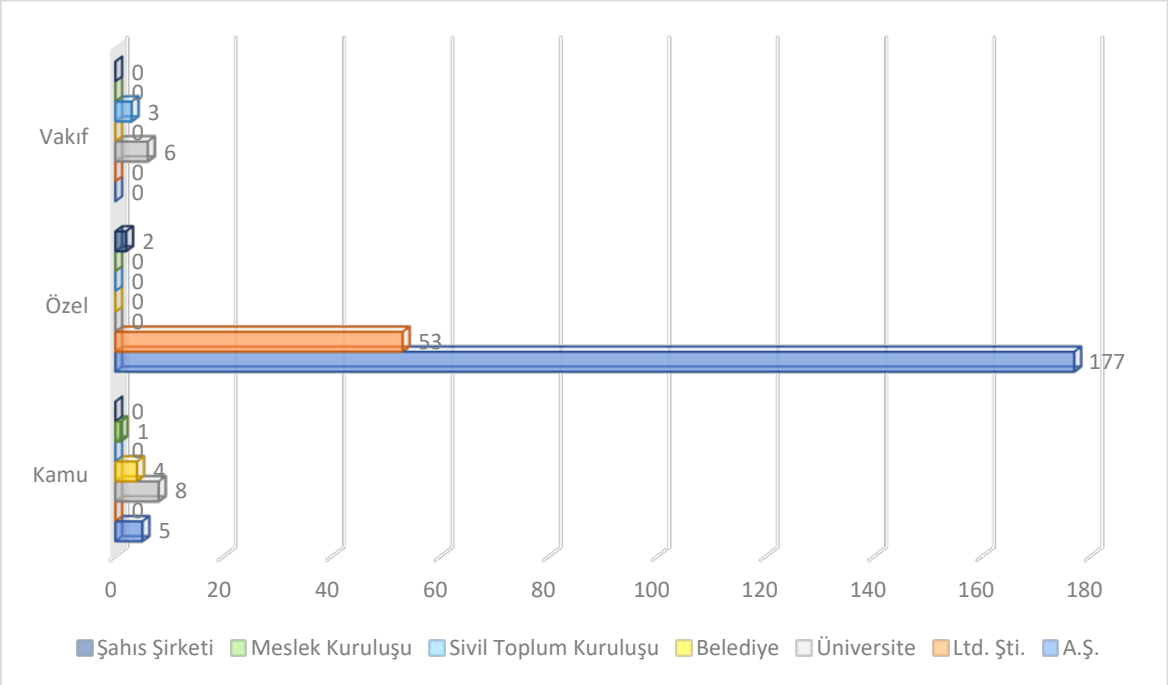
Şekil 3. Veri İhlallerinin Türü

Şekil 3'te KVKK kapsamında gerçekleşen veri ihlallerinin türleri ve bu ihlallerin niteliklerine göre dağılımı gösterilmiştir. Şekil 3'te sunulan ihlallerin türleri ve sayıları, veri güvenliği açısından hangi alanların daha fazla risk taşıdığını ve hangi ihlal türlerinin daha yaygın olduğunu göstermektedir.

Grafikten de görüldüğü üzere, 2018-2024 arası dönemde 87 adet siber saldırı gerçekleşmiştir. Bu durum, siber saldırıların veri sorumluları için en büyük tehditlerden biri olduğunu göstermektedir. Siber saldırılar, genellikle kötü amaçlı yazılımlar, fidye yazılımları veya dağıtılmış hizmet reddi (hizmet reddi (Distributed denial of service- DDoS)) saldırıları saldırıları gibi yöntemlerle gerçekleştirilmektedir. Siber saldırılar sonucunda, saldırganlar sadece verilere ulaşmakla kalmamıştır aynı zamanda ciddi veri kayıplarına da neden olmuşlardır. Bu saldırılar sonucunda 57 adet veri kaybı ve silme olayı, 16 adet elde edilen verilerin yetkisiz şekilde ifşa edilmesi olayı ve 5 adet de elde edilen verilerin doğruluğunun ve güvenilirliğinin zedelendiği veri bütünlüğünün bozulması olayı gerçekleşmiştir.

Siber saldırılardan sonra en fazla gerçekleşen veri ihlal türü ise yetkisiz erişimdir. 2018-2024 arası dönemde yetkisiz erişim sonucu 68 adet veri ihlali gerçekleşmiştir. Bu ihlal türü genellikle zayıf parola politikaları, güvenlik açıkları veya iç tehditlerden kaynaklanmaktadır. Yetkisiz erişim sonucunda 1 adet veri kaybı ve silme olayı gerçekleşirken, 23 adet yetkisiz ifşa olayı gerçekleşmiştir. Bu durum, kurumların siber güvenlik önlemlerini artırması ve özellikle erişim kontrol mekanizmalarını güçlendirmesi gerektiğini ortaya koymaktadır.

Siber saldırı ve yetkisiz erişim gibi dış tehditler dışında kalan, yalnızca verilerin ifşa edilmesiyle sonuçlanan veri ihlali vakalarının sayısı 2 olarak raporlanmıştır. Bu tür ihlaller genellikle kötü niyetli bir saldırıdan ziyade, çalışanların yaptığı hatalar, yanlış yapılandırılmış sistemler veya güvenlik protokollerine uyulmaması gibi insan kaynaklı faktörlerden kaynaklanmaktadır.



