İSTANBUL UNIVERSITY PRESS

Bilgi ve Belge Araştırmaları Dergisi
The Journal of Information and Documentation Studies
BBA 2025, (23): 1–20

https://doi.org/10.26650/bba.2025.23.1577974
Başvuru | Submitted 01.11.2024
Revizyon Talebi | Revision Requested 24.01.2025
Son Revizyon | Last Revision Received 10.03.2025
Kabul | Accepted 27.03.2025

Bilgi ve Belge Araştırmaları Dergisi
The Journal of Information and Documentation Studies

Araştırma Makalesi | Research Article

Açık Erişim | Open Access

Kamu Sektöründe Veri Yönetimine İlişkin Anonimleştirme, Silme ve Yok Etme Süreçlerinin Hukuki ve Teknik Açıdan Değerlendirilmesi: Aydın İli Örneği

Legal and Technical Evaluation of Anonymization, Deletion and Destruction Processes Related to Data Management in the Public Sector: The Case of Aydın Province

Haktan Yavaş [1] & Türkay Henkoğlu [2]

[1] Pamukkale Üniversitesi Yönetim Bilişim Sistemleri Bölümü, Pamukkale, Türkiye
[2] Aydın Adnan Menderes Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, Aydın, Türkiye

Öz Bireylerin mahremiyetini korumanın giderek zorlaştığı kamu kurumlarında kişisel verilerin güvenli biçimde saklanması ve işlenmesi için teknik ve idari boyutları içeren politika ve prosedürlere olan ihtiyaç her geçen gün artmaktadır. Bu çalışmada kamu kurumlarındaki veri yönetimi süreçleri, hukuki düzenlemeler, teknik gereksinimler ve uygulamada karşılaşılan zorluklar çerçevesinde incelenmiş ve tespit edilen eksikliklere yönelik çözüm önerileri sunulmuştur. Araştırma kapsamında, Aydın ilindeki 103 kamu kurumunun yöneticileri, idari ve teknik personeliyle yüz yüze görüşmeler gerçekleştirilmiş, yarı yapılandırılmış sorular yöneltilmiştir. Bulgular, veri yönetim politikalarının genellikle merkezi yönetimle sınırlı kaldığını, taşra teşkilatlarında etkin uygulanmadığını göstermiştir. Veri anonimleştirme, silme ve yok etme süreçlerinde K-anonimlik, L-çeşitlilik ve T-yakınlık gibi teknik yöntemlerin kullanılmadığı; risk analizleri ve veri eğitimlerinin yetersiz olduğu tespit edilmiştir. Ayrıca, veri silme süreçlerinin çoğunlukla dosya sistemi düzeyinde pasifleştirme ile sınırlı olduğu ve bu durumun güvenlik risklerini artırdığı belirlenmiştir. Çalışmada, teknik prosedürlerin ulusal ve uluslararası düzenlemelerle uyumlu hale getirilmesi ve kamu kurumlarında uygulanabilir bir veri yönetimi çerçevesinin oluşturulması gerekliliği vurgulanmıştır.

Abstract Safeguarding personal data in public institutions is becoming increasingly important due to growing risks to individual privacy. This study examines legal and technical challenges in data management within the Turkish public sector, focusing on anonymization, deletion, and destruction processes. Semi-structured interviews were conducted with administrators and personnel from 103 public institutions in Aydın province. Findings reveal that data management policies are largely centralized and rarely implemented effectively in local branches. Technical methods such as k-anonymity, l-diversity, and t-closeness are not employed, and risk analysis procedures are insufficient or undocumented. Data deletion practices are often limited to superficial file system deactivation, increasing the risk of data recovery. Training programs on data governance are infrequent and lack depth. The study highlights the absence of standardized practices for secure data handling at the local level, despite existing national and international legal frameworks. It recommends developing an applicable and auditable data management framework for public sector institutions that aligns with privacy legislation and ensures organizational accountability. By addressing both regulatory and procedural gaps, this research contributes to the advancement of secure, transparent, and rights-respecting data governance in public administration.

Anahtar Kelimeler Veri yönetimi · Verilerin anonimleştirilmesi · Verilerin silinmesi · Verilerin yok edilmesi · Kişisel veriler

Keywords Data management · Data anonymization · Data deletion · Data destruction · Personal data

Atıf | Citation: Yavaş, H. & Henkoğlu, T. (2025). Legal and technical evaluation of anonymization, deletion and destruction processes related to data management in the public sector: The case of Aydın Province. *Bilgi ve Belge Araştırmaları Dergisi–The Journal of Information and Documentation Studies*, (23), 1-20. https://doi.org/10.26650/bba.2025.23.1577974

This work is licensed under Creative Commons Attribution-NonCommercial 4.0 International License.

2025. Yavaş, H. & Henkoğlu, T.

Sorumlu Yazar | Corresponding author: Haktan Yavaş haktanyavas@outlook.com

Yazar Notu Bu araştırma, 2023 yılında Aydın Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Bilişim Sistemleri Anabilim Dalında Haktan Yavaş tarafından Doç. Dr. Türkay Henkoğlu danışmanlığında tamamlanan "Kamu kurumlarının, verilerin anonimleştirilmesi, silinmesi ve yok edilmesine yönelik hukuksal sorumluluklar çerçevesinde değerlendirilmesi: Aydın ili örneği" başlıklı yüksek lisans tez çalışmasından üretilmiştir.

Author Note This study is derived from the master's thesis titled "Evaluation of Public Institutions within the Framework of Legal Responsibilities for the Anonymization, Deletion and Destruction of Data: The Case of Aydın Province," completed in 2023 by Haktan Yavaş under the supervision of Assoc. Prof. Türkay Henkoğlu at the Department of Management Information Systems, Graduate School of Social Sciences, Aydın Adnan Menderes University

Extended Summary

In an era where personal data flows have become integral to public service operations, ensuring data security, privacy, and legal compliance has emerged as a critical challenge for public institutions. This study investigates the data governance landscape within the Turkish public sector by focusing on the legal, technical, and organizational dimensions of anonymization, deletion, and destruction processes. Despite the existence of national regulations such as the Turkish Personal Data Protection Law (KVKK), discrepancies between central and regional data management practices persist. This research provides a comprehensive evaluation of these inconsistencies and offers practical recommendations to establish a harmonized and enforceable data governance framework.

The study employs a qualitative research design based on semi-structured interviews with managers, administrative staff, and IT personnel in 103 public institutions located in Aydın province. The data collection process involved face-to-face interviews guided by a flexible set of open-ended questions aimed at exploring institutional awareness, technical infrastructure, regulatory compliance, and procedural implementation concerning data protection and management.

The results reveal that although public institutions demonstrate a general awareness of data protection requirements, substantial gaps exist in terms of practical implementation. One key finding is that data governance strategies are often limited to central authorities, with regional offices lacking the autonomy or expertise to operationalize relevant procedures. This imbalance creates a significant vulnerability in the public sector's ability to maintain secure and legally compliant data practices across decentralized units.

From a technical standpoint, methods for data anonymization, such as k-anonymity, l-diversity, and t-closeness, are rarely employed, even though they are widely accepted in privacy-preserving data analytics. Most institutions still rely on rudimentary approaches such as logical deletion (file deactivation) instead of irreversible deletion or secure overwriting methods. This limited technical capacity elevates the risk of unauthorized access and data leakage, particularly in cases of external audits or cybersecurity incidents.

Institutional policies on data classification, access control, backup, and disposal are either missing or inconsistently applied across different departments. Where such policies exist, they tend to be centrally managed by IT units with minimal input or oversight from legal or administrative departments. Moreover, the absence of a unified data responsibility matrix means that individual accountability for data handling is often unclear, leading to fragmented implementation and poor coordination during data lifecycle transitions (e.g., from collection to deletion).

Another significant barrier identified is the inconsistent interpretation of the legal obligations outlined in the Regulation on the Deletion, Destruction, and Anonymization of Personal Data. Although this regulation derives from KVKK, many public institutions—especially those exempt from registration in the Data Controllers' Registry (VERBIS)—struggle with defining the scope and depth of their compliance duties. This ambiguity is particularly pronounced in public agencies operating in the domains of social services and local governance, where data-intensive programs are prevalent, but internal control mechanisms are weak or outdated.

The study also finds that employee training on data protection remains insufficient in both frequency and content. Central authorities may offer periodic training sessions, but regional units report limited participation and poor retention of information. As a result, frontline personnel who directly handle sensitive data often lack the necessary skills to identify potential vulnerabilities or apply preventive measures. This lack of capacity further compounds institutional exposure to risks such as unauthorized disclosures, legal sanctions, and reputational damage.

Importantly, the research underscores the need for a multi-dimensional data governance framework that bridges regulatory mandates with practical enforcement mechanisms. Such a framework should include standardized

procedures for data anonymization, deletion, and destruction; clearly defined roles and responsibilities; mandatory training programs; and periodic audits to ensure compliance and accountability. The establishment of a centralized but adaptable data governance model would also facilitate better coordination between central and local units, allowing for uniform implementation without compromising operational flexibility.

In conclusion, this study contributes to the broader discourse on public sector digital transformation by highlighting the critical role of secure data governance in ensuring citizen trust, institutional transparency, and regulatory compliance. As public institutions increasingly adopt digital tools for service delivery, investing in robust data management policies and infrastructures is no longer optional but essential. The findings are particularly relevant for policymakers, public administrators, and data protection officers seeking to align institutional practices with both national regulations and global standards in data privacy and security.

Giriş

Bilgi teknolojilerindeki hızlı gelişmeler, kişisel verilerin toplanması, işlenmesi ve kullanımı konusunda yeni zorlukları ortaya çıkarmıştır. Bu durum, bireylerin mahremiyet haklarının korunması ihtiyacını daha da önemli hale getirmiştir. Bankacılıktan sosyal medyaya, e-ticaretten bulut depolama hizmetlerine kadar tüm sistemler bir takım veri yönetim süreçlerine tabii tutulmaktadır. Özel sektörün veri süreçlerinde yaşanabilecek aksamalar bir takım hizmet duraksamalarına ve finansal kayıplara yol açabilecekken devletin veri işleme süreçleri merak konusudur. Toplumun veri depolama ve işleme ihtiyaçlarını karşılamak üzere internet tabanlı bulut bilişime olan güveninin artmasıyla, bu sistemlerin altyapısını oluşturan veri merkezlerinin kişisel ve kurumsal bilginin güvenliği hem devletlerin siber güvenlik stratejilerinde öne çıkmış hem de özel sektörün bilgi güvenliği uygulamalarında merkezi bir konuma ulaşmıştır (Knapp, Denney ve Barner, 2011).

Büyük veri çağında, kurum ve kuruluşlar veriye dayalı karar alma süreçlerini optimize etmek için büyük veri kümelerini analiz etmektedirler. Bu durum, rekabette üstünlük sağlamak adına önemli bir fırsat sunarken, aynı zamanda veri güvenliği konusunda yeni zorluklar ortaya çıkarmaktadır (Attaallah ve diğerleri, 2022). Artan veri hacmi, karmaşık veri yapıları ve veri paylaşımının yaygınlaşmasıyla birlikte, siber saldırılara karşı savunmasız hale gelme riski artmaktadır (Cheng, Liu ve Yao, 2017). Veri ihlalleri kurum ve kuruluşların itibarına zarar vererek müşteri güvenini sarsmakta ve önemli kayıplara yol açmaktadır (Shu, Zhang, Yao ve Feng, 2016).

Büyük veri ya da veri bilimi alanıyla hükümetler de ilgilenmektedir (Bates, Heitmueller, Kakad ve Saria, 2018). Özel firmaların eriştiği veriye kıyasla devasa boyutlara ulaşabilen kamu sektörünün bilgi erişimi ve veri işleme süreçlerinde kişisel veriler de yoğun olarak işlenmektedir (National Research Council, 1993). Çoğu zaman özel nitelikli kişisel veriler de kamu kurum ve kuruluşlarında işlenmekte, saklanmakta ve kurumlararasında paylaşılmaktadır. Bu durumda kamu kurum ve kuruluşlarının veri güvenliği hususunda yaptığı çalışmalar ve yatırımlara yönelik şüphe artmaktadır. Kamu sektörünün sebep olduğu veri ihlali vakaları da özel sektörde olduğu gibi yıkıcı itibar kayıplarına sebep olabilmektedir. Büyük veri kullanımı değerler ve ilkeler ile dengelenmediğinde, halkın güvenini azaltabilmektedir (Richards ve King, 2014). Kamu sektörünü ilgilendiren veri ihlalleri özel sektörde yarattığından daha büyük sonuçlara neden olabilmektedir. Neticede kurum ve kuruluşların güvenilirliğinin mahremiyetin korunmasına yönelik endişeler nedeniyle azalması, finans dünyasını ve yabancı yatırımları da ilgilendiren yıkıcı etkilere neden olabilmektedir (Liu, 2021).

