International
SOCIAL SCIENCES STUDIES Journal
Open Access Refereed E-Journal & Indexed & Publishing
e-ISSN: 2587-1587

RESEARCH ARTICLE
Public Administration

Kamu Yönetiminde Kurumlar Arası Stratejik İş Birliği ve Siber Güvenlik Tehditlerine Karşı Bilgi Paylaşımı

Inter-Institutional Strategic Cooperation in Public Administration and Information Sharing Against Cyber Security Threats

Faruk Selahattin Yolcu [1]

ÖZET

Bilgi paylaşımı, kamu kurumları arasında koordinasyon sağlanması, hizmet kalitesinin artırılması ve kamu yönetiminin dijital dönüşüm sürecine uyum sağlaması açısından kritik bir süreçtir. Ancak, bürokratik engeller, kurumsal güven eksikliği, yasal sınırlamalar ve teknik uyumsuzluklar, bilgi paylaşımını sınırlayan temel faktörlerdir. Bu çalışma, kamu yönetiminde kurumlar arası bilgi paylaşımının etkinliğini artırmak ve siber güvenlik tehditlerine karşı dirençli bir yapı oluşturmak amacıyla stratejik iş birliği modellerini incelemektedir. Çalışmada, Türkiye'de *e-Devlet Kapısı, UYAP, MERNİS* ve *Sağlık Bilgi Sistemleri* gibi mevcut bilgi paylaşım mekanizmalarının etkinliği incelenmiş ve kamu kurumları arasındaki bilgi akışını kolaylaştıran ve engelleyen unsurlar analiz edilmiştir. Çalışma, teorik bir çerçeve üzerinden yürütülerek sosyal sermaye teorisi, bilgi tabanlı teori ve örgütsel öğrenme teorisi ışığında kamu yönetimindeki bilgi paylaşımının iyileştirilebilir yönlerini ele almaktadır. Elde edilen bulgular, bilgi paylaşımının siber güvenlik tehditlerine karşı kolektif bir savunma mekanizması sunduğunu ve kamu hizmetlerinin etkinliğini artırdığını göstermektedir. Türkiye'de mevcut bilgi paylaşım altyapılarının belirli ölçüde başarılı olduğu ancak veri güvenliği, yasal düzenlemeler, insan kaynağı eksikliği ve kurumlar arası güven sorunu nedeniyle bazı aksaklıklar yaşandığı tespit edilmiştir. İyileştirilebilir yönelere ışık tutan on temel politika önerisi sunulmuştur. Sonuç olarak, bilgi paylaşımının etkin bir şekilde gerçekleştirilmesi için veri entegrasyonu, ortak risk yönetimi, eğitim ve farkındalık artırma stratejileri ile yasal çerçevenin güncellenmesi gerekmektedir. Çalışma kapsamında geliştirilen politika önerileri, kamu kurumlarının daha koordineli, güvenli ve verimli çalışmasını sağlayarak vatandaşlara sunulan hizmetlerin kalitesini artırmayı amaçlamakatadır.

Anahtar Kelimeler: Kamu Yönetimi, Stratejik Yönetim, Bilgi Paylaşımı, Siber Güvenlik, Türkiye.

ABSTRACT

Information sharing is a critical process in terms of ensuring coordination among public institutions, increasing service quality and adapting to the digital transformation process of public administration. However, bureaucratic obstacles, lack of institutional trust, legal limitations and technical incompatibilities are the main factors limiting information sharing. This study examines strategic cooperation models in order to increase the effectiveness of information sharing between institutions in public administration and to create a structure resistant to cybersecurity threats. In the study, the effectiveness of existing information sharing mechanisms such as e-Government Gateway, UYAP and Health Information Systems in Türkiye was examined and the elements that facilitate and hinder the flow of information between public institutions were analyzed. The study was conducted within a theoretical framework and addressed the improvable aspects of information sharing in public administration in light of social capital theory, knowledge-based theory and organizational learning theory. The findings obtained show that information sharing provides a collective defense mechanism against cybersecurity threats and increases the effectiveness of public services. It was determined that the existing information sharing infrastructures in Türkiye are successful to a certain extent, but some problems are experienced due to data security, legal regulations, lack of human resources and trust issues between institutions. Ten basic policy recommendations that shed light on areas for improvement have been presented. As a result, data integration, common risk management, education and awareness-raising strategies and the legal framework need to be updated to ensure effective information sharing. The policy recommendations developed within the scope of the study aim to increase the quality of services provided to citizens by ensuring more coordinated, secure and efficient operation of public institutions.