Şekil 4. Kurumların Türü ve Dağılımı

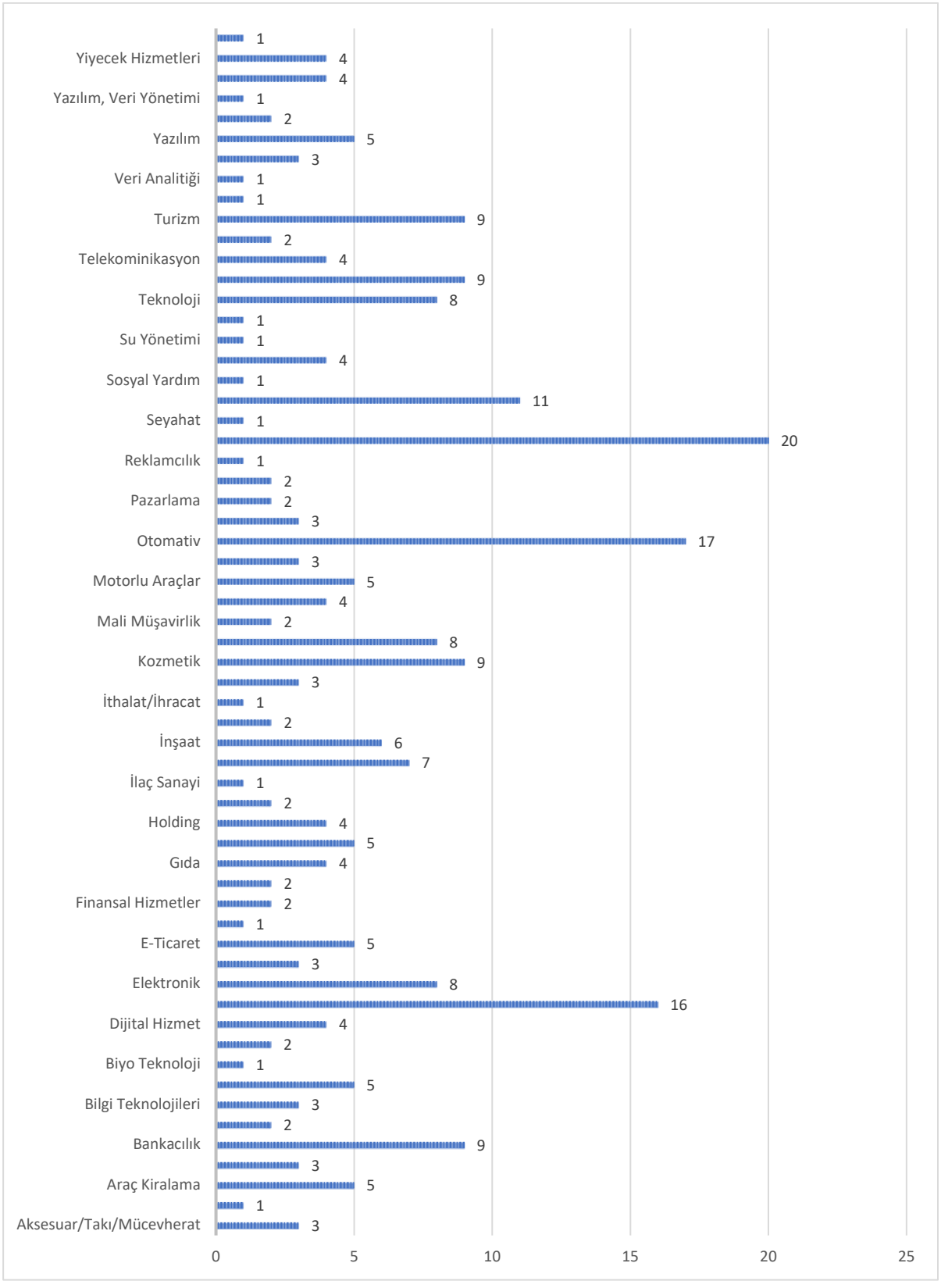
Şekil 4'te KVKK kapsamında gerçekleşen veri ihlallerinin kurum türlerine göre dağılımı gösterilmektedir. Şekil 4'te sunulan grafikte, farklı kurum türlerinde meydana gelen ihlallerin sayıları karşılaştırmalı olarak sunulmaktadır. Bu veriler, ihlallerin hangi tür

kurumlarda daha yaygın olduğunu ve sektörel bazda güvenlik açıklarının nerede yoğunlaştığını analiz etmek için önemli bir kaynak oluşturmaktadır.

Kamu sektöründe, veri ihlallerinin en çok üniversitelerde ve anonim şirket statüsündeki kamu kuruluşlarında gerçekleştiği görülmüştür. 2018-2024 arası dönemde Kamu üniversitelerinde 8 adet ihlal vakası gözlemlenirken, anonim şirket statüsündeki kamu kuruluşlarında ise 5 adet ihlal vakası gerçekleşmiştir. Üniversitelerdeki ihlallerin yüksek olması, bu kurumların bünyesinde barındırdığı büyük ölçekli öğrenci ve personel verileri ile siber güvenlik altyapılarının yetersiz oluşundan kaynaklanmaktadır.

Özel sektörde, veri ihlallerinin en çok anonim şirket statüsündeki firmalarda ve limited şirket statüsündeki firmalarda gerçekleştiği görülmüştür. 2018-2024 arası dönemde anonim şirket statüsündeki firmalarda 177 adet ihlal vakası gözlemlenirken, limited şirket statüsündeki firmalarda ise 53 adet ihlal vakası gerçekleşmiştir. Anonim ve limited şirket statüsündeki firmalarda ihlal vakalarının yüksek olması, bu firmaların sahip olduğu geniş müşteri portföyleri ve iş süreçlerinin dijitalleşmesiyle ilişkilidir. Ayrıca, bu tür şirketler siber saldırılar için daha cazip hedeflerdir. Şahıs firmalarındaki düşük veri ihlal vakaları bu durumu kanıtlar niteliktedir. Çünkü bu tür firmalar doğaları gereği daha küçük ölçeklidirler ve daha az veri işlerler. Ele alınan analiz sürecinde bildirimi yapılan veri ihlal vakaları ise 2 adettir.

Vakıf sektöründe ise veri ihlal vakaları en çok üniversitelerde ve sivil toplum kuruluşlarında gerçekleşmiştir. Sırasıyla ele alınan analiz sürecinde vakıf üniversitelerinde 6 adet veri ihlali, sivil toplum kuruluşlarında ise 3 adet veri ihlal vakası bildirimi yapılmıştır. Vakıf üniversitelerindeki gerçekleşen veri ihlallerinin nedenleri, kamu üniversitelerindeki veri ihlal nedenleriyle aynıdır. Sivil toplum kuruluşlarındaki ihlaller, bu kurumların genellikle sınırlı bütçelerle çalışması nedeniyle yeterli siber güvenlik yatırımı yapamamasıyla ilişkilidir.



Şekil 5. Veri İhlallerinin Sektörel Dağılımı

Şekil 5'te KVKK kapsamında gerçekleşen veri ihlallerinin sektörel bazda sayısal dağılımı gösterilmektedir. Şekil 5'te sunulan grafikte, hangi sektörlerin veri ihlallerine daha açık olduğu ve hangi alanlarda daha fazla önlem alınması gerektiği açısından önemli bir kaynak oluşturmaktadır.

Grafikten de anlaşılacağı üzere, 2018-2024 arası dönemde en fazla veri ihlaline maruz kalan üç sektör sırasıyla sağlık, otomotiv ve eğitimdir. Sağlık sektörü, 20 ihlal ile en yüksek sayıda veri ihlal vakası görülen sektördür. Sağlık sektörünün özel nitelikli kişisel verileri içermesi, bu sektörü siber saldırılara karşı daha cazip ve tercih edilebilir hale getirmiştir. Nitekim Karaçadır (2022) tarafından yapılan bir panel veri analizinde, OECD ülkelerinde internet kullanımının sağlık harcamalarıyla ilişkili olduğu gösterilmiştir. Bu durum, sağlık alanındaki dijital verilerin büyüklüğünü ve korunması gereken stratejik önemini ortaya koymaktadır. Otomotiv sektörü ise 17 ihlal ile en yüksek sayıda veri ihlal vakası görülen ikinci sektördür. Otomotiv sektörünün dijital dönüşüm süreci ve bağlı araç teknolojileri, bu sektörü siber saldırılara karşı daha açık hale getirmektedir. Nitekim Tanyılmaz ve Erten (2001), otomotiv sektörünün hem Türkiye'de hem de küresel ölçekte ekonomik büyüme ve dijitalleşmeyle nasıl dönüştüğünü ayrıntılı biçimde ele almışlardır. Bu dönüşüm, veri güvenliği politikalarının da sektörün stratejik öncelikleri arasına alınmasını gerekli kılmaktadır. Eğitim sektörü ise, 16 ihlal vakası ile üçüncü sırada yer almaktadır. Eğitim sektörü, özellikle üniversiteler, geniş öğrenci ve personel verisi barındırmaları nedeniyle kişisel verilerin işlenmesi açısından kritik kurumlardır. Artan dijitalleşme ile birlikte bu kurumlar da veri ihlallerine açık hale gelmiştir. Güneren Genç (2017) çalışmasında üniversitelerin ülkelerin gelişmişlik düzeyleriyle ilişkisini incelerken, bu kurumların stratejik önemini ve kamu güveni açısından taşıdığı rolü de vurgulamaktadır. Bu bağlamda üniversitelerdeki veri güvenliği uygulamaları, yalnızca bireysel mahremiyet açısından değil, kurumsal ve toplumsal kalkınma açısından da önem arz etmektedir.