Bu kapsamda kamu kurumlarının kişisel veri işlemedeki sorumluluklarının ortaya konabilmesi için sürece teknik ve hukuki olmak üzere iki perspektifte yaklaşılmalıdır. Hukuksal düzenlemeler kapsamındaki sorumlulukların yerine getirilebilmesi için ilgili politika ve yönergelerin hazırlanması gerekmektedir. Söz konusu kurum ve kuruluşlar neyi nasıl yapacağını politika ve yönergeler ışığında belirlemektedirler. Bu doğrultuda Türkiye'nin kültürel, siyasi, insani ve coğrafi açıdan heterojen yapısı göz önünde bulundurulduğunda,

Türkiye'nin 922 ilçesinde de uygulanabilecek veri yönetimi politikaları ile karşılaşılması beklenmektedir. Ancak kamu kurumlarının taşra teşkilatlarında uygulanması amacıyla hazırlanmış veri yönetim politikaları bulunmamaktadır. Veri koruma hukuku verinin adil ve insani biçimde işlenmesi, kurum ve kuruluşların veri işleme sürecinde bireylerin kişilik haklarını ve mahremiyetlerini güvenceye alması, kişisel verilerin nasıl yönetileceğiyle ilgili temel sınırların belirlenmesi amacıyla ortaya çıkmış ve zaman içinde birtakım evrimsel süreçlerden geçmiştir.

Geçmişten Günümüze AB ve Türk Hukuk Mevzuatında Veri Koruma İlkeleri

Kişisel veri koruma hukukunun kökenleri, 1970'lere kadar uzanmaktadır. 1970 yılında kabul edilen Hessen Veri Koruma Kanunu, dünyanın ilk ve en eski gizlilik kanunu olarak kabul edilmektedir (State Chancellery of Hessen - Minister for Digital Strategy and Innovation, 2023). Benzer şekilde, 1973'te İsveç Parlamentosu tarafından kabul edilen İsveç Kişisel Veri Kanunu da kişisel verilerin korunması konusunda öncü olmuştur (DSV Stockholm University, 2000). 1970'li yıllarda Avrupa'da başlayan veri koruma hareketleri, Amerika Birleşik Devletleri'nde de yankı bulmuştur. 1974 tarihli Birleşik Devletler Gizlilik Kanunu, federal kurumlar tarafından tutulan kişisel verilerin korunmasıyla ilgili düzenlemeler içermektedir (The United State Department of Justice, 2014).

Avrupa'da ise 1978 yılı kişisel veri koruma hukuku için dönüm noktası olmuştur. Almanya, Fransa, Danimarka, Norveç ve Avusturya gibi ülkeler, kişisel verilerin korunması amacıyla kapsamlı yasal düzenlemeler yapmışlardır. Almanya'nın "Federal Veri Koruma Kanunu", Fransa'nın "Bilgisayarlar, Veriler ve Özgürlüklere İlişkin Kanun"u" ve diğer Avrupa ülkelerindeki benzer kanunlar, kişisel verilerin işlenmesi süreçlerinde şeffaflık, hesap verebilirlik ve bireylerin haklarının korunması gibi temel ilkeleri vurgulamıştır (Datenschutz-Wiki, 2016; European Center for Digital Rights, 2017, 2020; European Union Agency for Fundamental Rights, 2018; University of Cambridge, 2020).

1980 yılında Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) kişisel verilerin korunması ve gizliliği konusunda uluslararası standartlar belirlemek amacıyla "OECD Gizlilik İlkeleri"ni yayınlamıştır. Bu ilkeler, veri koruma yasalarının geliştirilmesinde ve uygulanmasında küresel bir referans noktası olarak kabul edilmiştir (Cate, Cullen ve Mayer-Schonberger, 2013).

Avrupa ülkelerindeki ulusal veri koruma düzenlemeleri, 1995 yılında kabul edilen 95/46/EC Sayılı Veri Koruma Direktifi ile birleştirilmiştir. Bu direktif, kişisel verilerin işlenmesi ve serbest dolaşımına ilişkin standartları belirlerken, bireylerin temel hak ve özgürlüklerinin korunmasını amaçlamaktadır (Wong, 2012). Avrupa Veri Koruma Direktifi, daha sonra yerini AB'nin Genel Veri Koruma Tüzüğü'ne (GDPR) bırakmıştır, ancak GDPR'nin temelleri büyük ölçüde bu direktifin üzerine inşa edilmiştir (Wong, 2012).

1996 yılında kabul edilen Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA), Amerika Birleşik Devletleri'nde (ABD) sağlık bilgilerinin korunması için önemli bir düzenleme olarak öne çıkmaktadır. HIPAA, sağlık bilgilerinin korunması konusunda iki ana kural belirlemiştir. Bunlar; gizlilik kuralı ve güvenlik kuralıdır. Gizlilik kuralı, sağlık bilgilerinin korunması ve yetkisiz ifşaların önlenmesi için gerekli önlemleri tanımlarken, güvenlik kuralı elektronik sağlık bilgilerinin korunması için teknik ve idari güvenlik önlemlerini belirlemektedir (Appelbaum vd., 2009).

Avrupa Birliği (AB), 2002 yılında elektronik iletişimde gizliliği korumak amacıyla e-Gizlilik Direktifi'ni kabul etmiştir. Bu direktif, özellikle çerezler, elektronik pazarlama ve iletişim verilerinin gizliliği gibi konularda düzenlemeler getirmiştir (Gonzalez, De Hert ve Papakonstantinou, 2020).

Asya-Pasifik Ekonomik İşbirliği (APEC), 2004 yılında kişisel verilerin sınır ötesi akışını kolaylaştırmak ve veri koruma standartlarını uyumlu hale getirmek amacıyla bir gizlilik çerçevesi oluşturmuştur. APEC

Gizlilik Çerçevesi, üye ülkeler arasında veri koruma uygulamalarının uyumlu hale getirilmesini ve veri transferlerinde güvenliğin sağlanmasını amaçlamaktadır (*APEC Privacy Framework*, 2005).

2016 yılında uygulamaya konulan Privacy Shield, AB-ABD arasındaki kişisel veri transferleri için güvenli bir yasal temel oluşturmayı amaçlamaktadır. Ancak 2020 yılında Avrupa Adalet Divanı'nın Schrems II kararında, ABD'deki veri koruma düzenlemelerinin AB vatandaşlarının haklarını yeterince korumadığı tespit edilmiş ve Privacy Shield geçersiz kılınmıştır. Karar, uluslararası veri transferlerine yönelik güvenlik tedbirlerinin daha da sıkılaştırılmasını ve alternatif yasal mekanizmaların kullanılmasını zorunlu hale getirmiştir (Neiazy, 2021). Schrems II kararı, ismini Maximilian Schrems adlı Avusturyalı aktivistten almaktadır. Schrems, 2015 yılında AB-ABD arasındaki bir önceki veri transferi mekanizması olan Safe Harbor'un geçersiz kılınmasını sağlamış ve ardından Privacy Shield'e karşı yeni bir dava açmıştır. Bu yeni dava, ilk karardan sonra olduğu için Schrems II olarak adlandırılmaktadır (Bradford, Aboy ve Liddell, 2021).

2018 yılında yürürlüğe giren GDPR, kişisel verilerin korunması konusunda tüm AB vatandaşları için önemli bir güvenlik katmanı oluşturmaktadır. GDPR'nin temel ilkeleri arasında veri minimizasyonu, amaçla sınırlı işleme ve şeffaflık yer almaktadır. Bu ilkeler, veri sorumlularının topladıkları ve işledikleri veriler konusunda hesap verebilir olmalarını zorunlu kılmaktadır. Veri işleme faaliyetleri, veri sahibi bireylerin açık rızasına veya belirli yasal gerekçelere dayanmak zorundadır (Burenok, 2023). Kurum ve kuruluşlar büyük miktarlarda vatandaş verisi toplarken, bu verilerin işlenmesi ve korunması konusunda hem yasal hem de etik sorumlulukları bulunmaktadır (Garg, Verma ve Kumar, 2024). GDPR kişisel verilerin anonimleştirilmesi konusunda önemli yeni düzenlemeleri içermektedir. Anonimleştirme, kişisel verilerin bireylerle ilişkilendirilemeyecek hale getirilmesi sürecidir. Bu süreçle bireylerin kimlikleri yeniden tespit edilemeyecek hale getirilebilmektedir (Cormode ve Srivastava, 2010). Mevzubahis yöntem, GDPR kapsamında kişisel verilerin korunması ilkelerinden biri olan "Veri Minimizasyonu" (Data Minimization) ilkesiyle de yakından ilişkilidir. Bu ilke, kişisel verilerin sadece gerekli olduğu sürece toplanması ve işlenmesini gerektirmektedir. Anonimleştirilmiş veriler kişisel veri olarak kabul edilmemekte ve GDPR'ın uygulama alanı dışında kalmaktadır (Avrupa Konseyi, 2016). Bununla birlikte, anonimleştirme işleminin doğru yapılmadığı durumlarda, bireylerin yeniden tanımlanma riski doğabilmekte ve bu durumda veri ihlali söz konusu olabilmektedir (Bolognini ve Bistolfi, 2017).

Kişisel verilerin korunmasına yönelik düzenlemeler, dijitalleşmenin hızlanmasıyla dünya genelinde büyük önem kazanmıştır. Türkiye de bu konuda önemli adımlar atmış ve 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu (KVKK) ile kişisel verilerin işlenmesi, korunması, silinmesi ve anonimleştirilmesi süreçlerini düzenlemiştir. KVKK, GDPR'ye paralel olarak yapılandırılmış olup, özellikle anonimleştirme, silme ve yok etme süreçlerine yönelik kuralları da düzenlemektedir (Ersoy, 2019). KVKK'da kişisel verilerin işlenmesi ve korunmasına ilişkin kurallarla birlikte, bireylerin haklarına ve veri sorumlularına ilişkin yükümlülükleri de tanımlanmaktadır.

KVKK'nın öncelikli olarak dikkate alınması gereken temel ilkeleri şunlardır;

- Aydınlatma Yükümlülüğü: Veri sorumluları, veri sahiplerini kişisel verilerinin işlenme amacı, işlenecek veri kategorileri ve aktarılacak üçüncü taraflar gibi konularda bilgilendirme yükümlülüğüne sahiptir (Ersoy, 2019).
- Açık Rıza: Kişisel verilerin işlenmesi için ilgili kişinin açık rızası gerekmektedir. Ancak, uygulamada bu rızanın nasıl alınacağı, özellikle çocuklar gibi özel kategorilerde belirsizliklere neden olabilmektedir (Dülger, Kahraman ve Yalçın, 2021).
- Veri Sahiplerinin Hakları: KVKK, veri sahiplerine kişisel verilerinin işlenip işlenmediğini öğrenme, verilerin silinmesini, düzeltilmesini veya anonimleştirilmesini talep etme hakkı tanır. Veri sorumlularının bu talepleri yerine getirme yükümlülüğü bulunur (Yılmaz, Arıkan, Su ve Yürekten, 2020).

KVKK, Anayasa'nın 20. maddesinde düzenlenen özel hayatın gizliliği hakkıyla da doğrudan ilişkilidir. Bu madde, kişisel verilerin korunması hakkını anayasal güvence altına alırken, KVKK bu hakkın somut olarak uygulanmasını sağlayan yasal düzenlemeleri içermektedir (Helvacıoğlu ve Stakheyeva, 2017). Bununla beraber, veri güvenliğine dair yönetmelikler veri sorumlularının bu konudaki yükümlülüklerini detaylandırarak yasal çerçeveyi oluşturmaktadır (Dülger, 2021).