Keywords: Public Administration, Strategic Management, Information Sharing, Cyber Security, Türkiye.

How to Cite This Article
Yolcu, F. S. (2025). "Kamu Yönetiminde Kurumlar Arası Stratejik İş Birliği ve Siber Güvenlik Tehditlerine Karşı Bilgi Paylaşımı" International Social Sciences Studies Journal, (e-ISSN:2587-1587) Vol:11, Issue:9; pp:1598-1606. DOI: https://doi.org/10.5281/zenodo.17221538

Arrival: 20 July 2025
Published: 27 September 2025

[1] Dr. Öğr. Üyesi, Kocaeli Üniversitesi, Siyasal Bilgiler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı, Kocaeli, Türkiye, ORCID:0000-0001-9942-7669.

GİRİŞ

Bilgi ve iletişim teknolojilerinin hızla gelişmesi, kamu kurumlarının işleyişinde ve hizmet sunumunda köklü değişikliklere yol açmıştır. Bu dönüşüm süreci, kamu kurumları arasındaki bilgi paylaşımının ve iş birliğinin önemini artırmıştır. Özellikle siber güvenlik tehditlerinin artan karmaşıklığı ve sıklığı, kamu kurumlarının bilgi güvenliği ve iş birliği konularına daha fazla önem vermesini zorunlu kılmaktadır. Bu bağlamda, kamu kurumları arasında etkili bilgi paylaşımı ve iş birliği mekanizmalarının oluşturulması, hem siber güvenlik tehditlerine karşı dayanıklılığı artırmakta hem de kamu hizmetlerinin etkinliğini ve verimliliğini yükseltmektedir. Bu doğrultuda çalışma, Türkiye'deki kamu kurumları arasında bilgi paylaşımının mevcut durumunu ve bu süreci etkileyen faktörleri detaylı bir şekilde incelemektedir. İlk olarak, bilgi paylaşımının tanımı ve kamu kurumları açısından önemi ele alınmakta, ardından siber güvenlik tehditlerinin doğası ve bu tehditlere karşı alınması gereken önlemler tartışılmaktadır. Bilgi paylaşımı ve iş birliği ile ilgili teorik yaklaşımlar, sosyal sermaye teorisi, bilgi tabanlı teori ve örgütsel öğrenme teorisi gibi çerçeveler üzerinden açıklanmakta ve bilgi paylaşımının nasıl teşvik edilebileceği incelenmektedir.

Türkiye'de kamu kurumları arasında bilgi paylaşımını engelleyen bürokratik engeller, kurumsal güven eksikliği ve yasal sınırlamalar gibi faktörler de çalışma kapsamında ele alınmaktadır. Bu engellerin aşılması için önerilen yöntemler ve stratejiler tartışılmakta, bilgi paylaşımının etkin bir şekilde gerçekleştirilmesi için gerekli olan bütünleşik hizmet anlayışı ve politika önerileri sunulmaktadır. Bütünleşik hizmet anlayışı unsurlarının entegrasyonu, bilgi akışının düzenlenmesi ve kurumlar arası iş birliğinin artırılması için önemli çözümler olarak değerlendirilmektedir. Bu doğrultuda on temel politika önerisi geliştirilmiştir. Son olarak, çalışmanın bulguları özetlenmekte ve gelecekteki araştırmalar için öneriler sunulmaktadır.

Bu çalışma, Türkiye'deki kamu kurumlarının bilgi paylaşımını nasıl daha etkili hale getirebileceği konusunda kapsamlı bir analiz sunmakta ve siber güvenlik tehditlerine karşı daha dirençli bir yapı oluşturulmasına katkıda bulunmaktadır. Bilgi paylaşımı ve iş birliği konularında sağlanacak iyileştirmeler, kamu yönetiminin modernizasyonunu destekleyerek vatandaşlara sunulan hizmetlerin kalitesini artıracaktır.