Orta seviyede veri ihlal vakasına maruz kalan ilk üç sektör ise sırasıyla sigorta, tekstil ve turizmdir. Sigorta sektöründe 2018-2024 arası dönemde 11 adet veri ihlal vakası raporlanmıştır. Sigorta şirketleri, müşterilerinin kimlik bilgileri, sağlık kayıtları ve finansal verileri gibi önemli bilgileri barındırmasının yanı sıra, gerekli teknik ve idari tedbirleri almamaları durumunda bu verilerle ilgili güvenlik ihlalleri riski taşımaktadır. Nitekim Akhisar

ve Tezergil (2014) tarafından yapılan verimlilik analizi, Türk sigorta sektörünün performansını değerlendirirken, sektördeki teknolojik gelişmelerin etkisini de ortaya koymaktadır. Bu durum, veri güvenliği stratejilerinin sektörün dijitalleşme süreciyle birlikte ele alınmasını zorunlu kılmaktadır. Üretim ve perakende alanlarında faaliyet gösteren tekstil sektöründe ise 9 adet veri ihlal vakası gerçekleşmiştir. Bu sektörün, müşteri bilgileri, tedarik zinciri verileri ve ödeme sistemleri gibi hassas verileri içermesi, tekstil sektörünü siber saldırılar için daha cazip hale getirmektedir. Seyahat ve konaklama gibi faaliyetlerini bünyesinde barındıran turizm sektörü özelinde ise 9 adet veri ihlal vakası raporlanmıştır. Seyahat ve konaklama sektöründe faaliyet gösteren işletmeler, müşterilere ait kimlik, ödeme ve konum verilerini topladıkları için ciddi düzeyde kişisel veri güvenliği sorumluluğu taşımaktadır. Dijital platformlar üzerinden gerçekleşen işlemlerin artması, bu sektörü hem paylaşım ekonomisinin bir parçası haline getirmiş hem de siber tehditlere daha açık hale getirmiştir. Akan ve Tepeler (2022), paylaşım ekonomisinin sürdürülebilirlik ve güven temelli yapısını ele aldığı çalışmasında, özellikle dijital ortamda kurulan güven ilişkilerinin veri güvenliği ile doğrudan ilişkili olduğunu vurgulamıştır. Otel rezervasyon sistemleri, havayolu biletleme platformları ve müşteri sadakat programları gibi çeşitli dijital altyapılarda geniş kişisel ve finansal verilerin işlenmesi bu sektörü siber saldırganlar için daha cazip hale getirmektedir.

Biyoteknoloji, faktöring, sosyal yardım, su yönetimi, tarım, ulaşım ve taşımacılık, ilaç sanayi, ithalat/ihracat, reklamcılık ve veri analitiği gibi sektörlerde 2018-2024 arası dönemde yalnızca birer adet veri ihlal vakası raporlanmıştır. Bu sektörlerde daha az kişisel veri işleniyor oluşu diğer sektörlere kıyasla bu sektörlerde faaliyet gösteren firmaların siber saldırı riskini azaltmıştır.

KVKK kapsamında yapılan incelemeler doğrultusunda, farklı sektörlerde gerçekleşen veri ihlal vakaları sayısal olarak analiz edilmiştir. 2018-2024 arası dönemi kapsayan söz konusu analiz çerçevesinde, mali müşavirlik sektöründe toplam 2 adet veri ihlal vakası tespit edilmiştir. Bu durum, sektörde işlenen verilerin niteliği ve güvenlik önlemleri açısından incelenmesini mümkün kılmaktadır.

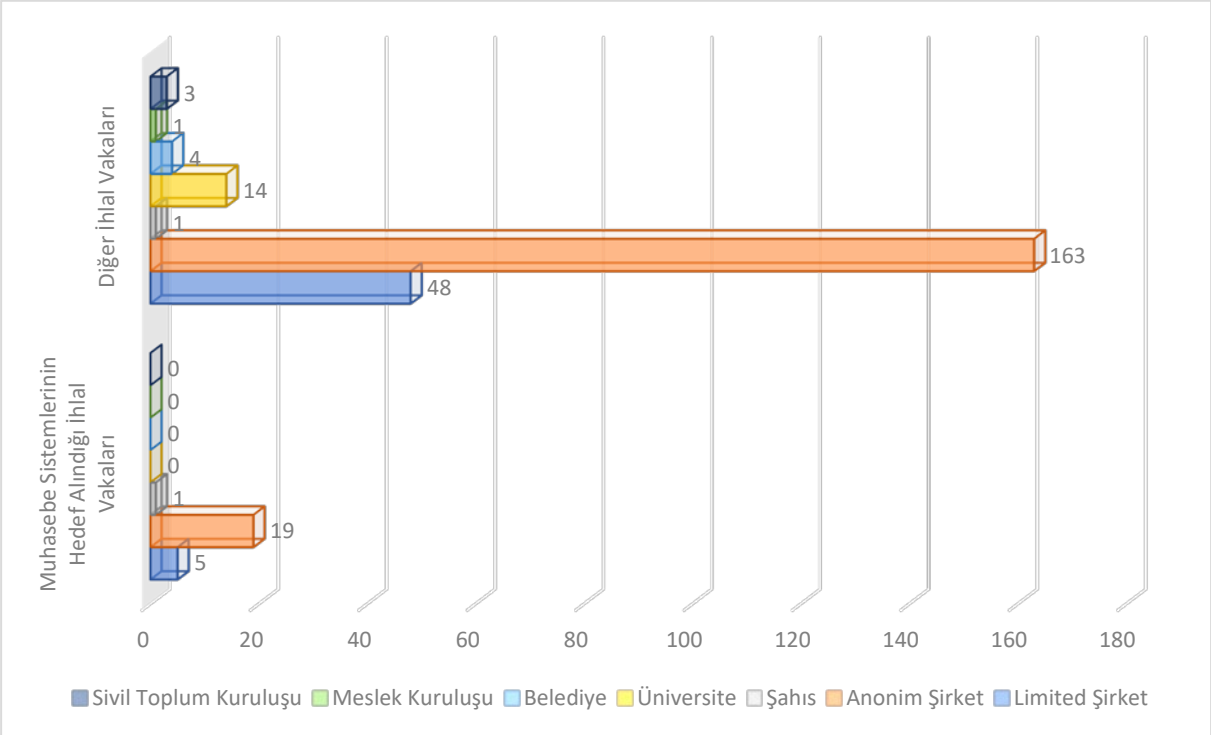
Tablo 1. Mali Müşavirlik Sektöründe Veri İhlalleri

Kurum	Başlama	Bitiş	Bildirim	Etkilenen Kişi	İhlal Kaynağı	İhlal Türü
"------" Mali Müşavirlik ve Bağımsız Denetim Hizmetleri Anonim Şirketi	16.07.2022	9.08.2022	16.08.2022	Bilinmiyor	Dış Kaynak	Siber Saldırı
"------" Serbest Muhasebeci Mali Müşavir	31.03.2021	6.04.2021	27.05.2021	130	Dış Kaynak	Siber Saldırı

Tablo 1'de iki farklı mali müşavirlik firmasında gerçekleşen veri ihlal vakalarının detayları sunulmaktadır. Her iki firma içinde gerçekleşen ihlal vakaları dış kaynaklı fidye yazılımı saldırıları sonucu gerçekleşmiş ve farklı boyutlarda etkiler oluşturmuştur. Bu ihlal vakaları, mali müşavirlik sektörünün siber güvenlik açısından karşılaştığı risklere dair önemli bilgiler sunmaktadır.