Veri Anonimleştirme

KVKK'nın 7. maddesi, kişisel verilerin işlenme amaçlarının sona ermesi durumunda bu verilerin silinmesi, yok edilmesi ya da anonim hale getirilmesi gerektiğini düzenlemektedir. KVKK çerçevesinde veri anonimleştirme işlemi, verilerin bireyler ile ilişkilendirilemeyecek hale getirilmesini zorunlu kılmaktadır. Uygulamada kimliksizleştirme işlemleriyle verilerin toplanması, işlenmesi, arşivlenmesi, dağıtılması veya yayınlanması aşamalarında gizlilik riskinin azaltılması yönteminin de tercih edildiği görülmektedir (Garfinkel, 2015). Yalnızca kimliksizleştirilmiş verilerin gizlilik anlamında yeterli olduğunu söylemek mümkün değildir. Kayıt altına alınan veriler kimliksizleştirilmiş olsa dahi belirli bir kural setine göre tasnif ediliyorsa farklı veri setleri kullanılarak kişilerin kimlikleri tespit edilebilmektedir (Miller, Herrera, Jun, Landay ve Bailenson, 2020). Bu sebeple sıklıkla anonimleştirme süreçlerine başvurulduğu görülmektedir. Anonimleştirilmiş bir veri kümesi, içinde yer alan her kaydın en azından diğerlerinden ayırt edilemez olduğu veri kümesi anlamını taşımaktadır (Bayardo ve Agrawal, 2005).

Veri anonimleştirme ve anonimlik düzeyinin ölçülmesi amacıyla kullanılan başlıca teknikler şunlardır;

- **K-Anonimity (K-Anonimlik):** K-anonimlik, bir bireyin veri kümesinde en az k farklı bireyle ayırt edilemez hale geldiğini ifade eder (M E Nergiz, Clifton ve Nergiz, 2009). K ne kadar büyükse, anonimlik seviyesi o kadar yüksek olur.
- **L-Diversity (L-Çeşitlilik):** K-anonimity'nin bazı durumlarda yetersiz kalabileceğini göstermek için geliştirilen L-diversity, her bir anonimleşmiş grup içinde hassas niteliklerin (örneğin hastalık türü, gelir düzeyi) yeterli çeşitlilikte olmasını sağlar (Machanavajjhala, Kifer, Gehrke ve Venkitasubramaniam, 2007). Her anonimleşmiş grup en az L farklı hassas niteliğe sahip olmalıdır.
- **T-Closeness (T-Yakınlık):** L-diversity'nin de yeterli olmadığı durumlar için önerilen bu yöntem, her anonim grup içinde hassas niteliklerin dağılımının tüm veri kümesindeki dağılıma ne kadar yakın olduğunu ölçer (Li, Li ve Venkatasubramanian, 2007).
- **δ-Presence (Delta-Prensence):** Bu yöntem, bir bireyin bir veri kümesinde olup olmadığının belirlenme olasılığını ölçer (Nergiz, Atzori ve Clifton, 2007).

Anonimleştirme KVKK'nın temel bileşenlerinden biri olup, kişisel verilerin hukuka aykırı işlenmesini engellemek amacıyla uygulanmaktadır. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin (CBDDO) Bilgi ve İletişim Güvenliği Rehberi, bu süreçte izlenecek adımları ve alınması gereken teknik önlemleri detaylandırmaktadır (Yılmaz vd., 2020).

Veri Yok Etme

Verilerin yok edilmesi işlemi, verilerin elektronik ortamda veya fiziksel olarak geri döndürülemez şekilde imha edilmesi anlamına gelmektedir. Özellikle hassas verilerin yok edilmesi, veri güvenliği ihlallerinin önüne geçmek için kritik öneme sahiptir (Dülger, 2021). Uygulamada, veri silme ve yok etme süreçlerinde karşılaşılan başlıca zorluklar arasında, verilerin tam anlamıyla yok edilmesinin teknik olarak nasıl sağlanacağı ve silinen verilerin geri getirilemez hale dönüştürülmesinin nasıl garanti edileceği bulunmaktadır. Bu konuda veri sorumlularının VERBİS'e kayıt ve raporlama yükümlülükleri bulunmaktadır.

Bulut tabanlı veri yönetimi sistemlerinde veri yok etme işlemi, verilerin yalnızca belirli bir sunucudan değil, dünya çapındaki birçok yedekten ve depolama ağından da kaldırılmasını gerektirir. Veri yok etme

süreci, veri silme işlemi ile benzerlik gösterse de teknik açıdan verinin tamamen fiziksel olarak imha edilmesi anlamına gelmektedir. Bu süreç, genellikle veri taşıyıcılarının (örneğin sabit diskler) yok edilmesi veya üzerinde yer alan bilgilerin geri dönüşümü mümkün olmayacak şekilde silinmesiyle gerçekleştirilir (Güler, 2020, s. 195-215). Özellikle bulut tabanlı veri yönetim sistemleri ve taşınabilir veri cihazları üzerindeki verilerin imhası önem taşımaktadır (Kuner, Bygrave, Docksey, Drechsler ve Tosoni, 2021).

Veri yok etme işlemleri için kullanılan başlıca yöntemler aşağıda sıralanmıştır;

- **Fiziksel Yok Etme:** Depolama medyalarının (örneğin sabit diskler, SSD'ler, optik diskler) delme, parçalama, eritme gibi yöntemlerle fiziksel olarak imha edilmesi, verilerin geri dönüşü olmayan şekilde ortadan kaldırılmasını sağlar (Kissel, Regenscheid, Scholl ve Stine, 2014).
- **Manyetik Boşaltma (Degaussing):** Manyetik veri depolama birimlerinin güçlü bir manyetik alana maruz bırakılarak verilerin okunamaz hale getirilmesi yöntemidir. Bu sayede manyetik tabanlı veriler kurtarılamaz düzeye indirilir (Swanson ve Guttman, 1996).
- **Mantıksal (Yazılımsal) Güvenli Silme:** Verilerin bulunduğu sektörlere birden çok kez rastgele veya özel desenlerde veri yazılmasıyla geri getirilemez kılınması sağlanır. Bu yöntem, "Gutmann yöntemi" veya "DoD 5220.22-M" standardı gibi çoklu geçiş algoritmaları kullanarak verilerin kurtarılmasını engeller (Gutmann, 1996; U.S. Department of Defense, 1995).
- **Kriptografik Silme:** Verilerin önceden şifrelenmesi ve şifreleme anahtarının güvenli bir şekilde yok edilmesi esasına dayanır. Depolama cihazları üzerindeki veriler aslında kalıcı olarak silinmez; ancak anahtarın yok edilmesiyle birlikte veriler deşifre edilemez hale geldiğinden etkin bir yok etme yöntemi olarak kabul edilir (Kissel vd., 2014).

Veri Minimizasyonu

Veri minimizasyonu, kişisel verilerin belirli bir amaca hizmet edecek şekilde toplanması ve işlenmesi gerektiğini vurgulayan veri koruma ilkesidir. Bu ilkenin temel amacı, gereksiz veri toplamanın ve uzun süre saklamanın doğurabileceği riskleri minimize etmektir (Anderson ve Von Seck, 2020; Wouters vd., 2021). Veri minimizasyonu ilkesi, aynı zamanda bireylerin veri işleme süreçlerindeki güvenliğini sağlamak ve gereğinden fazla veri toplamanın neden olabileceği etik ve yasal sorunları önlemek için de geliştirilmiştir (Ganesh, Tran, Shokri ve Fioretto, 2024). Veri minimizasyonu, bu bağlamda hem bireylerin mahremiyetini hem de veri güvenliğini koruyan bir unsur olarak kabul edilmektedir (Shanmugam, Diaz, Shabanian, Finck ve Biega, 2022). Büyük veri analitiği ve makine öğrenimi gibi teknolojiler, çok büyük miktarda veriye dayandığından, bu ilkenin uygulanması karmaşık hale gelebilmektedir. Ancak, temel veri koruma ilkelerinden biri olarak veri minimizasyonu, teknolojik gelişmelerin bireylerin mahremiyetini tehdit etmemesini sağlamak için kritik öneme sahiptir (Goldsteen, Ezov, Shmelkin, Moffie ve Farkash, 2022).

Araştırmanın Amacı ve Soruları

Türkiye'deki kamu kurumlarının taşra teşkilatlarında uygulanması hedeflenen herhangi bir veri yönetim politikasının olup olmadığı ve taşra teşkilatlarında verinin nasıl yönetildiği bilinmemektedir. Son yıllarda bilgi ve iletişim teknolojilerinin kullanımına bağlı olarak artan veri ihlalleri (Avllazagaj, Ayday ve Çiçek, 2016; DataBreaches LLC, 2016), kurumlarda işlenen kişisel verilerin güvenliğine yönelik endişelerin de artmasına neden olmaktadır. Bu çalışmada Aydın İli'ndeki (Türkiye) kamu kurumlarının veri güvenliğinin sağlanmasına yönelik yasal sorumluluklarının belirlenmesi, kurumların riskleri nasıl yönettiklerinin ve uygulamalarının mevzuata uygunluğunun araştırılması amaçlanmaktadır. Bu kapsamda Aydın mülki idare amirliği içerisinde faaliyet gösteren kamu kurumları belirlenerek; bu kurumların, verilerin anonimleştirilmesine, silinmesine ve yok edilmesine yönelik faaliyetlerinin hukuksal çerçevede değerlendirilmesi hedeflenmiştir. Araştırmadan

elde edilen bulgulara bağlı olarak sunulan önerilerin, kamu yararına faaliyet gösteren tüm kuruluşlara ve özel sektöre de katkı sağlayacağı düşünülmektedir.

Bu araştırmada aşağıdaki sorulara yanıt bulunması amaçlanmıştır;

1. Kurumda kişisel verilerin anonimleştirilmesi, silinmesi ve yok edilmesi için politikalar geliştirilmiş midir? Geliştirilmiş ise bu politikalar neleri kapsamaktadır?
2. Kurumda veri sorumlusu görevi yazılı olarak tanımlanmış mıdır? Tanımlanmışsa sorumlulukları ve yetkileri nelerdir?
3. Kurumda elektronik ortamda yer alan bilgilerin arşivlenmesi hangi politika ve prosedürlere göre yapılmaktadır?
4. Kurumda kişisel verilerin korunmasına yönelik riskler nasıl yönetilmektedir?
5. Kişisel ve kurumsal verilerin depolandığı cihazlarla ilgili gereksinimler tanımlanmış mıdır?
6. Verilerin anonimleştirilmesi, silinmesi ve yok edilmesine yönelik sorumluluklar belirlenmiş midir?
7. Kurum içinde veri yönetim süreçleri ile ilgili çalışanlara yönelik olarak eğitsel çalışmalarda kullanılan eğitim materyalleri nelerdir?

Araştırmanın Yöntemi

Kamu kurumlarında veri yönetim süreçlerinin halihazırda nasıl yürütüldüğünü ortaya koymak ve kurumların kanuni sorumluluklarını karşılama yetisini tespit edebilmek için betimleme yöntemi kullanılmıştır. Betimleme yöntemi, öznelerin mevcut durumunu, çevreleri ve etkileşimleriyle birlikte zengin ayrıntılar sunarak anlamayı amaçlar (Rubin ve Babbie, 2016). Betimlemenin amacı, bireyleri, olayları, olguları veya durumları kendi koşulları içinde olduğu gibi inceleyip tanımlamaktadır (Siedlecki, 2020).