KURUMLARARASI BİLGİ PAYLAŞIMI VE SİBER GÜVENLİK

Bilgi Paylaşımının Tanımı ve Önemi

Bilgi paylaşımı, bir birey veya kuruluşun sahip olduğu bilgileri diğer bireyler veya kuruluşlarla aktif olarak paylaşma süreci olarak tanımlanmaktadır. Bu süreç, veri, bilgi ve bilgeliğin bir kişiden veya birimden diğerine aktarılmasını içermekte olup, iletişim, koordinasyon ve iş birliği gibi kritik yönleri barındırmaktadır (Wang ve Noe, 2010: 117). Bilgi paylaşımının türleri arasında bilgi yayma, bilgi aktarımı, bilgi oluşturma ve bilgi alışverişi gibi kategoriler bulunmaktadır (Davenport ve Prusak, 1998: 70). Bu kategoriler, bilgi paylaşımının farklı biçimlerde gerçekleşebileceğini ve her birinin kendine özgü yöntemleri ve stratejileri olduğunu göstermektedir.

Kamu kurumları açısından bilgi paylaşımı, daha iyi karar verme, hizmet kalitesini artırma ve kaynakları daha verimli kullanma gibi pek çok önemli fayda sağlamaktadır. Örneğin, sağlık sektöründe kamu hastaneleri arasındaki bilgi paylaşımı, hastalıkların yayılmasını engellemede ve halk sağlığını korumada kritik bir rol oynamaktadır (Yang ve Maxwell, 2011: 168). Bilgi paylaşımı, kamu kurumlarının kriz yönetimi ve acil durum müdahalelerinde de etkili olmaktadır. Doğal afetler sırasında bilgi paylaşımı, kaynakların hızlı ve etkili bir şekilde dağıtılmasını sağlamakta ve afet yönetiminde koordinasyonu artırmaktadır.

Siber güvenlik bağlamında, bilgi paylaşımı, kamu kurumları arasında tehditlere karşı ortak bir savunma mekanizması oluşturmayı mümkün kılmaktadır. Örneğin, bir kamu kurumunda tespit edilen bir siber tehdit, diğer kurumlarla paylaşılarak benzer saldırılara karşı önleyici tedbirlerin alınmasına olanak tanımaktadır (Wang ve Noe, 2010: 125-126). Bu tür bilgi paylaşımı, kurumlar arası iş birliğini ve koordinasyonu güçlendirmekte ve siber saldırılara karşı daha dirençli bir yapının oluşturulmasına katkıda bulunmaktadır.

Bilgi paylaşımını engelleyen bürokratik engeller ve bu engellerin aşılması için önerilen yöntemler de önemli bir tartışma konusudur. Kurumsal güven eksikliği, yasal sınırlamalar, teknik uyumsuzluklar ve kültürel bariyerler, bilgi paylaşımını zorlaştıran başlıca faktörlerdir. Örneğin, farklı kamu kurumları arasındaki yasal uyumsuzluklar, bilgi paylaşımının önünde büyük bir engel teşkil edebilmektedir. Bu tür zorlukların aşılması için, ortak bilgi paylaşım protokollerinin geliştirilmesi ve kurumlar arası güvenin artırılması gerekmektedir (Tsai, 2002: 180). Bilgi paylaşımının kurumsal güveni artırdığı ve siber saldırılara karşı kurumlar arası dayanışmayı güçlendirdiği de vurgulanmaktadır. Bilgi paylaşımı, kurumların sadece kendi deneyimlerinden değil, aynı zamanda diğer kurumların tecrübelerinden de öğrenmelerine olanak tanımaktadır. Bu durum, siber saldırılar karşısında daha hazırlıklı ve dirençli bir yapı oluşturulmasına katkıda bulunmaktadır (Nonaka, 1994: 27). Örneğin, siber saldırılara maruz kalan bir kurumun deneyimleri, diğer kurumlarla paylaşılması durumunda, benzer tehditlerle karşılaşma olasılığı olan