"------" Mali Müşavirlik ve Bağımsız Denetim Hizmetleri Anonim Şirketi'nde ihlal vakası, 16.07.2022'de başlamış ve 09.08.2022'de tespit edilmiştir. Bu, ihlalin yaklaşık 24 gün boyunca fark edilmediğini göstermektedir. Ayrıca veri sorumlularının, ihlali tespit ettikten sonra 72 saat içinde bildirimde bulunma yükümlülüğü vardır. Ancak söz konusu şirketin yasal süre içerisinde bildirim yapmadığı görülmüştür. Etkilenen kişi sayısı ise tespit edilememiştir. Bu durum, veri ihlalinin kapsamının tam olarak belirlenemediğini göstermekle birlikte etkilerinin beklenenden daha büyük olabileceğini göstermektedir. Siber saldırı sonucunda kimlik (ad, soyad) ve iletişim (e-posta, telefon) bilgileri ile finansal veriler (fatura, ticari kayıtlar) etkilenmiştir. Bu veriler, firmanın mevcut müşterilerinin ve potansiyel müşterilerinin kişisel ve ticari bilgilerini içermektedir. Söz konusu veri ihlali, mali müşavirlik süreçlerinde kullanılan ticari verileri de hedef almıştır. Bu durum, müşterilere ait finansal kayıtların, gelir-gider tablolarının ve diğer kritik muhasebe bilgilerinin yetkisiz erişime maruz kaldığını ve müşterilerin mali güvenliğinin riske girdiğini göstermektedir. Bunlara ek olarak veri sorumlularının, ihlali tespit ettikten sonra 72 saat içinde bildirimde bulunma yükümlülüğü vardır. Ancak söz konusu "------" Serbest Muhasebeci Mali Müşavirlik firmasındaki ihlal vakası, 31.03.2021 ile 06.04.2021 tarihleri arasında gerçekleşmiş ve 04.04.2021'de tespit edilmiştir. Ancak bu veri sorumlusunun da bildirim için yasal süre olan 72 saat içerisinde

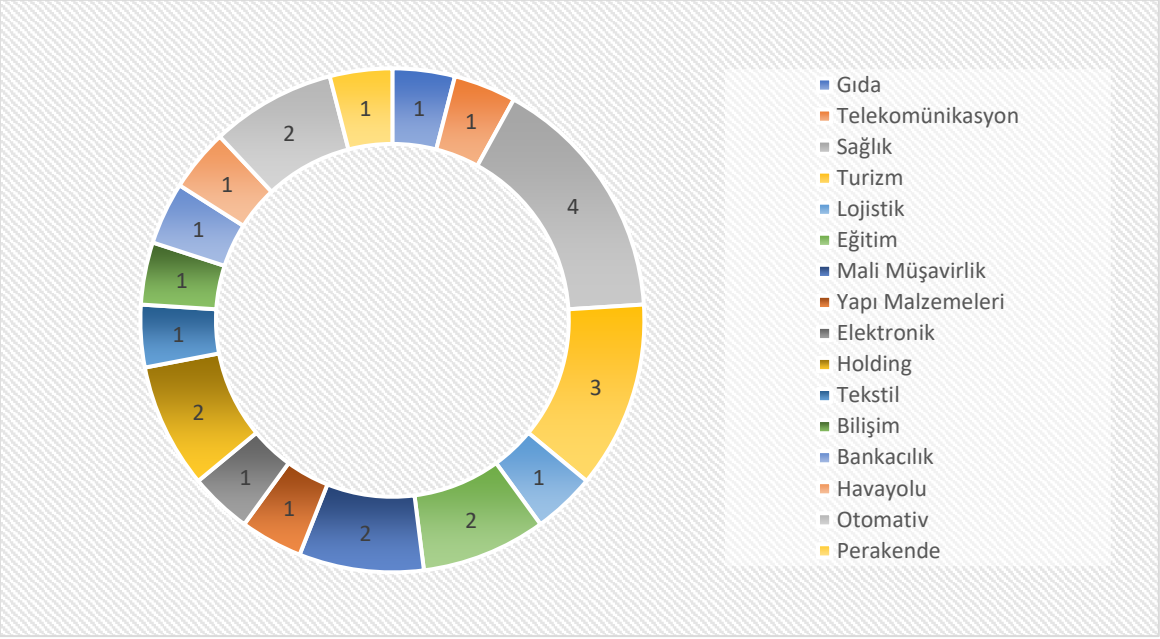
bildirim yapmadığı görülmüştür. İhlalin tespit süresi diğer firmaya nazaran daha kısa olsa da saldırganlar fidye talep etmiş ve fidyenin ödenmesi sonucunda kilitlenmiş olan sistemleri tekrar kullanıma açmışlardır. Bu firmaya yönelik gerçekleşen siber saldırıdan yaklaşık 130 gerçek ve tüzel kişi etkilenmiştir. Bu sayı, ihlalin nispeten daha sınırlı bir kapsamda kaldığını göstermektedir. Siber saldırı sonucunda Kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, finans, mesleki deneyim, görsel ve işitsel kayıtlar gibi geniş bir veri yelpazesi etkilenmiştir. Bu, ihlalin kapsamının oldukça geniş bir tabana yayıldığını göstermektedir. Söz konusu veri ihlali, mali müşavirlik süreçlerinde kullanılan ticari verileri de içermektedir. Talep edilen fidyenin ödenmesi ise saldırganların taleplerine boyun eğildiğini göstermektedir.