Teknik ve hukuki soruların daha iyi anlaşılması, yanıtlama oranının yüksek olması ve kişisel veri güvenliğiyle ilgili farkındalığın gözlemlenmesi için yüz yüze görüşme yöntemi uygulanmıştır. Araştırma kapsamında Aydın ili kurumlarının yöneticileri ile görüşülmüştür. Görüşme sırasında yöneltilen yarı yapılandırılmış anket sorularıyla kurum politikaları, personel farkındalığı, teknik yatırım ve çalışmalar hakkında veri toplanmıştır. Uygulanan anket soruları kamu kurumlarının veri yönetim süreçleriyle ilgili bilgi almayı hedeflerken aynı zamanda kurum yöneticilerinin farkındalığını artırmayı ve onları bilinçlendirmeyi de hedeflemektedir. Görüşme ve anketlerin hazırlanmasında, uluslararası bilgi güvenliği standartları, diğer kurumlarda yapılan denetimlerin raporları, kişisel verilerin korunmasına yönelik etik ilkeler, GDPR, KVKK ve ilgili hukuksal düzenlemeler dikkate alınmıştır. Bu makaleye ilişkin araştırma için Aydın Adnan Menderes Üniversitesi Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu'ndan (31906847/050.04.04-08-329) izin alınmıştır.

Araştırma Evreni ve Örneklem

Araştırma evreni, Aydın mülki idare sınırları içinde faaliyet gösteren 103 kamu kurumu ve kuruluşundan oluşmaktadır. Araştırmada örneklem alınmamış, tüm evren üzerinde çalışılmıştır. Bu kurumların yöneticileriyle yapılan yüz yüze görüşmeler sonucunda elde edilen veriler analiz edilmiştir.

Katılımcılara yüz yüze görüşme esnasında 34 adet anket sorusu yöneltilmiştir. Bu soruların 19'u politika, prosedür ve ilkelerle ilgiliyken, 8'i teknik yöntemlerle, 5'i hukuki sorumluluklarla ve 2'si kurum içi eğitim süreçleriyle ilgilidir. Anket soruları literatür kısmında belirtilen teknik konular, ulusal ve uluslararası veri hukuku bağlamında hazırlanmıştır.

Bulgular

Kamu Kurumlarının Veri Yönetimine Dair Uyguladıkları Politikalar ve Teknik Çalışmalar

İl müdürlükleri düzeyinde ziyaret edilen kamu kurumlarının internet sitelerinde yapılan içerik analizine göre, %57,3'ünün (n=59) veri güvenliği politikası içerdiği tespit edilmiştir. Ancak, bu politikaların yalnızca %14,6'sı (n=15) veri silme ve yok etme süreçlerine dair açıklama içermektedir. Ayrıca politikaların hiçbirinde anonimleştirme kavramına değinilmemiş; bu konu ne ilkesel ne de teknik düzeyde ele alınmıştır. Sorumluluk matrisi konusundaki incelemede ise çoğu kurumda bir sorumluluk matrisi oluşturulmadığı görülmüştür. Bu durumda, çalışanlar olası aksaklıklarda doğrudan kurum müdürü ile iletişime geçmekte veya teknik desteği kurum içindeki teknisyenlerden ya da teknik bilgiye sahip diğer personelden almaktadır.

Tablo 1

Kamu Kurumlarının Veri Yönetimine Dair Uyguladıkları Politikalar ve Teknik Çalışmalar

	Evet		Hayır	
	N	%	N	%
Kurum genelini kapsayan, veri yönetimi süreci bileşenleri ile ilintili bir sorumluluk matrisi oluşturulmuş mudur?	0	0	103	100
Kurum nezdinde kullanılan ya da bulundurulan kişisel ya da kurumsal veriler için bir erişim politikası mevcut mudur?	0	0	103	100
Kurum çalışanlarını kapsayan bir veri erişim matrisi oluşturulmuş mudur?	0	0	103	100
Merkezi veri depolama sistemi kullanılıyor ise bu sistemlere dijital erişim sınırlandırması getirilmiş midir?	36	100	-	-
Merkezi veri depolama sistemi kullanılıyor ise bu sistemlerin bulunduğu mekân için erişim sınırlandırması getirilmiş midir?	36	100	-	-
Kişisel veri toplanırken Kişisel Verilerin Korunması Kanunu'nun 5'inci maddesine istinaden ilgili kişinin açık rızası alınıyor mu?			103	100
Özel nitelikli kişisel veriler toplanıyor mu?	27	26,2	76	73,8

Tablo 1 verilerine göre, incelenen kurumların hiçbirinde operasyonel bilgisayarlara yönelik bir erişim politikası bulunmamaktadır. Tablodaki sonuçlar, taşra teşkilatlarındaki veri güvenliği açıklarını göz önüne sermekte ve kapsamlı erişim politikalarının oluşturulması gerektiğini ortaya koymaktadır. Merkez teşkilattan sağlanan bilişim sistemlerinde kullanıcı oturumları üzerinden sağlanan kategorizasyon ve erişim sınırlamaları uygulanmakla birlikte, taşra teşkilatlarında bu tür sistematik erişim sınırlamaları mevcut değildir. Bu nedenle, taşra teşkilatlarındaki bilgisayarlarda bulunan hesap tabloları veya PDF formatındaki dijital belgeler denetim olmaksızın diğer çalışanlara ya da kurum bilgisayarlarına aktarılabilmektedir.

Katılımcılara Tablo 1'de listelenen sorular yöneltilirken, sorumluluk matrisine ve erişim politikasına dair ayrıntılı açıklamalar yapılarak, isimlendirme farklılıklarından kaynaklanabilecek yanlış anlamaların önüne geçilmesi hedeflenmiştir. Erişim politikası, çalışan kategorilerine göre erişim yetkilerini, veri güvenliği seviyelerini ve hangi verilerin hangi yetki seviyesinde erişilebilir olduğunu tanımlamaktadır. Erişim politikasının yetki kademelerine uygun erişim sınırlarını belirleyerek, veri ihlallerini ve yetkisiz erişim risklerini en aza indirmesi beklenmektedir. Bununla birlikte, erişim politikasının etkin bir şekilde uygulanması için, hangi durumlarda ve hangi personelin erişim talep edebileceği ya da yetki artırımı yapabileceği de açıkça belirtilmelidir.

Erişim politikasına ek olarak, sorumluluk matrisi olası senaryolarda hangi personelden rapor ya da bilgi talep edileceğini açık olarak ortaya koymalıdır. Ayrıca, personelin sorumlu olduğu alt sistemlerin işleyişiyle birlikte, erişim politikası çerçevesinde hangi seviyede erişim yetkisine sahip olduğu da tanımlanmalıdır. Bu sayede, kurum çalışanları bir sorun olması halinde kiminle iletişime geçmesi gerektiğini veya hangi

protokolü izlemesi gerektiğini kolaylıkla öğrenebilecektir. Sorumluluk matrisinin ve erişim politikasının bulunmaması, bilgi sistemlerinin sürdürülebilirliğine yönelik sorunları derinleştirerek çözüm sürecini önemli ölçüde uzatabilmektedir.

Merkezi veri depolama sistemleri kullanan kurumlarda, bu sistemlerin genellikle güvenlik kamerası kayıtları gibi dijital varlıkların depolanması amacıyla kullanıldığı tespit edilmiştir. Merkezi teşkilatlarca geliştirilen kapsamlı bilgi işlem yazılımları kullanılmakla birlikte, taşra teşkilatlarında iş zekâsı, kurumsal kaynak planlama yazılımları veya diğer merkezi çözümler mevcut değildir. Bu depolama sistemlerine erişim yalnızca bilgi işlem personeli veya kurum yöneticileriyle sınırlandırılmıştır.

Açık rıza almayan kurumlara, KVKK 5. maddenin 2. fıkrasında belirtilen koşullardan hangilerinin sağlandığı sorulmuştur. Kurumların %1'i (n=1) c bendindeki, %25,3'ü (n=26) ç bendindeki, %26,2'si (n=27) ise ç ve e bentlerindeki koşulları sağladığını belirtmiştir. %17,5'i (n=18) e ve f bentlerindeki, %12,6'sı (n=13) c, ç, e ve f bentlerindeki koşulları karşıladığını ifade etmiştir. Bunun yanı sıra, %17,5'i (n=18) ise hiçbir özel koşulun gerçekleşmediğini belirtmiştir. Ayrıca kurumların operasyonel bilgisayarlarında ve veri depolama ortamlarında bulundurulan verilerin saklama sürelerine dair herhangi bir düzenleme yapılmadığı ve dijital veriler için azami bulundurma veya arşivleme süresi belirlenmediği gözlemlenmiştir. Taşra teşkilatlarındaki kişisel verilerin imhasında ise sorumluluğun hangi birime ait olduğu net değildir.

Elektronik belge yönetim sistemleri gibi sistemlerde işlenen verilerin çoğu dijital kaynaklardan elde edilmekte, açık rıza alma süreci ise dijital kanallar üzerinden gerçekleşmektedir. Ancak, yerel düzeyde toplanan kişisel verilerde açık rıza alınmamakta ve bu durum KVKK'nın 5. maddesinin 2. fıkrasındaki c, ç, e veya f bentlerine dayandırılmaktadır. Bununla birlikte, açık rıza alınamadığı durumlarda herhangi bir iç komisyon kararı, kurul onayı veya bilgilendirme çalışması yapılmadığı tespit edilmiştir.

Katılımcı kurumların %26,2'si özel nitelikli veri topladığını ifade etmiştir. KVKK'nın 6. maddesinin 3. fıkrası gereğince, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetleri gibi amaçlarla özel nitelikli veriler, sır saklama yükümlülüğü bulunan kişiler veya yetkili kurumlarca açık rıza olmaksızın işlenebilmektedir. Bu bağlamda, özel nitelikli veri işlediğini belirten kurumların yasal koşulları sağladığı görülmektedir.

KVKK'nın 12. maddesi gereği alınan teknik ve idari tedbirlere yönelik sorulara verilen cevaplarda, katılımcılar çoğunlukla merkez teşkilatları tarafından yönetilen bilgi sistemlerine atıfta bulunmuştur. Taşra teşkilatlarının veri yönetim süreçlerine etkin katılımını sağlamak için bölgesel risk analiz ekipleri oluşturulmalı ve bu ekipler tarafından hazırlanan raporlar merkezi yönetimle entegre edilmelidir.

Kurum Yöneticilerinin Veri Yönetimine İlişkin Sorumluluk Bilinci

Araştırmada incelenen taşra teşkilatlarının hiçbirinin veri sorumlusu belirlemediği, katılımcıların da bu görevin merkezi teşkilatlarına ait olduğunu düşündüğü tespit edilmiştir. On katılımcı dışında, kurum yöneticileri KVKK'nın 5. maddesindeki "gerçek veya tüzel kişilik" ifadesi nedeniyle taşra teşkilatlarına bu konuda bir sorumluluk yüklenmediğini bilmemektedir. Ayrıca dijital belgelerin saklanması, taşınması veya imhasında oluşabilecek zarar ve risklerin tam olarak anlaşılmadığı gözlemlenmiştir.

Kamu Kurumlarında Veri Toplama ve Tasnif Yöntemleri

Kamu kurumlarının tamamında veri sınıflandırmasına yönelik sistematik bir çalışma olduğu tespit edilmiştir. Araştırmaya dahil edilen tüm kurumlar, "Kurum nezdinde kullanılan veya bulundurulan kişisel ya da kurumsal veriler için bir gizlilik derecesine ya da kişisel/kurumsal veri olma durumuna göre sınıflandırma politikası mevcut mudur?" sorusuna "evet" cevabını vermiştir. Bu sınıflandırma politikası, Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'e dayandırılmaktadır. Yönetmelik kapsamında,

belgeler üç milli gizlilik derecesine ayrılmaktadır: Çok Gizli, Gizli ve Hizmete Özel. Çok Gizli ve Gizli belgelerin ifşasının Devletin menfaatlerine, güvenlik ve teknoloji faaliyetlerine zarar verebileceği belirtilmektedir (T.C. Resmî Gazete, 2022). Ancak araştırmaya dahil edilen kamu kurumlarının taşra teşkilatlarında bu kategorilere giren belge ya da bilgilerin bulunmadığı, dolayısıyla taşra teşkilatlarındaki tüm verilerin Hizmete Özel olarak sınıflandırıldığı ifade edilmiştir.