kurumlar için değerli bir kaynak oluşturabilmektedir. Ayrıca, bilgi paylaşımı için kurum içi örgütlenmeler inşa edilmesi de kurumsal öğrenme sürecini hızlandırmakta ve organizasyonel hafızanın gelişimine katkıda bulunmaktadır. Bu durum, kamu kurumlarının stratejik hedeflerine ulaşmada daha esnek ve uyumlu olmalarını sağlamaktadır (Cummings, 2004: 355). Kamu kurumları, bilgi paylaşımı yoluyla yenilikçi çözümler geliştirebilmekte ve hizmet kalitesini artırabilmektedir. Örneğin, belediyeler arasında akıllı şehir uygulamaları hakkında bilgi paylaşımı, daha verimli ve sürdürülebilir şehir yönetimine katkıda bulunabilmektedir.

Bilgi paylaşımı, kamu kurumlarının hem bireysel hem de kolektif performansını artırmada kritik bir rol oynamaktadır. Bilgi paylaşımının önemi, kamu yönetimi literatüründe geniş bir yer bulmakta ve kamu kurumlarının operasyonel ve stratejik başarılarına doğrudan katkıda bulunmaktadır. Bilgi paylaşımının etkin bir şekilde yönetilmesi, kamu kurumlarının karşılaştıkları karmaşık ve dinamik sorunlara daha etkili çözümler üretmelerine olanak tanımaktadır. Bu nedenle, kamu kurumları arasında bilgi paylaşımının önemi, kurumlar arası güveni artırmakta, iş birliğini güçlendirmekte ve hizmet kalitesini yükseltmektedir.

Siber Güvenlik Tehditlerinin Doğası

Siber güvenlik tehditleri, bilgi sistemlerine, ağlara ve veriye zarar verme veya erişim sağlama amacıyla gerçekleştirilen kötü niyetli faaliyetler olarak tanımlanmaktadır (Akt.Yılmaz, 2017: 26). Bu tehditler, çeşitli formlarda ortaya çıkmakta olup, her biri farklı teknikler ve hedefler içermektedir. Siber güvenlik tehditleri genellikle kötü amaçlı yazılımlar (malware), fidye yazılımları (ransomware), hizmet aksatma saldırıları (DDoS), oltalama (phishing) ve iç tehditler gibi kategorilere ayrılmaktadır (Symantec, 2019: 4; Çelik ve Çeliktaş, 2018: 108-111). Etkili mücadele süreçlerini kolaylaştırmak amacıyla oluşturulan bu kategoriler ışığında siber güvenliğe ilişkin üç temel tehdit türü şöyle açıklanabilir:

1- Kötü amaçlı yazılımlar (malware), bilgisayar sistemlerine zarar vermek veya kontrol altına almak amacıyla tasarlanmış yazılımlardır. Virüsler, solucanlar, truva atları ve casus yazılımlar bu kategoriye girmektedir. Fidye yazılımları (ransomware), kullanıcıların verilerini şifreleyerek şifreyi çözmek için fidye ödemelerini talep eden kötü amaçlı yazılımlardır (Anderson ve Agarwal, 2010: 614).

2- Hizmet aksatma saldırıları (DDoS), hedef sistemlerin veya ağların hizmet vermesini engellemek amacıyla aşırı yüklenmesine neden olan saldırılardır. Bu tür saldırılar, hedeflenen sunucuların veya ağların işleyişini durdurmakta ve kullanıcıların hizmetlere erişimini engellemektedir (Mirkovic ve Reiher, 2004: 40).

3- Oltalama (phishing), kullanıcıların kişisel bilgilerini, şifrelerini veya finansal bilgilerini ele geçirmek amacıyla sahte e-postalar veya web siteleri kullanarak gerçekleştirilen dolandırıcılık girişimleridir. İç tehditler ise, kuruluş içindeki çalışanlar veya eski çalışanlar tarafından gerçekleştirilen ve kurumun bilgi sistemlerine zarar verme veya bilgi çalma amaçlı faaliyetleri içermektedir (Greitzer, vd., 2014: 2395).