Şekil 6. Muhasebe Sistemlerinin Hedef Alındığı Veri İhlal Vakalarının Kurumsal Dağılımı

Şekil 6'da KVKK kapsamında gerçekleşen ve muhasebe sistemlerinin hedef alındığı vakalar ile diğer vakalara ait veri ihlallerinin kurum türlerine göre dağılımı gösterilmektedir. Bu veriler, muhasebe sistemlerinin siber güvenlik açısından ne kadar risk altında olduğunu ve hangi veri sorumlusu türlerinin daha fazla önlem alması gerektiğini analiz etmek adına önemlidir. Muhasebe sistemlerine yönelik gerçekleştirilen veri ihlal vakaları, genel ihlallerin yaklaşık %9,65'ini oluşturmaktadır. Bu oran, muhasebe sistemlerinin önemli bir hedef

olduğunu, ancak diğer ihlal türlerine kıyasla daha düşük bir risk düzeyine olduğunu göstermektedir. Muhasebe sistemlerinin hedef alındığı vakalar anonim şirket, gerçek kişi ve limited şirket özelinde gerçekleşmiştir. Muhasebe sistemlerinin hedef alındığı veri ihlal vakalarının en fazla görüldüğü kurum türü 19 adet veri ihlal vakası ile anonim şirketlerdir. Anonim şirketlerin genellikle daha büyük ölçekli finansal işlemler gerçekleştirmesi, geniş bir müşteri ve tedarikçi ağına sahip olması ve muhasebe sistemlerinin daha karmaşık yapıda olması, sistemlerin yönetimini zorlaştırarak güvenlik açıklarına neden olmaktadır. Dolayısıyla bu tür şirketler, siber saldırganlar için daha cazip hedef hâline gelmektedir. Limited şirketler de finansal verileri işlediği için benzer risklerle karşı karşıya kalmaktadır. Limited şirket özelinde muhasebe sistemlerinin hedef alındığı vaka sayısı 5 adet olarak raporlanmıştır. Şirket türlerinin veri işleme kapsamı, KVKK çerçevesinde "meşru menfaat" ilkesi doğrultusunda da farklılık gösterebilmektedir (Saat, 2024: 626). Limited şirketlerin, anonim şirketlere kıyasla daha küçük ölçekli olmaları, finansal işlem hacimlerinin daha sınırlı olması ve muhasebe sistemlerinin görece daha az karmaşık olması nedeniyle veri ihlal vakaları daha az gerçekleşmiştir. Analiz süreci boyunda, şahıs şirketlerinin muhasebe sistemlerini hedef alan sadece 1 adet vaka raporlanmıştır. Üniversite, belediye, meslek kuruluşu ve sivil toplum kuruluşlarında ise muhasebe sistemlerine yönelik veri ihlal vakası görülmemiştir.



Şekil 7. Muhasebe Sistemlerinin Hedef Alındığı Veri İhlal Vakalarının Sektörel Dağılımı

Şekil 7'de, muhasebe sistemlerinin hedef alındığı veri ihlallerinin farklı sektörlerdeki dağılımı gösterilmiştir. Muhasebe sistemleri, finansal verilerin işlendiği ve depolandığı kritik sistemler olduğundan siber saldırganlar için daha cazip bir hedef haline gelmektedir. Sağlık sektörü, hasta kayıtları, finansal işlemler ve tedarik zinciri yönetimi gibi karmaşık muhasebe sistemlerine sahiptir. Bu sistemler, siber saldırganlar için cazip bir hedef oluşturduğu için sağlık sektöründe 4 adet muhasebe sistemini hedef alan veri ihlal vakası gerçekleşmiştir. Turizm sektörü, rezervasyon sistemleri, ödeme işlemleri ve müşteri verileri gibi geniş bir veri yelpazesine sahiptir. Ayrıca bu verilerin muhasebe sistemlerine entegre olması ise ihlal riskini artırmaktadır. Dolayısıyla turizm sektöründe 3 adet muhasebe sistemini hedef alan veri ihlal vakası gerçekleşmiştir. Eğitim sektörünün muhasebe sisteminde öğrenci ücretleri, burs ödemeleri ve personel maaşları gibi geniş portföye sahip finansal veriler yer almaktadır. Bu durum ise eğitim sektörünü siber saldırganlar için cazip bir hedef haline getirmektedir. Eğitim sektörünün muhasebe sistemi hedef alan 2 adet veri ihlal vakası raporlanmıştır. Otomotiv sektörünün karmaşık muhasebe sistemlerine sahip olması, tedarik zinciri, müşteri portföyleri, satış ve finansman işlemleri ile finansal raporlama süreçlerinin kapsamlı yapısı ve sektördeki dijital dönüşümün hızlanması, veri ihlal riskini artırmaktadır. Otomotiv sektöründe ise analiz süreci boyunca muhasebe sistemini hedef alan 2 adet veri ihlal vakası gerçekleşmiştir. Holdingler, birden fazla şirketin finansal verilerini entegre bir şekilde yönetmektedir. Bu entegrasyon, muhasebe sistemlerinin veri ihlallerine karşı daha büyük bir risk altında olmasına neden olmaktadır. Holdinglerde de muhasebe sistemini hedef alan 2 adet veri ihlal vakası gerçekleşmiştir. Gıda, Telekomünikasyon, Lojistik, Yapı Malzemeleri, Elektronik, Tekstil, Bilişim, Bankacılık, Havayolu ve Perakende sektörlerinde ise analiz süreci boyunca muhasebe sistemlerini hedef alan 1'er adet veri ihlal vakası raporlanmıştır.

Tablo 2. Muhasebe Sistemlerine Yönelik Veri İhlal Vakalarının Türleri ve Etkileri

Kurum	Etkilenen Kişi	İhlalin Türü	İhlalin Muhasebe Verilerine Etkisi
"-----" Gıda Pazarlama ve Dağıtım Ticaret Limited Şirketi	1000	Siber Saldırı, Veri Kaybı ve Silinme	Muhasebe Programına Ait Bilgiler, Fatura Bilgileri, Resmi Defterler, Borç-Alacak Bakiyeleri, Personel Bilgileri, Dosya Şifreleme, Fidye
"-----" İletişim Hizmetleri A.Ş.	1254	Siber Saldırı, Veri Kaybı ve Silinme	Muhasebe Programına Ait Bilgiler, Fatura Bilgileri, Resmi Defterler, Borç-Alacak Bakiyeleri, Personel Bilgileri, Dosya Şifreleme, Fidye