Kullanım süresi dolan kişisel veya kurumsal verilerin arşivlenmesine yönelik bir planlamanın yapılıp yapılmadığı sorulduğunda, tüm katılımcılar arşivleme planlaması yapıldığını belirtmiştir. Geleneksel bilgi ve belgelerin arşivlenmesi konusunda, katılımcıların tamamı, Devlet Arşiv Hizmetleri Hakkında Yönetmelik (2019) gereğince, basılı belgelerin arşivlenmesi, imha edilmesi veya Devlet Arşivleri Başkanlığına gönderilmesi süreçlerine dair bir planlama yapıldığını ifade etmişlerdir. Bu yönetmelik, kâğıt üzerindeki belgelerin arşivlenmesi ve ilgili süreçlerin nasıl yürütüleceği konusunda bir çerçeve sunmaktadır (T.C. Resmî Gazete, 2019).

Veri Yönetimi Hususunda Risk Faktörleri ve Risk İşleme

Tablo 2'de yer alan bulgulara göre, araştırmaya dahil edilen kamu kurumlarının %45,6'sı (n=47) genel merkez teşkilatları tarafından risk analizi yapıldığını belirtmiştir. Ancak bu risk analizlerine ilişkin herhangi bir yazılı belge bulunmamakta ve kurum yöneticilerine risk faktörleri sorulduğunda, bu bilgilerin araştırmacı talep ederse merkezi teşkilatlarına başvurularak elde edilebileceği ifade edilmiştir. Ayrıca yerel teşkilatlarda veri güvenliği konusunda risk yönetimi yapılmadığı tespit edilmiştir.

Tablo 2

Risk Analizi ve Risk İşleme

	Evet		Hayır	
	N	%	N	%
Kurumunuzda veri güvenliğinin sağlanmasına yönelik bir risk analizi yapılmış mıdır?	47	45,6	56	54,4
Kurumunuzda risk analizi yapılmış ise risk analizine istinaden risk işleme yapılmış mıdır?	47	45,6	56	54,4

Risk işleme konusundaki soruya verilen yanıtlar incelendiğinde, tüm kurumların risk işleme süreçlerinin yürütüldüğünü belirttiği görülmektedir, ancak bu konuda da herhangi bir yazılı belgeye ulaşılamamıştır. Görüşmeler sırasında yöneltilen sorulara rağmen, kurumlarda risk işleme süreçlerine yönelik alınan kararlar veya uygulamalar hakkında bilgi edinilememiştir. Risk işleme süreçlerinin merkez teşkilatları tarafından yürütülen ilkesel eylemler olduğu varsayılmaktadır. Tüm kurumların risk işleme yöntemi olarak riskten kaçınma ve riski azaltma stratejilerini tercih ettiği anlaşılmıştır; riskin kabulü ya da transferi yöntemlerine dair herhangi bir bulguya rastlanmamıştır.

Araştırma kapsamında veri toplanan kamu kurumlarının %10,7'si (n=11) son altı ay içinde, %31,1'i (n=32) ise iki yıldan daha uzun süre önce risk analizi gerçekleştirmiştir. Bununla birlikte risk analizi gerçekleştirmiş kurumların %3,9'u (n=4) risk analizinin ne zaman yapıldığını bilmemektedir. Katılımcıların %54,4'ü (n=56) ise herhangi bir risk analizi yapılmadığını belirtmiştir.

Kamu Kurumlarında Veri Saklama Yöntemleri

Tablo 3'te görüldüğü gibi, araştırmaya dahil edilen kamu kurumlarının tamamında Elektronik Belge Yönetim Sistemi (EBYS) kullanılmaktadır. Katılımcılardan yalnızca 2'si, "Kurumda kullanılan ya da bulundurulan kişisel veya kurumsal verilerin depolandığı merkezi bir veri depolama sistemi mevcut mudur?" sorusuna "evet" yanıtını vermiştir. Araştırmadaki tüm kamu kurumlarında en az bir adet sistem odası olduğu tespit

edilmiştir. Bazı sistem odalarında veri depolama donanımları bulunsa da bu soruya "hayır" yanıtı veren kurumlarda varsa bu sistemler merkez teşkilatının bilgi işlem birimleri tarafından yönetilmektedir. Ayrıca bazı kurumlarda güvenlik kameralarının görüntülerinin depolandığı fakat bu sistemlerin uzaktan erişime kapalı olduğu görülmüştür. Sisteme fiziksel erişim kısıtlaması ise sadece geleneksel kilit mekanizmaları ile sağlanmış, bilgi sistemleri kullanılmamıştır. Merkezi veri depolama sistemlerinde kullanılan donanımlara ilişkin soruya katılımcıların tamamı sabit disk yanıtını vermiştir. Taşra teşkilatlarının hiçbirinin dijital yedekleme sistemleri kullanmadığı tespit edilmiştir.

Tablo 3

Kamu Kurumlarında Veri Depolama ve Bulundurma Yöntemleri

	Evet		Hayır	
	N	%	N	%
Belge yönetimi sürecinde elektronik belge yönetim sistemi kullanılıyor mu?	103	100	0	0
Kurum nezdinde kullanılan ya da bulundurulan kişisel ya da kurumsal verilerin depolandığı merkezi bir veri depolama sistemi mevcut mudur?	36	35	67	65

Verilerin Yok Edilmesi, Silinmesi ve Anonimleştirilmesiyle İlgili Süreçler

Tablo 4'te, kamu kurumlarında veri silme, yok etme ve anonimleştirmeye dair bulgular yer almaktadır. KVKK'nın 7. maddesinin 1. fıkrasına göre, kişisel verilerin veri sorumlusu tarafından re'sen veya ilgili kişinin talebi üzerine silinmesi, imha edilmesi veya anonim hale getirilmesi gerektiği belirtilmektedir. Araştırmaya katılan kurumlarda, en azından kişisel verilerle ilgili olarak silme, yok etme veya anonimleştirme sorumluluklarının belirlenmiş olması beklenmektedir. Ancak Tablo 4'e göre, katılımcıların yalnızca %26,2'si (n=27), verilerin anonimleştirilmesine, silinmesine veya yok edilmesine dair sorumlulukların belirlendiğini belirtmiştir.

Tablo 4

Verilerin Yok Edilmesi, Silinmesi ve Anonimleştirilmesiyle İlgili Süreçler

	Evet		Hayır	
	N	%	N	%
Verilerin anonimleştirilmesi, silinmesi ve yok edilmesine yönelik sorumluluklar belirlenmiş midir?	27	26,2	76	73,8
Kurumda kişisel veriler için veri anonimleştirmesi yapılmakta mıdır?	0	0	103	100
Kurumun bilgisayarları değiştiğinde/yenilendiğinde, eski bilgisayarların üzerindeki sabit diskler imha ediliyor mu?	103	100	0	0
Kurumun bilgisayarları üzerindeki kullanım süresi sona eren veriler için veri yok etme işlemleri uygulanıyor mu?	-	-	-	-

Tablo 4'teki "kişisel veriler için veri anonimleştirmesi yapılmakta mıdır?" sorusuna tüm katılımcılar hayır cevabı vermiştir. Kullanım süresi dolmuş kişisel verilerin silinmediği, sadece pasif hale getirildiği veya farklı bir kategoriye taşındığı tespit edilmiştir; bu durumun mevzuata uygun olmadığı belirtilmiştir. Anonimleştirmenin yapılmamasının ana nedeni olarak, detaylı bir yönetmeliğin eksikliği ve teknik zorluklar olduğu belirtilmiştir.

Verilerin yok edilmesi ve anonimleştirilmesi süreçlerindeki eksikliklerin temel nedenleri; ilgili personelin teknik bilgi yetersizliği, bu süreçlerde hangi yöntemlerin uygulanacağına ilişkin yasal düzenlemelerdeki belirsizlik ve bu durumun personelin inisiyatif almasını zorlaştırması olarak değerlendirilmektedir. Ayrıca, söz konusu süreçlerin etkin bir şekilde yürütülmesi için gerekli olan araç, gereç ve yazılımların merkez teşkilatları tarafından temin edilmemesi, uygulamayı zorlaştırmaktadır. Tüm katılımcılar, değiştirilen cihazların

depolama birimlerinin imha edildiğini belirtmiştir. Ekonomik ömrünü tamamlayan cihazlar ya Makine ve Kimya Endüstrisi'ne gönderilerek fiziksel olarak imha edilmekte ya da kamu idareleri arasında bedelsiz devredilmektedir. Bedelsiz devir işlemi daha kolay ve hızlı olduğu için sıkça tercih edilmekte olup, bu cihazlar genellikle halk eğitim merkezlerinde veya danışma alanlarında kullanılmaktadır. Ancak bu süreçte veri yok etme işlemi uygulanmadığı, sadece veri silme işlemi yapıldığı tespit edilmiştir.

"Kurumun bilgisayarlarındaki kullanım süresi dolmuş veriler için veri yok etme işlemi uygulanıyor mu?" sorusuna ise bilgisayarlarda veri bulundurma süresi ile ilgili bir üst limit tespit edilmediği için katılımcılar cevap vermemiştir.

Veri Yönetimi Hususunda Bilgilendirme ve Eğitim Çalışmaları

Kamu kurumlarında veri güvenliği konusunda periyodik eğitim çalışmalarının düzenlendiği tüm katılımcılar tarafından ifade edilmiştir. Katılımcıların %42,7'si (n=44) iki yılda bir, %39,8'i (n=41) ise yılda bir eğitim yapıldığını belirtmiştir. Katılımcıların %17,5'i (n=18) periyodik bir bilgi paylaşmamış, ancak eğitimlerin düzenli olarak gerçekleştirildiğini ifade etmiştir. Bu eğitimlerde kullanılan materyallerin tüm katılımcılar için merkez teşkilatları tarafından sağlandığı tespit edilmiştir. İl müdürlükleri statüsündeki kurumlar, merkez teşkilatlarından temin edilen materyallere ek olarak kendi sunumlarını hazırlamış olup, bu kurumlar toplam katılımcıların %5,9'unu (n=6) oluşturmaktadır. Ayrıca ilçe düzeyinde hizmet veren müdürlükler, hastaneler, müzeler ve diğer hizmet noktalarının kendi kurumlarında eğitim yapmadıkları, bağlı bulundukları il müdürlüğünün eğitim çalışmalarına katıldıkları belirlenmiştir.

Tartışma

Kamu Kurumlarının Taşra Teşkilatlarında Uygulanan Veri Gizliliğine, Güvenliğine ve Erişilebilirliğine Dair Politikalar

Araştırma kapsamında veri toplanan kamu kurumlarında çeşitli politikaların mevcut olması beklenmektedir. Bu politikalar arasında sorumluluk matrisi, veri sınıflandırma, erişim, yedekleme, veri imha ve anonimleştirme gibi ilkesel çalışmalar yer almaktadır. Değişen ihtiyaçlara göre oluşturulacak yeni politikalar, kamu kurumlarında öngörülebilir ve istikrarlı sonuçlar elde edilmesi açısından önemlidir. Ancak incelenen kurumlarda bu politikaların yalnızca sınırlı bir kısmının uygulandığı tespit edilmiştir. Birçok politika ve kural seti, merkez teşkilatları tarafından belirlenip uygulanmakta, ancak bu sistemlerin dışına çıkıldığında işlevselliği kaybolmaktadır. Bazı kurumlar LDAP gibi teknolojiler kullansa da yerel dosyaların varlığı, taşra teşkilatlarındaki veri güvenliğinde zafiyet yaratmaktadır.

Katılımcıların %38,9'u (n=40) kurumlarında "temiz masa / temiz ekran" politikası olduğunu belirtmiştir. Ancak bu politikalara dair yazılı bir metne rastlanmamış; politika metni sorulduğunda, bağlı oldukları bakanlığın internet sitesinde yayınlanan metin gösterilmiştir. İncelenen tüm kurumlarda sorumluluk matrisi oluşturulmamıştır. Küçük ölçekli kurumlar için bu durum kabul edilebilirken, il ölçeğinde hizmet veren kurumlarda bu eksiklik veri güvenliği ve bilgi teknolojileri süreçlerinde belirsizlikler doğurmakta ve hizmet akışında aksaklıklara neden olmaktadır. Örneğin bu hususta bir politikanın belirlenmediği kurumlarda kişisel verilerin kaydedildiği bir dosyanın ne zaman yok edileceği bilinmemektedir. Bu tür durumlarda, kurum yöneticileri bilişim sorunlarını bireysel olarak müdahale ederek çözmek zorunda kalmaktadırlar. Sorumluluk matrisinin eksikliği, teknik veya yönetimsel sorunların çözüm süreçlerinde belirsizliğe yol açmakta ve iş gücünde kayıplara neden olmaktadır.