"-----" Uzmanlar Sağlık Hizmetleri San. Paz. Tic. A.Ş.	2000000	Siber Saldırı, Veri Kaybı ve Silinme	Personel ve Muhasebe İşlemleri İçin Kullanılan Programın Veri Sorumlusunun Bir Şubesine Kurulumu Sırasında Kısa Süreli Port Açıklığı Sebebiyle Siber Saldırıya Uğradığı
"-----" Sağlık Hizmetleri İnş. Tur. San ve Tic. A.Ş. (Özel Aktif Hastanesi)	2000000	Siber Saldırı, Veri Kaybı ve Silinme	Personel ve Muhasebe İşlemleri İçin Kullanılan Programın Veri Sorumlusunun Bir Şubesine Kurulumu Sırasında Kısa Süreli Port Açıklığı Sebebiyle Siber Saldırıya Uğradığı
"-----" Sağlık Turizm İnşaat San. ve Tic. A.Ş.	10000	Siber Saldırı, Veri Kaybı ve Silinme	Personel ve Muhasebe İşlemleri İçin Kullanılan Programın Veri Sorumlusunun Bir Şubesine Kurulumu Sırasında Kısa Süreli Port Açıklığı Sebebiyle Siber Saldırıya Uğradığı
"-----" Otelcilik Turizm ve Tic. A.Ş.	Tespit Edilemedi	Siber Saldırı, Veri Kaybı ve Silinme	Muhasebe Programına Ait Bilgiler, Fatura Bilgileri, Resmi Defterler, Borç-Alacak Bakiyeleri, Personel Bilgileri, Dosya Şifreleme, Silme
"-----" Otelcilik Turizm ve Tic. AŞ.	Tespit Edilemedi	Siber Saldırı, Veri Kaybı ve Silinme	Muhasebe Programına Ait Bilgiler, Fatura Bilgileri, Resmi Defterler, Borç-Alacak Bakiyeleri, Personel Bilgileri, Dosya Şifreleme, Silme
"-----" İnş. Taşımacılık Paz. San. ve Tic. A.Ş.	Tespit Edilemedi	Siber Saldırı, Veri Kaybı ve Silinme	Muhasebe Programına Ait Bilgiler, Fatura Bilgileri, Resmi Defterler, Borç-Alacak Bakiyeleri, Personel Bilgileri, Dosya Şifreleme, Silme
"-----" Eğitim ve Eğitim Dan. A.Ş.	Tespit Edilemedi	Siber Saldırı	Muhasebe Kayıtları, Ücret Bilgileri
"-----" Alaçatı Turizm Yatırımları A.Ş.	450	Siber Saldırı	Muhasebe Programına Ait Bilgiler, Fatura Bilgileri, Resmi Defterler, Borç-Alacak Bakiyeleri, Personel Bilgileri, Dosya Şifreleme, Silme
"-----" Yeminli Mali Müşavirlik ve Bağımsız Denetim Hizmetleri Anonim Şirketi	Tespit Edilemedi	Siber Saldırı	Yeminli Mali Müşavirlik ve Bağımsız Denetim Faaliyetleri Kapsamında Tüzel Kişi Müşterilerden Elde Edinilen Ticari Veriler İçinde Bulunan Kimlik (Ad, Soyadı), İletişim (E-Posta Adresi, Telefon Numarası) ve Finans (Fatura, Ticari Kayıtlar)
"-----" İlaç San. ve Tic. Ltd. Şti.	981	Yetkisiz Erişim	Bordro Bilgileri
"-----" İnşaat ve Yapı Elemanları San. ve Tic. A.Ş. ile "-----" Insulation Izolation San. ve Tic. A.Ş.	Tespit Edilemedi	Yetkisiz Erişim	Muhasebe Programına Ait Bilgiler, Fatura Bilgileri, Resmi Defterler, Borç-Alacak Bakiyeleri, Personel Bilgileri
"-----" The Advanced Biometric Solution Elektronik San. ve Tic. Ltd. Şti.	1000	Siber Saldırı, Veri Kaybı ve Silinme	Muhasebe Programına Ait Bilgiler, Fatura Bilgileri, Resmi Defterler, Borç-Alacak Bakiyeleri, Personel Bilgileri, Programa Erişilememe
"-----" Yatırım Holding A.Ş., "-----" Demir Çelik Sanayi A.Ş., "-----" Entegre Ağaç	Tespit Edilemedi	Siber Saldırı, Veri Kaybı ve Silinme	E-Fatura, E-Defter, Muhasebe, Lojistik, Stok, Personel, İnsan Kaynakları, Üretim, Yönetim ve Benzeri Sistemleri

Sanayi A.Ş., "-----" Gübre Sanayi A.Ş.			
"-----" İnovasyon ve Bilim Eğitim Hizmetleri Anonim Şirketi	79997	Yetkisiz Erişim	Ücret Bilgileri, Personel Bilgileri
"-----" İstanbul Giyim ve Tekstil Ticaret Ltd. Şti.	20005	Siber Saldırı, Veri Kaybı ve Silinme	Ücret Bilgileri, Personel Bilgileri
"-----" Şirketler Grubu	Tespit Edilemedi	Siber Saldırı, Veri Kaybı ve Silinme	Muhasebe, Özlük Dosyaları ile Resmi ve Özel Dosyaların Şifrelenmesi
"-----" Bilişim Teknolojileri A.Ş.	Tespit Edilemedi	Yetkisiz Erişim, Yetkisiz İfşa	Şirket Belgeleri, İmza Sirküleri, Vergi Levhası, Finans
"-----" (Serbest Muhasebeci Mali Müşavir)	130	Siber Saldırı	Bilgisayar Korsanlarına Fidye Ödenmesiyle İhlale Konu Sistemlerin Kullanıma Açıldığı
"-----" Bankası A.Ş.	2484	Yetkisiz Erişim, Yetkisiz İfşa	Kredi Risk ve Teminat Durumu, Ödeme Performans Bilgileri, Karşılıksız Çek ve Protestolu Senet Ödeme Bilgileri
Air "-----" Limited	3639702	Siber Saldırı	Müşteriler, Bilet Sayıları, Kredi Kartı Bilgileri
"-----" International Otomotiv San. ve Tic. A.Ş.	1084	Siber Saldırı, Veri Kaybı ve Silinme	Tedarikçiler, Müşteriler
"-----" Otomotiv San. ve Tic. A.Ş.	976	Siber Saldırı, Veri Kaybı ve Silinme	Tedarikçiler, Müşteriler
"-----" Bakırköy Alışveriş Hiz. Tic. Ltd. Şti.	806	Yetkisiz İfşa	E-Arşiv Faturalarının Yanlış Kişilere Gönderilmesi

Tablo 2'de muhasebe sistemlerinin hedef alındığı veri ihlal vakalarının farklı kurumlarda gerçekleşen örnekleri detaylı bir şekilde sunulmaktadır. İhlallerin türünü, etkilenen kişi sayısını, ihlalin muhasebe verilerine etkisini ve ihlalin kaynağını içermekte olan bu tablo, veri ihlallerinin kurumlar üzerindeki etkilerini analiz etmek için önemli bir kaynak oluşturmaktadır.

Tablo 2'de sunulan veri ihlallerinin büyük çoğunluğu siber saldırılar sonucu gerçekleşmiştir. Bu saldırılar, fidye yazılımı, veri kaybı, veri silme ve dosya şifreleme gibi yöntemlerle gerçekleştirilmiştir. Özellikle fidye yazılımı saldırıları, kurumların muhasebe sistemlerini kilitleyerek finansal kayıplara neden olmaktadır. Diğer ihlaller ise yetkisiz kişilerin muhasebe sistemlerine erişmesi veya hassas verileri ifşa etmesi sonucu gerçekleşmiştir. Bu tür ihlaller, genellikle iç kaynaklı zafiyetlerden veya çalışan hatalarından kaynaklanmaktadır.

Sağlık sektörü, büyük çapta hasta ve personel verisi işlediği için bu sektörde gerçekleşen bazı veri ihlal vakalarında 2.000.000 kişiyi etkilenmiştir. Diğer sektörlerde etkilenen kişi sayısı görece daha düşüktür. Veri ihlal vakalarından etkilenen kişi sayısının çok yüksek olduğu bir diğer sektör ise havayolu sektörüdür. Hava yolu şirketlerinin geniş müşteri tabanı, yüksek hacimli veri işlemleri ve hassas yolcu bilgileri barındırmasından dolayı veri ihlal riskleri oldukça yüksektir. Bu nedenle sektörde gerçekleşen veri ihlalinden 3.639.702 kişi etkilenmiştir. Bazı veri ihlal vakalarında ise etkilenen kişi sayısı tespit edilememiştir. Bu durum, ihlalin boyutunun henüz netleşmediğini ve kurumların ihlali tam olarak analiz edemediğini göstermektedir.

Tablo 2'den de anlaşılacağı üzere bazı veri ihlal vakaları, muhasebe programlarının kurulumu sırasında kısa süreli port açıklıkları nedeniyle gerçekleşmiştir. Bu durum, kurumların sistem yönetimi ve siber güvenlik önlemlerinde eksiklikler olduğunu göstermektedir. Diğer durumlardaki veri ihlal vakaları ise fidye yazılımı şeklinde gerçekleşen siber saldırılar sonucunda yaşanmıştır. Fidye yazılımı saldırıları sonucunda, muhasebe sistemleri kilitlenerek kurumların fidye ödenmesi istenmiştir. Bu tür saldırılar hem finansal kayıplara hem de veri kayıplarına neden olmuştur.

Muhasebe sistemlerine yönelik gerçekleştirilen veri ihlal vakalarında, fatura bilgileri, resmi defterler, borç-alacak bakiyeleri gibi kritik öneme sahip finansal verileri etkilemiştir. Bu tür kritik öneme sahip verilerin yetkisiz kişiler tarafından ele geçirilmesi veya bu tür verilen kaybı kurumların finansal tablolarında belirsizliğe yok açabileceği gibi finansal istikrarı da tehdit etmektedir. Muhasebe sistemlerine yönelik yapılan siber saldırılar, sadece kurumların finansal verilerini değil, aynı zamanda çalışanlara ait kimlik ve sicil bilgileri gibi kritik bilgileri de hedef almıştır. Özellikle bordro ve ücret bilgileri gibi hassas verilerin ele geçirilip ifşa edilmesi, çalışanların kişisel mahremiyetlerinin ihlal edilmesi anlamına gelmektedir. Bu tür veri ihlalleri, çalışanların güvenini sarsabileceği gibi, kurumların itibarını da zedeleyecektir. Muhasebe sistemlerine yönelik gerçekleştirilen siber saldırılarda e-fatura ve e-defter gibi elektronik kayıt sistemleri de hedef alınmıştır. Bu durum, kurumların finansal süreçlerini aksatmakla kalmayıp, aynı zamanda resmi muhasebe kayıtlarının bütünlüğünü de riske atmaktadır.

7. SONUÇ VE ÖNERİLER

Dijital dönüşüm çağında muhasebe mesleği, benzeri görülmemiş bir değişim sürecinden geçerken, veri güvenliği ve kişisel verilerin korunması gibi konular kritik bir önem kazanmıştır. Muhasebe sistemlerinin dijitalleşmesi, finansal süreçleri daha verimli hale getirirken, aynı zamanda siber tehditlerin ve siber saldırılan da odağı haline gelmesine neden olmuştur. Son yıllarda artan siber saldırılar ve veri ihlal vakaları, yalnızca muhasebe sektöründeki kurumları değil, aynı zamanda firmaların muhasebe verilerini de doğrudan hedef almaktadır.

Özellikle muhasebe programlarında saklanan fatura bilgileri, borç-alacak bakiyeleri, resmi defterler ve bordro kayıtları gibi hassas finansal veriler, fidye yazılımı saldırıları ve veri sızıntıları yoluyla ele geçirilmektedir. Ele geçirilen bu veriler silinerek kurumların işleyişini sekteye uğratmakta veya ifşa edilerek kurumların güvenilirliğini zedelemektedir.

Bu çalışmada, Kişisel Verileri Koruma Kurumu'na yapılan veri ihlal bildirimleri incelenerek mali müşavirlik sektörü başta olmak üzere farklı sektörlerde muhasebe sistemlerinin hedef alındığı veri ihlalleri incelenerek analiz edilmiş ve bu vakaların azaltılmasına yönelik çözüm önerileri geliştirilmiştir. Türkiye'de muhasebe sektöründeki veri ihlallerini sistematik bir yaklaşımla ele alan öncü araştırmalardan biri olan bu çalışma, sektördeki güvenlik açıklarını tespit etmeyi ve veri koruma konusunda farkındalık oluşturmayı hedeflemektedir.

Analiz sonuçlarına göre; muhasebe sistemlerine yönelik veri ihlallerin büyük çoğunluğunun siber saldırılar (özellikle fidye yazılımı) ve yetkisiz erişimler sonucu gerçekleştiği görülmektedir. Veri ihlallerinden sadece fatura bilgileri, borç-alacak bakiyeleri, resmi defterler gibi finansal veriler değil, aynı zamanda kimlik, iletişim, lokasyon ve sağlık bilgileri gibi hassas olan personel bilgileri de etkilenmiştir.

Sağlık, turizm, eğitim ve otomotiv sektörleri, muhasebe sistemlerine yönelik ihlallerde öne çıkmaktadır. Özellikle sağlık sektöründe 2.000.000 kişiyi etkileyen ihlaller, bu sektörün geniş hasta ve personel verisi işlemesi nedeniyle yüksek risk altında olduğunu ortaya koymaktadır. Anonim şirketler, 19 ihlal vakası ile en fazla hedef alınan kurum türü olmuştur.

Bu durum, anonim şirketlerin karmaşık muhasebe sistemleri ve geniş finansal işlem hacimlerinin siber saldırganlar için cazip bir hedef oluşturduğunu göstermektedir.

İhlallerin önemli bir kısmının, port açıklıkları ve sistem yönetimindeki zafiyetler gibi teknik eksikliklerden kaynaklandığı görülmektedir. Özellikle fidye yazılımlarına yönelik saldırılar sonucunda, kurumların hem finansal kayıplar yaşadığı hem de veri bütünlüğünün ciddi şekilde tehdit altında kaldığı tespit edilmiştir. Bu tür saldırılar, kurumların itibarını zedelemekte ve müşteri güvenini sarsmaktadır. Kara (2019) tarafından da belirtildiği üzere, fidye yazılımlarına karşı alınabilecek önlemler arasında; kaynağı bilinmeyen şüpheli e-postaların açılmaması, güvenli olmayan internet sitelerinin ziyaret edilmemesi, kullanılan yazılımların güncel tutulması, sistemde güvenlik açıklarının kapatılması ve güvenilir antivirüs ya da sandbox yazılımlarının kullanılması yer almaktadır. Ayrıca, kullanıcıların değerli verilerini düzenli olarak yedeklemesi ve olası bir saldırı durumunda bu yedekler aracılığıyla sistemin önceki haline döndürülmesinin sağlanması önem arz etmektedir. Kullanıcı farkındalığının artırılması ve alınması gereken önlemler hakkında bilinçlendirme yapılması da siber güvenlik yönetiminin ayrılmaz bir parçasıdır.

Sonuç olarak, muhasebe sistemlerinin siber güvenlik açısından korunması büyük önem taşımaktadır. Bu kapsamda, kurumlar siber güvenlik altyapılarını güçlendirmeli, erişim kontrolleri, ağ güvenliği, güncel antivirüs yazılımlarının kullanımı, log kayıtlarının düzenli tutulması gibi teknik önlemleri uygulamalıdır. Ayrıca, yetki matrisi oluşturulması, çalışanların siber güvenlik farkındalığına yönelik düzenli eğitimler verilmesi, kişisel verilere erişimin sınırlandırılması ve taşınabilir medya kullanımının denetlenmesi gibi idari tedbirler de hayata geçirilmelidir. Kişisel Verileri Koruma Kurumu'nun yayımladığı Veri Güvenliği Rehberi (2021) ve Kullanıcı Güvenliğine İlişkin Tavsiyeler doğrultusunda hareket edilmesi, ihlallerin önlenmesinde etkili olacaktır. Bu önlemler hem finansal istikrarın korunmasına hem de kurumların itibarı ve müşteri güveninin sağlanmasına doğrudan katkı sunacaktır.