Kamu kurumlarında merkezi depolama sistemlerine fiziksel erişim sınırlandırmaları getirilmiştir. Fiziksel erişim kısıtlaması uygulayan kurumların %63,9'u (n=36) RFID kart sistemleri kullanırken, %36,1'i (n=13) geleneksel kilit yöntemlerini tercih etmektedir.

Veri Silme, Yok Etme ve Anonimleştirme Hususundaki Mevzuat ve Hukuki Sorumlulukların Uygulanması

Veri silme, yok etme ve anonimleştirme konularında dikkate alınması gereken başlıca hukuki düzenlemelerden biri "Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik"tir. Bu yönetmeliğin bir üst hiyerarşik unsuru olan KVKK, veri silme, yok etme ve anonimleştirme ile ilgili hukuki sorumlulukları gerçek veya tüzel kişilere atfeden temel yasal düzenlemedir. KVKK'nın 16. maddesinin 2. fıkrası, veri işleyen gerçek ya da tüzel kişilerin veri işlemeye başlamadan önce VERBİS'e kaydolmalarını zorunlu kılmaktadır. Ancak araştırma kapsamında incelenen kamu kurumlarının taşra teşkilatlarının yasal statüleri göz önünde bulundurulduğunda, bu teşkilatlar için veri siciline kaydolma zorunluluğu olmadığı ve mevzuat kapsamında bir yükümlülük ortaya konmadığı anlaşılmaktadır. Bu taşra teşkilatları, merkez teşkilatına ve ilgili bakanlığın temsil ettiği devlet tüzel kişiliğine bağlı olarak faaliyet göstermektedir. Araştırmaya dahil olan bazı kurumlar, sosyal yardımlaşma vakıflarıdır. Vakıflar, 5737 sayılı Vakıflar Kanunu'nun 4. maddesi ile özel hukuk tüzel kişisi olarak tanımlanmıştır (T.C. Resmî Gazete, 2008). Aile ve Sosyal Hizmetler Bakanlığına (2022) göre, Sosyal Yardımlaşma ve Dayanışma Vakıfları (SYDV) her biri ayrı bir işyeri olarak kabul edilir ve her birinin kendine özgü karar kurulları bulunmaktadır. Kişisel Verileri Koruma Kurulu'nun 26.11.2019 tarihli 2019/353 sayılı kararı, aynı kurulun 2018/32 sayılı kararındaki "dernekler, vakıflar ve sendikalar sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına mahsus kişisel veri işleyebilir" ifadesinin "kendisine bağış yapanları" da kapsadığını belirtmektedir. Aile ve Sosyal Hizmetler Bakanlığının 2023 yılı verilerine göre, Türkiye genelinde toplam 971 SYDV bulunmaktadır. Kurulun bu kararı, SYDV'lerin yasal sorumluluklarını hafifletme amacı taşımaktadır.

Başlangıçta fark edilmeyen veya öngörülemeyen operasyonel gereksinim yaratan geniş kapsam, kurul kararları ile daraltılmaya çalışılmıştır. Sonuç olarak, taşra teşkilatlarının, derneklerin, vakıfların ve sendikaların yalnızca çalışanlarının, üyelerinin, mensuplarının ve bağışçılarının verilerini işledikleri ve bu nedenle KVKK kapsamında bir sorumluluklarının olmadığı düşünülebilir. Ancak, VERBİS'e kaydolma zorunluluğundan muaf olmaları, şeffaflığı azaltıcı bir yan etki doğurmakla sınırlı kalmaktadır. SYDV'ler de dahil olmak üzere tüm vakıf, dernek ve bakanlıkların taşra teşkilatları, periyodik imha, açık rıza ve KVKK kapsamında belirtilen sorumluluklardan muaf tutulmamaktadır. VERBİS'e kaydolma yükümlülüğünden istisna tutulmaları, hukuki sorumluluktan muaf oldukları anlamına gelmemektedir.

Kamu kurumlarında risk analizi eksikliği, veri yönetim sorumluluklarının yalnızca kurum müdürlerine veya teknisyenlere yüklenmesi, yerel cihazlardaki verilerin tüm çalışanlar tarafından erişilebilir olması, çalışanların hangi verilere erişebileceğini bilmemesi, veri silme işlemlerinin yapılmaması ve kişisel verilerin üçüncü şahısların eline geçme riski gibi sorunların, yukarıda bahsedilen "geniş kapsamın daraltılmaya çalışılması" sebebiyle yaşandığı düşünülmektedir. SYDV'lerin VERBİS'e kaydolmama istisnası, şeffaflığı azaltmakta ve kişisel veri koruma risklerini artırmaktadır. Bu istisna, SYDV'lerin hukuki sorumluluklarını ortadan kaldırmadığı gibi, veri ihlalleri veya kişisel verilerin üçüncü taraflara izinsiz geçmesi gibi riskleri artırarak kamu güvenini zedeleyebilmektedir.

Elektronik Ortamda Tutulan Verilerin Arşivlenmesi

Araştırma kapsamında incelenen tüm kurumlarda, kişisel veya kurumsal verilerin arşivlenmesi konusunda bir planlama olduğu tespit edilmiştir. Bu planlama, Devlet Arşiv Hizmetleri Hakkında Yönetmelik çerçevesinde belirlenen yükümlülüklerin yerine getirilmesini içermektedir. Ancak söz konusu yönetmelik yalnızca basılı belgelerin arşivlenmesine ilişkin bir yasal çerçeve sunmakta olup, anonimleştirilmiş kişisel verilerin ya da artık kullanılmayan operasyonel belgelerin arşivlenmesi konusunda bir düzenleme bulunmamaktadır.

Kamu Kurumlarının Taşra Teşkilatlarındaki Veri Yönetimi İçin Risk Temelli Yaklaşım

Araştırma kapsamında incelenen kamu kurumlarının %45,7'sinde (n=47) en az bir kez veri güvenliği odaklı risk analizi yapıldığı tespit edilmiştir. Risk analizi yapıldığı belirtilen tüm kurumların, bu analizlere dayalı olarak risk işleme süreçlerini gerçekleştirdikleri görülmüştür. Ancak bu analizlerin merkez teşkilatları tarafından yapıldığı ve taşra teşkilatlarının, bu analizler veya sonrasında alınacak kararlarda söz sahibi olmadığı anlaşılmıştır.

Dijital Verilerin Saklanma Biçimi ve Uygulanan Yöntemler

Araştırma bulguları, kamu kurumlarının %65'inde (n=67) merkezi bir veri depolama ünitesinin bulunmadığını ve bu kurumların merkez teşkilatları tarafından sağlanan Elektronik Belge Yönetim Sistemleri (EBYS) kullandığını göstermektedir. Merkezi veri depolama sistemleri genellikle yalnızca güvenlik kamera kayıt cihazlarını kapsamaktadır. Ayrıca ilgili kurumların bağımsız EBYS'leri bulunmakta, operasyonel veriler ise kurum çalışanları tarafından kişisel zimmetli iş bilgisayarlarında işlenmektedir; bu sürecin kontrol ve denetim sistemlerinden arındırılmış olduğu görülmektedir.

Verilerin merkezi veri yönetim süreçlerinden uzak bir şekilde işlenmesi, kişisel verilerin yetkisiz erişimine, kopyalanmasına, değiştirilmesine veya silinmesine yol açabilecektir. Bu durum, bireylerin mahremiyet haklarının ihlaline neden olabilmektedir. Güvenlik önlemlerinin alınmaması, veri güvenliğini zayıflatmakta ve siber saldırılar, veri hırsızlığı, veri ihlalleri ve hukuki sorumlulukların artışı gibi ciddi sonuçlara yol açabilmektedir. Ayrıca standartların ve prosedürlerin uygulanmaması, veri kalitesinin düşmesine, karar alma süreçlerinde hatalara ve kamu hizmetlerinin verimsizleşmesine neden olmaktadır. İş bilgisayarlarının yetkisiz erişime açık olması, kişisel verilerin kötü niyetli kişiler tarafından ele geçirilme riskini artırmakta, tehdit veya şantaj amacıyla kullanılmasına neden olabilmektedir. Bilgisayarların çalınması veya kaybolması da içerdikleri verilerin kaybolma veya çalınma riskini beraberinde getirmektedir.

Kamu kurumlarında ekonomik ömrünü tamamlamış sabit diskler için iki yöntem uygulanmaktadır: Sabit diskler, Taşınır Mal Yönetmeliği çerçevesinde gerekli evrak süreçleri tamamlanarak Makine ve Kimya Endüstrisine (MKE) imha için gönderilebilir ya da ihtiyaç duyan idarelere bedelsiz devredilebilir. Ancak birçok kurum yöneticisi, MKE'ye gönderimin uzun ve zahmetli bir süreç olduğunu belirterek genellikle bedelsiz devir yöntemini tercih ettiklerini ifade etmiştir. Bu devir sürecinde mantıksal veri yok etme işleminin yapılmadığı tespit edilmiştir.

Kamu kurumlarında, iş bilgisayarlarında tutulan kişisel, operasyonel veya kurumsal verilerin bedelsiz devredilme yöntemiyle başka bir kuruma aktarıldığı görülmektedir. Bilgisayarlardaki veriler silinmiş olsa bile veri yok etme tekniklerinin kullanılmaması, bu verilerin üçüncü kişiler tarafından ele geçirilme riskini artırmaktadır. Taşınır Mal Yönetmeliği'nin günümüz teknolojik ihtiyaçlarını karşılamadığı ve elektronik cihazlar açısından güncellenmesi gerektiği anlaşılmaktadır.

Verilerin Yok Edilmesi, Silinmesi ve Anonimleştirilmesiyle İlgili Uygulanan Yöntem ve Teknikler

Araştırma bulgularına göre, kamu kurumları veri yok etme veya anonimleştirme konusunda herhangi bir teknik yöntem uygulamamaktadır. Kurumlar, elektronik ortamda tutulan verileri silmek için yalnızca kişisel, operasyonel veya kurumsal verilerin işletim sistemlerinin dosya tablolarından kaldırılması yöntemini kullanmakta, bu da verilerin depolama cihazlarından tam anlamıyla silinmediği anlamına gelmektedir.

Anonimleştirilmeyen veriler, kamu kurumlarına stratejik tehditler doğurabilmektedir. Bu veriler, gerçek kişiler veya kurumlarla ilişkilendirilerek tehdit veya şantaj aracı olarak kullanılabilir. Yetkisiz olarak işlenen anonimleştirilmemiş veriler, kurumlar veya bireyler hakkında mahrem bilgilerin açığa çıkmasına yol açabilir.

Özellikle SYDV'ler ile sağlık kurumlarının bireylere ilişkin hassas nitelikli veriler bulundurduğu bilinmektedir. Bu tür kurumların, sahip oldukları verilerle ilgili riskleri yönetmeleri gerekmektedir.

Örneğin, 2023 yılında bir vakfın topladığı veriler arasında engellilik durumu, kronik ruhsal sağlık sorunu, sürekli ilaç kullanımı, göç durumu ve göç nedenleri gibi hassas nitelikli bilgiler yer almaktadır (Osmaneli Sosyal Yardımlaşma ve Dayanışma Vakfı, 2023). Bu tür özel nitelikli veriler, kişilerin kişilik haklarını ihlal etmek veya tehdit amacıyla kullanılabilecek verilerdir. Ayrıca borç veya taksit sahipliği, konut durumu, kira bedeli, ısıtma yöntemi, yemek pişirme için kullanılan yakıt gibi kişisel detaylar da SYDV'ler tarafından toplanmaktadır. SYDV'lerin VERBİS'e kaydolma zorunluluğundan muaf tutulmaları, bu verilerin nasıl yönetildiği ve güvenceye alındığı konusunda şeffaflığın azalmasına neden olmaktadır. SYDV'lerin şeffaflıklarını artırmak için VERBİS kaydının zorunlu hale getirilmesi ve düzenli veri imha prosedürlerinin raporlanması gerekmektedir.