KAYNAKLAR

Achar, Sandesh (2018). "Security of accounting data in cloud computing: a conceptual review". Asian Accounting and Auditing Advancement, 9 (1), 60–72.

Akan, Y.- Tepeler, M. İ. (2022). "Sürdürülebilirlik ve güven ekseninde paylaşım ekonomisi". Sosyoekonomi, 30(53), 447-464.

Akhisar, İ.- Tezergil, S. (2014). "Malmquist toplam faktör verimlilik endeksi: Türk sigorta sektörü uygulaması". Finansal Araştırmalar ve Çalışmalar Dergisi, 5(10).

Atasoy, Kemal (2016). "Kişilik hakkı kapsamında sosyal medyada kişisel verilerin korunması ve veri sahibinin rızası". Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 22(3), 269-301.

Büyükarıkan, Ulukan - Öğünç, Harun - Eryılmaz, Cengiz (2021). "Muhasebe öğrencilerinin kişisel verilerin korunması kanunu hakkında farkındalık düzeyinin belirlenmesi". Muhasebe ve Vergi Uygulamaları Dergisi, 14 (1), 249-273.

Civelek, Mehmet, A. - Durukan, Banu (1998). "Günümüz koşullarında muhasebe mesleği ve meslek ahlakı". III. Türkiye Muhasebe Denetimi Sempozyumu, Muhasebe Denetiminde Yetkiler, Sorumluluklar ve Meslek Ahlakı. Antalya: İSMMMO Yayını.

Çetin, Hakan (2014). "Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi". Akdeniz İİBF Dergisi. 14(29), 86-105.

Dilsiz, Volkan. (2021). "Dijital dünyada kişisel veri kavramı ve KVKK / GDPR kapsamında bir değerlendirme". İstanbul Marka Bilim Topluluğu. https://istanbulmarka.science/pdf/Dijital-Dunyada-Kisisel-Veri-Kavrami-ve-KVKK-GDPR-Kapsaminda-Bir-Degerlendirme.pdf. (Erişim Tarihi: 13/02/2025).

ENISA. (2023). ENISA Threat landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. (Erişim Tarihi: 08/05/2025).

Ertan, Alpkaan (2022). "Nesnelerin internetinin kişisel verilerin korunması kapsamında incelenmesi". Kişisel Verileri Koruma Dergisi. 4(2), 48-68.

Evci Eralp, Özge (2023). "İşyerlerinde kişisel sağlık verilerinin işlenmesinde sır saklama yükümlülüğünün kapsamı". Kişisel Verileri Koruma Dergisi, 5(2), 28-38.

Genç, E. G. (2017). "Üniversitelerin ülke sıralamaları ve insani gelişme endeksi: Panel nedensellik analizi". Eurasian Econometrics Statistics & Emprical Economics Journal, 89-101.

IBM Security. (2023). Cost of a data breach report 2023. https://www.ibm.com/reports/data-breach. (Erişim Tarihi: 08/05/2025).

Kara, İ. (2019). "Interpol fidye yazılım saldırısı ve analizi" İleri Teknoloji Bilimleri Dergisi, 8(2), 117-128.

Karaçadır, V. (2022). "Sağlık harcamaları ve internet kullanım ilişkisi: OECD ülkeleri için panel veri analizi". Journal of Public Economy and Public Financial Management, 2(2), 41-52.

Kauffman, Robert. J.- Lee, Yong, Jick - Prosch, Marilyn, M.G. - Steinbart, Paul, J. (2011). "A survey of consumer information privacy from the accounting information systems perspective". Journal of Information Systems, 25(2). 47-79.

Kılınç, Doğan (2012). "Anayasal bir hak olarak kişisel verilerin korunması". Ankara Üniversitesi Hukuk Fakültesi Dergisi, 61(3), 1089-1172.

Kişisel Verileri Koruma Kurumu. (2023). Faaliyet Raporu, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/1ee4f609-711f-4a85-aefc-69181bbcdf3a.pdf. (Erişim Tarihi: 10/02/2025).

Kişisel Verileri Koruma Kurumu. Veri güvenliği rehberi. https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf. (Erişim Tarihi: 08/05/2025).

Kutlu, Önder - Kahraman, Selçuk (2017). "Türkiye'de kişisel verilerin korunması politikasının analizi". Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi, 5(5), 45-62.

Lois, Petros - Drogalas, George A. - Karagiorgos, Alkiviadis - Thrassou, Alkis - Vrontis, Demetris "Internal auditing and cyber security: audit role and procedural contribution". International Journal of Managerial and Financial Accounting, 13(1), 25–47.

Özer Deniz, Miray (2020). "Kişisel verilerin korunması kanunu ile arabuluculuğa hâkim gizlilik ilkesinin birlikte değerlendirilmesi". Kişisel Verileri Koruma Dergisi, 2(1), 63-71.

Perwej, Yusuf - Abbas, Qamar - Dixit, Jai Pratap - Akhtar, Nikhat - Jaiswal, Anurag Kumar (2021). "A systematic literature review on cyber security". International Journal of Scientific Research and Management, 9(12), 669–710.

Saat, D. (2024). "Kişisel Verilerin Korunması Kanunu'nda öngörülen meşru menfaat kavramının ticaret şirketleri bakımından değerlendirilmesi". Anadolu Üniversitesi Hukuk Fakültesi Dergisi, 10(2), 617-638.

Sevindi, Sena Nur - Ordu, Muhammet Emin (2023). "AB ve Türk hukukunda veri ihlalinin tespiti ve bildirim süresinin karşılaştırmalı değerlendirmesi". Kişisel Verileri Koruma Dergisi, 5(1), 12-22.

Smith, Alan D. - Rupp, William T. (2002). "Issues in cybersecurity; understanding the potential risks associated with hackers/crackers". Information Management & Computer Security, 10(4), 178-183.

Stanciu, Victoria - Rîndaşu, Sinziana M. (2018). "The impact of general data protection regulation in the accounting profession–evidences from Romania". Journal of Information Assurance & Cyber security, 1-9.

Świetla, Katarzyna (2019). "Protection of personal data in the system of modern accounting in the context of the ımplementation of the regulation of the european parliament and of the EU council 2016/679 of 27 April 2016". Financial Sciences. Nauki o Finansach, 24(3), 59-71.

Tanyılmaz, K. - Erten, A. N. - Dairesi, B. M. İ. S. A. (2001). Dünyada ve Türkiye'de otomotiv sektörü. Birleşik Metal-İş Yayınları.

Tao, Hai - Bhuiyan, Md Zakirul Alam - Rahman, Md Arafatur - Wang, Guojun - Wang, Tian - Ahmed, Md. Manjur - Li, Jing (2019). "Economic perspective analysis of protecting ample data security and privacy". Future Generation Computer Systems, 98, 660–671.

Verizon. (2023). 2023 Data breach ınvestigations report. Verizon Business Group. https://www.verizon.com/business/resources/reports/dbir/. (Erişim Tarihi: 08/05/2025).