Veri Yönetimi ve Veri Güvenliği ile İlgili Eğitsel Çalışmalar

Katılımcıların, veri güvenliği ve veri yönetimi konularında dönemsel eğitimler düzenledikleri görülmektedir. Bu eğitimlerin merkez teşkilatları tarafından planlandığı ve içeriğinin de bu teşkilatlar tarafından sağlandığı belirtilmiştir. Bağımsız tüzel kişiliğe sahip SYDV'ler de periyodik kurum içi eğitimlerden bahsetmekte, ancak bu eğitimlerin içeriğinin yetersiz ve yalnızca yüzeysel bilgilerle sınırlı olduğu anlaşılmaktadır. Eğitimlerin kavramların tanımlanmasıyla sınırlı kaldığı ve derinlikten yoksun olduğu tespit edilmiştir.

Veri güvenliği ve veri yönetimi konusundaki eğitimler, veri ihlali tehditlerinin neden olabileceği zararları en aza indirmekte kritik bir rol oynamaktadır. Bu tür eğitimler, hassas verilerin gizliliğini korumak ve veri ihlali risklerini azaltmak için önemli bir araçtır. Eğitimler, çalışanlara hassas verilerin doğru ve güvenli bir şekilde nasıl toplanacağı, işleneceği ve depolanacağı konularında bilgi sağlamaktadır. Ayrıca çalışanların veri ihlali tehditlerini fark etmesine ve bu tehditlere karşı nasıl önlem alacaklarını öğrenmesine yardımcı olabilecektir. Ancak mevcut eğitimlerin yeterli kapsam ve derinlikte olmadığı görülmektedir.

Sonuç ve Öneriler

Kişisel Verileri Koruma Kurumunun 02.04.2018 Tarihli ve 2018/32 Sayılı Kararı gereğince birtakım vakıf, dernek ve sendikaların VERBİS'e kaydolmamalarının bir sonucu olarak, bu kurumların hangi kişisel verileri işlediği, bu verileri hangi yasal dayanakla topladığı, ne kadar süreyle sakladığı veya hangi güvenlik önlemlerini aldıkları belirsizdir. Bu kurumlar kişisel veri işlemeye devam ettiği sürece, hukuki sorumlulukları da devam etmektedir. VERBİS'e kaydolmamaları, Kişisel Verileri Koruma Kurumu tarafından yapılacak bir denetimde dikkate alınmayacakları anlamına gelmemektedir. Bu nedenle, VERBİS'e kaydolma yükümlülüğünden muafiyetin kaldırılması ve bu kurumların da VERBİS'e kaydolmalarının sağlanmasının, şeffaflığın artırılması ve denetim mekanizmalarının etkin çalışabilmesine katkı sağlayacağı düşünülmektedir.

Bakanlıkların taşra teşkilatlarının veri sorumlusu olarak kabul edilmemesi, birtakım yönetimsel ve hukuki riskler doğurmaktadır. Verilerin toplandığı ve işlendiği taşra teşkilatlarının hukuksal sorumluluğunun bulunmaması ve tüm sorumluluğun merkez teşkilatlarına yüklenmesi bazı yönetim sorunlarına yol açmaktadır. Örneğin, araştırma kapsamında incelenen kurumlarda erişim yetkilendirmesi ile ilgili bir politika olmaması, yetkisiz kişilerin kritik veya özel nitelikli verilere erişmesini mümkün hale getirmektedir. Ayrıca dijital veriler için saklama süresinin belirlenmemesi, bu verilerin kötü amaçla kullanılma riskini artırmaktadır. Dijital verilerin arşivlenmemesi, mükerrer kayıtların oluşmasına ve iş gücü kaybına yol açmaktadır. Taşra teşkilatlarında toplanan ve üretilen verilerin miktarı dikkate alındığında, veri madenciliği gibi uygulamalarla yönetim amaçlı kıymetli bilgilerin üretilme potansiyeli de kaybolmaktadır.

Araştırmada bir kamu kurumunun arşivini dijitalleştirmek amacıyla özel bir firmayla anlaştığı ve firmanın tüm hasta kayıtlarına eriştiği tespit edilmiştir. Bu süreci kontrol eden bir mekanizma olmadığı için firmanın verileri kopyalama veya manipüle etme riski bulunmaktadır. Birçok birey için birden fazla kayıt dosyası oluşturulduğu için kurumlarda kırtasiye masraflarının artmış olduğu görülmektedir. Bu durumun, verilerin elektronik ortamda arşivlenmemesi sebebiyle gerçekleştiği düşünülmektedir. LTO bant depolama gibi teknolojilerle anonimleştirilmiş kişisel veriler süresiz olarak saklanabilmekte ve veri madenciliği teknikleriyle işlevsel bilgi üretilebilmektedir. Verilerin arşivlenebilmesi için bazı kişisel verilerin anonimleştirilmesi gerekmektedir. Bu bağlamda, anonimleştirme süreçleri ile ilgili hem teknik hem de ilkesel politikalar oluşturulmalı ve dijital arşivleme süreçleriyle entegre edilmelidir.

Taşra teşkilatlarının da hukuki olarak veri sorumlusu statüsünde ele alınması ve yerel birimlerde aktif veri yönetiminin başlatılmasının, veri güvenliği risklerini azaltabileceği düşünülmektedir. Veri yönetim zincirinin tüm halkaları güçlendirilerek, taşra teşkilatlarının veri yönetim süreçlerinin daha etkili hale getirilebilmesi mümkün olacaktır. Ayrıca veri toplama ve saklama süreçlerinde kayıplar azaltılarak daha derin ve anlamlı bilgiler üretilebilecektir. Böylece ulusal çapta veri derinliği artarken, yerel ölçekte veri madenciliği gibi uygulamaların da önü açılabilecektir.

Sorumluluk matrisinin eksikliğini gidermek amacıyla, kamu kurumlarındaki sistem ve mekanizmalar, sorumluları ile listelenmeli, süreçler yazılı hale getirilmeli ve kurum paydaşlarına duyurulmalıdır. Ayrıca sık karşılaşılan sorunlar için çözüm yolları belirlenerek, çalışanların yardıma ihtiyaç duymadan bu sorunları çözebilmesi sağlanmalıdır. Sorumlu kişilerin açık bir şekilde belirlenmesi, sorunların hızla çözülmesine ve iş süreçlerinde aksaklıkların önlenmesine yardımcı olacaktır. Risk temelli yaklaşım, aktif bir veri yönetim süreci için bir çatı görevi görmektedir. Etkin olarak uygulanan veri yönetim politikaları, risk temelli yaklaşım için gerekli temel koşulları oluşturmaktadır. Veri yönetim unsurlarının, paydaşların ve çalışanların belirlenmesi, bu kapsamda yetkilerin, erişimlerin ve sorumlulukların net bir şekilde tanımlanması; potansiyel tehditlerin ve olası kayıpların ölçümlenmesi, risklerin öngörülmesi için gereklidir. Bu koşullar yerine getirildiğinde, olası riskler daha kolay tespit edilebilecek ve risk işleme süreçleri yürütülebilecektir.

Araştırma kapsamında incelenen kamu kurumlarında yazılı bir erişim politikasına rastlanmamıştır. EBYS haricinde yerel depolama alanlarında bulunan pdf, xls, doc vb. uzantılı dosyalar için kimlerin erişim sağlayabileceği veya verilerin hangi cihazlara transfer edilebileceğiyle ilgili bir politika bulunmamaktadır. Bilgi erişim politikasının olmaması, herhangi bir kurum çalışanının yetkisiz bir şekilde kritik öneme sahip verilere erişim sağlamasına olanak tanımaktadır. Bu durumda kişisel ve kamusal zararların oluşma potansiyeli bulunmaktadır. Erişim politikası, çalışanların yalnızca yetkileri dahilinde verilere erişimini sağlayarak veri ihlali risklerini azaltmaktadır. Erişim politikalarının oluşturulması için çalışan rolleri detaylı bir şekilde belirlenmeli ve veri türleri gizlilik derecelerine göre sınıflandırılmalıdır. Ayrıca, erişim yönetiminde ISO 27001 gibi uluslararası standartlar esas alınmalıdır.

Veri depolama ortamlarında silinen veya formatlanan veriler dahi gelişmiş veri kurtarma yazılımlarıyla okunabilir hale gelebilmektedir. Bu nedenle, kamu kurumlarında kullanım ömrünü tamamlamış sabit disklere verileri yok etme işlemleri uygulanmadığında, yetkisiz kişiler bu disklere erişerek kişisel, operasyonel ya da kurumsal verilere ulaşabilmektedir. Eski sabit disklerde veri yok etme işleminin yapılmaması, veri güvenliğinin ihlal edilmesine neden olabilmektedir. Bu nedenle sabit diskler, parçalayıcı kullanımı gibi fiziksel imha yöntemiyle veya yazılım tabanlı yöntemlerle (örneğin, NIST 800-88 standardı doğrultusunda) yok edilmelidir. Ayrıca bu işlemler için düzenli denetim mekanizmaları kurulmalıdır.

Etik Kurul Onayı Bu makaleye ilişkin araştırma için Aydın Adnan Menderes Üniversitesi Sosyal ve Beşerî Bilimler Araştırmaları Etik Kurulu'ndan (31906847/050.04.04-08-329) izin alınmıştır.

Bilgilendirilmiş Onam Katılımcılardan bilgilendirilmiş onam alınmıştır.
Hakem Değerlendirmesi Dış bağımsız.
Yazar Katkısı Çalışma Konsepti/Tasarım- T.H., H.Y.; Veri Toplama- H.Y.; Veri Analizi/Yorumlama- H.Y.; Yazı Taslağı- T.H., H.Y.; İçeriğin Eleştirel İncelemesi- T.H.; Son Onay ve Sorumluluk- T.H., H.Y.
Çıkar Çatışması Yazarlar çıkar çatışması bildirmemiştir.
Finansal Destek Yazarlar bu çalışma için finansal destek almadığını beyan etmiştir.

Ethics Committee Approval Ethics approval for this research was obtained from the Aydın Adnan Menderes University Social and Human Sciences Research Ethics Committee (Approval No: 31906847/050.04.04-08-329).
Informed Consent Informed consent was obtained from the participants.
Peer Review Externally peer-reviewed.
Author Contributions Conception/Design of study: T.H., H.Y.; Data Acquisition- H.Y.; Data Analysis/ Interpretation- H.Y.; Drafting Manuscript- T.H., H.Y.; Critical Revision of Manuscript- T.H.; Final Approval and Accountability- T.H., H.Y.
Conflict of Interest The authors have no conflict of interest to declare.
Grant Support The authors declared that this study has received no financial support.

Yazar Bilgileri / Author Details

Haktan Yavaş
[1] Pamukkale Üniversitesi Yönetim Bilişim Sistemleri Bölümü, Pamukkale, Türkiye
0000-0001-9610-5226 haktanyavas@outlook.com

Türkay Henkoğlu
[2] Aydın Adnan Menderes Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, Aydın, Türkiye
0000-0002-0567-5408

Kaynakça | References

Anderson, D., & Von Seck, R. (2020). The GDPR and its impact on the web. doi:10.2313/NET-2020-11-1_01

APEC Privacy Framework. (2005). Singapore: APEC Secretariat.

Appelbaum, P., Beattie, E., Boutin, M., W. Croghan, T., W. Crosley, S., J. Horning, S., ... W. Yancy, C. (2009). *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. (S. J. Nass, L. A. Levit ve L. O. Gostin, Ed.). Washington, D.C.: The National Academies Press. http://www.nap.edu/catalog/12458.html adresinden erişildi.

Attaallah, A., Alsuhabi, H., Shukla, S., Kumar, R., Kumar Gupta, B., & Khan, R. A. (2022). analyzing the big data security through a unified decision-making approach. *Intelligent Automation & Soft Computing*, *32*(2), 1071-1088. doi:10.32604/iasc.2022.022569

Avllazagaj, E., Ayday, E., & Çiçek, A. E. (2016). privacy-related consequences of Turkish citizen database leak. *arXiv (Cornell University)*. doi:10.48550/arxiv.1605.05847

Avrupa Konseyi. (2016). *Regulation (EU) 2016/679 Of The European Parliament and Of The Council*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN adresinden erişildi.

Bates, D. W., Heitmueller, A., Kakad, M., & Saria, S. (2018). Why policymakers should care about "big data" in healthcare. *Health Policy and Technology*, *7*(2), 211-216. doi:10.1016/j.hlpt.2018.04.006

Bayardo, R. J. ve Agrawal, R. (2005). Data privacy through optimal k-anonymization. *21st International Conference on Data Engineering (ICDE'05)*. doi:10.1109/icde.2005.42

Bolognini, L., & Bistolfi, C. (2017). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law & Security Review*, *33*(2), 171-181. doi:10.1016/J.CLSR.2016.11.002

Bradford, L., Aboy, M., & Liddell, K. (2021). Standard contractual clauses for cross-border transfers of health data after Schrems II. *Journal of Law and the Biosciences*, *8*(1). doi:10.1093/jlb/lsab007

Burenok, D. S. (2023). The mandatory state digital register of personal data processing consents. *2023 Seminar on Information Computing and Processing (ICP)* içinde (ss. 11-17). doi:10.1109/ICP60417.2023.10397191

Cate, F. H., Cullen, P., & Mayer-Schonberger, V. (2013). Data Protection Principles for the 21st Century. Redmond, WA: Books & Book Chapters by Maurer Faculty. https://www.repository.law.indiana.edu/facbooks adresinden erişildi.

Cheng, L., Liu, F., & Yao, D. (Daphne). (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *WIREs Data Mining and Knowledge Discovery*, *7*(5), e1211. doi:10.1002/widm.1211

Cormode, G., & Srivastava, D. (2010). Anonymized Data: Generation, models, usage. *2010 IEEE 26th International Conference on Data Engineering (ICDE 2010)* içinde (ss. 1211-1212). doi:10.1109/ICDE.2010.5447721

DataBreaches LLC. (2016, 3 Nisan). Turkish Citizenship Database Leak (Update 2). 29 Ekim 2023 tarihinde https://www.databreaches.net/turkish-citizenship-database-leak/ adresinden erişildi.

Datenschutz-Wiki. (2016). Bundesdatenschutzgesetz (1977) – Datenschutz-Wiki. 29 Ekim 2023 tarihinde https://www.datenschutz-wiki.de/BDSG_1977 adresinden erişildi.

DSV Stockholm University. (2000, 9 Haziran). The Swedish Personal Information Act. *Dsv.su.se*. 29 Ekim 2023 tarihinde https://people.dsv.su.se/~jpalme/society/eu-data-directive-freedom.html adresinden erişildi.

Dülger, M. V. (2021). Kişisel Verileri Koruma Kurulu'nun 18 Ağustos 2018 Tarihli Resmi Gazete'de Yayınlanan Kararlarına İlişkin Değerlendirme. *SSRN Electronic Journal*. doi:10.2139/ssrn.3792274

Dülger, M. V., Kahraman, C. C., & Yalçın, S. (2021). GDPR ve KVKK bakımından çocukların kişisel verilerinin korunması ve konuya ilişkin kurul kararının değerlendirilmesi. *SSRN Electronic Journal*. doi:10.2139/ssrn.3792410

Ersoy, E. C. (2019). Examining Turkish law on data protection. *Computer Fraud & Security*, *2019*(9), 9-11. doi:10.1016/S1361-3723(19)30095-8

European Center for Digital Rights. (2017). Data Protection in Austria - GDPRhub. *GDPRhub*. 29 Ekim 2023 tarihinde https://gdprhub.eu/Data_Protection_in_Austria adresinden erişildi.

European Center for Digital Rights. (2020). Data Protection in Denmark - GDPRhub. *GDPRhub*. 29 Ekim 2023 tarihinde https://gdprhub.eu/Data_Protection_in_Denmark adresinden erişildi.

European Union Agency for Fundamental Rights. (2018, 25 Ekim). Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties. 29 Ekim 2023 tarihinde https://fra.europa.eu/en/law-reference/act-ndeg78-17-6-january-1978-data-processing-data-files-and-individual-liberties adresinden erişildi.

Ganesh, P., Tran, C., Shokri, R., & Fioretto, F. (2024). The Data Minimization Principle in Machine Learning. http://arxiv.org/abs/2405.19471 adresinden erişildi.

Garfinkel, S. L. (2015). De-identification of personal information. *National Institute of Standards and Technology Internal Report*, *8053*. doi:10.6028/nist.ir.8053

Garg, S., Verma, K. K., & Kumar, G. (2024). An Analysis on the Threats on Public Data Collection. *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)* içinde (ss. 1-6). doi:10.1109/ISCS61804.2024.10581271

Goldsteen, A., Ezov, G., Shmelkin, R., Moffie, M., & Farkash, A. (2022). Data minimization for GDPR compliance in machine learning models. *AI and Ethics*, *2*(3), 477-491. doi:10.1007/s43681-021-00095-8

Gonzalez, E. G., De Hert, P., & Papakonstantinou, V. (2020). The proposed ePrivacy regulation: The commission's and the parliament's draft s at a crossroads? D. Hallinan, R. Leenes, S. Gutwirth ve P. De Hert (Ed.), *Data protection and privacy* içinde (ss. 267-298). Hart Publishers.

Gutmann, P. (1996). Secure Deletion of Data from Magnetic and Solid-State Memory. *Sixth USENIX Security Symposium Proceedings* içinde . https://web.archive.org/web/20230927105247/https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html adresinden erişildi.

Güler, C. (2020). *Elektronik belgelerin imhası: Teori ve uygulama*. Hiperyayın, 2020.

Helvacıoğlu, A. D., & Stakheyeva, H. (2017). The tale of two data protection regimes: The analysis of the recent law reform in Turkey in the light of EU novelties. *Computer Law & Security Review*, *33*(6), 811-824. doi:10.1016/j.clsr.2017.05.014

Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014). *Guidelines for Media Sanitization*. Gaithersburg, MD. doi:10.6028/NIST.SP.800-88r1

Knapp, K. J., Denney, G. D., & Barner, M. E. (2011). Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly*, *28*(4), 533-541. doi:10.1016/j.giq.2010.10.008

Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L, & Tosoni, L. (2021). The EU General Data Protection Regulation: A Commentary/Update of Selected Articles. *SSRN Electronic Journal*. doi:10.2139/SSRN.3839645

Li, N., Li, T., & Venkatasubramanian, S. (2007). t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. *2007 IEEE 23rd International Conference on Data Engineering* içinde (ss. 106-115). doi:10.1109/ICDE.2007.367856

Liu, L. (2021). The Rise of Data Politics: Digital China and the World. *Studies in Comparative International Development*, *56*, 45-67. doi:10.1007/s12116-021-09319-8

Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). L-diversity: Privacy beyond k-anonymity. *ACM Trans. Knowl. Discov. Data*, *1*(1), 3–es. doi:10.1145/1217299.1217302

Miller, M. R., Herrera, F., Jun, H., Landay, J. A., & Bailenson, J. N. (2020). Personal identifiability of user tracking data during observation of 360-degree VR video. *Scientific Reports*, *10*(1), 17404. doi:10.1038/s41598-020-74486-y

National Research Council. (1993). *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics*. *Private Lives and Public Policies*. Washington, DC: The National Academies Press. doi:10.17226/2122

Nergiz, M E, Clifton, C., & Nergiz, A. E. (2009). Multirelational k-Anonymity. *IEEE Transactions on Knowledge and Data Engineering*, *21*(8), 1104-1117. doi:10.1109/TKDE.2008.210

Nergiz, M. E.; Atzori, M., & Clifton, C. (2007). Hiding the presence of individuals from shared databases. *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data* içinde , SIGMOD '07 (ss. 665-676). New York, NY, USA: Association for Computing Machinery. doi:10.1145/1247480.1247554

Osmaneli Sosyal Yardımlaşma ve Dayanışma Vakfı. (2023). Osmaneli Sosyal Yardımlaşma ve Dayanışma Vakfı. 27 Ekim 2024 tarihinde https://osmanelisydv.gov.tr/upload/docs/5_Hane_Beyan_Formu.pdf adresinden erişildi.

Richards, N. M., & King, J. H. (2014). Big Data Ethics. *Wake Forest Law Review*. http://strata.oreilly.com/2012/01/what-is- adresinden erişildi.

Rubin, A., & Babbie, E. R. (2016). *Essential research methods for social work* (4. bs.). Cengage Learning.

Shanmugam, D., Diaz, F., Shabanian, S., Finck, M., & Biega, A. (2022). Learning to Limit Data Collection via Scaling Laws: A Computational Interpretation for the Legal Principle of Data Minimization. *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* içinde , FAccT '22 (ss. 839-849). New York, NY, USA: Association for Computing Machinery. doi:10.1145/3531146.3533148

Shu, X., Zhang, J., Yao, D. D. ve Feng, W.-C. (2016). Fast Detection of Transformed Data Leaks. *IEEE Transactions on Information Forensics and Security*, *11*(3), 528-542. doi:10.1109/TIFS.2015.2503271

Siedlecki, S. L. (2020). Understanding Descriptive Research Designs and Methods. *Clinical Nurse Specialist*, *34*(1), 8-12. doi:10.1097/NUR.0000000000000493

State Chancellery of Hessen - Minister for Digital Strategy and Innovation. (2023). *Digital Hesse Where the future begins*. *digitales.hessen.de*. https://digitales.hessen.de/sites/digitales.hessen.de/files/2023-01/Digitalstrategie%20englisch_barrierefrei.pdf adresinden erişildi.

Swanson, M. ve Guttman, B. (1996). *Generally accepted principles and practices for securing information technology systems*. Gaithersburg, MD. doi:10.6028/NIST.SP.800-14

T. C. Aile ve Sosyal Hizmetler Bakanlığı. (2022). Sosyal Yardımlaşma ve Dayanışma Vakıfları. 29 Ekim 2023 tarihinde https://www.aile.gov.tr/sygm/genel-mudurluk/sosyal-yardimlasma-ve-dayanisma-vakiflari/ adresinden erişildi.

T.C. Resmî Gazete. (2008). Vakıflar Kanunu. 29 Ekim 2023 tarihinde https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5737.pdf adresinden erişildi.

T.C. Resmî Gazete. (2019, 18 Ekim). Devlet Arşiv Hizmetleri Hakkında Yönetmelik. 29 Ekim 2023 tarihinde https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=33899&MevzuatTur=7&MevzuatTertip=5 adresinden erişildi.

T.C. Resmî Gazete. (2022). Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. 29 Ekim 2023 tarihinde https://www.mevzuat.gov.tr/MevzuatMetin/21.5.5529.pdf adresinden erişildi.

The United State Department of Justice. (2014, 17 Haziran). Privacy Act of 1974. *Justice.gov*. 29 Ekim 2023 tarihinde https://www.justice.gov/opcl/privacy-act-1974 adresinden erişildi.

University of Cambridge. (2020). Norway | Centre for Intellectual Property and Information Law. *Cam.ac.uk*. 29 Ekim 2023 tarihinde https://www.cipil.law.cam.ac.uk/projectseuropean-data-protection-laws-and-freedom-expression/norway adresinden erişildi.

U.S. Department of Defense. (1995). National Industrial Security Program Operating Manual (NISPOM). *U.S. Department of Defense*. www.reginfo.gov/public/do/PRAMain. adresinden erişildi.

Wong, R. (2012). The Data Protection Directive 95/46/EC: Idealisms and realisms. *International Review of Law, Computers & Technology*, *26*(2-3), 229-244. doi:10.1080/13600869.2012.698453

Wouters, B., Shaw, D., Sun, C., Ippel, L., van Soest, J., van den Berg, B., ... Townend, D. (2021). Putting the GDPR into Practice: Difficulties and Uncertainties Experienced in the Conduct of Big Data Health Research. *European Data Protection Law Review*, *7*(2), 206-216. doi:10.21552/edpl/2021/2/9

Yılmaz, T., Arıkan, S. M., Su, F. & Yürekten, Ö. (2020). Protecting Personal Information in Enterprise Applications. *2020 Turkish National Software Engineering Symposium (UYMS)* içinde (ss. 1-4). doi:10.1109/UYMS50627.2020.9247020