İncelenen bu siber güvenlik tehditleri, ekonomik kayıplara, veri ihlallerine ve kurumsal itibar kaybına neden olmaktadır. Örneğin, bir fidye yazılımı saldırısı, kritik verilerin kaybına ve büyük maliyetlere yol açabilmektedir. Hizmet aksatma saldırıları, şirketlerin faaliyetlerini durdurarak gelir kaybına ve müşteri memnuniyetsizliğine neden olabilmektedir. Ayrıca, siber güvenlik tehditleri, ulusal güvenlik açısından da ciddi riskler taşımaktadır. Devlet kurumlarına yönelik siber saldırılar, hassas bilgilerin çalınmasına veya manipüle edilmesine yol açabilmektedir. Bu durum, ulusal güvenliği tehdit edebilecek boyutlara ulaşabilmektedir.

Siber Güvenlik Tehditlerine Karşı Alınması Gereken Önlemler: Siber güvenlik tehditlerine karşı alınması gereken önlemler, teknik, idari ve eğitsel stratejilerden oluşmaktadır. Teknik önlemler arasında, güçlü şifreleme yöntemleri, güvenlik duvarları ve antivirüs yazılımları gibi araçlar yer almaktadır (Symantec, 2019: 18). İdari önlemler ise, güvenlik politikalarının oluşturulması, risk yönetimi süreçlerinin uygulanması ve düzenli güvenlik denetimlerinin yapılmasını içermektedir (NIST, 2018: 5). Eğitsel stratejiler, çalışanların siber güvenlik konusunda bilinçlendirilmesi ve eğitilmesini kapsamaktadır. Çalışanların oltalama girişimlerine karşı dikkatli olmaları, güvenli şifre kullanımı ve şüpheli e-postaları bildirme gibi konularda eğitilmeleri gerekmektedir (ENISA, 2019: 22).

Nihai olarak, siber güvenlik tehditleri, bilgi sistemlerine ve ağlara yönelik çeşitli ve karmaşık tehditler olarak ortaya çıkmaktadır. Bu tehditlere karşı etkili önlemler alınması hem teknik hem de idari stratejilerin yanı sıra eğitim ve farkındalık programlarını içermektedir. Kamu kurumları ve özel sektör, bu tehditlere karşı dayanıklılıklarını artırmak için iş birliği yapmalı ve sürekli olarak güvenlik önlemlerini güncellemelidir.

Bilgi Paylaşımı ve İşbirliğine İlişkin Teorik Yaklaşımlar

Bilgi paylaşımı ve kurumlar arası iş birliği, bilgi yönetimi ve örgütsel teori literatüründe geniş bir şekilde ele alınan konular arasında yer almaktadır. Bilgi paylaşımının teorik temelleri, genellikle sosyal sermaye teorisi, bilgi tabanlı teori ve örgütsel öğrenme teorisi gibi yaklaşımlar üzerinden açıklanmaktadır. Sosyal sermaye teorisi, bireyler ve

kurumlar arasındaki sosyal ilişkilerin, bilgi paylaşımını nasıl kolaylaştırdığını veya engellediğini açıklamaktadır. Bu teoriye göre, sosyal ağların yapısı ve niteliği, bilgi akışını etkileyen kritik faktörler arasında yer almaktadır (Nahapiet ve Ghoshal, 1998: 243). Bilgi tabanlı teori, bilgiye dayalı kaynakların, kurumların rekabetçi avantaj elde etmesinde temel rol oynadığını öne sürmektedir. Bu teoriye göre, bilgi paylaşımı, kurumların yenilikçilik kapasitesini artırmakta ve stratejik hedeflerine ulaşmada kritik bir unsur olmaktadır (Grant, 1996: 110). Bilgi tabanlı teori, özellikle bilgi yaratma, transfer ve entegrasyon süreçlerine odaklanarak, kurumlar arası iş birliğinin önemini vurgulamaktadır. Örgütsel öğrenme teorisi ise, kurumların sürekli olarak bilgi edinme, paylaşma ve uygulama süreçleri yoluyla nasıl geliştiğini ve adapte olduğunu açıklamaktadır. Bu teoriye göre, bilgi paylaşımı, örgütsel öğrenme sürecinin merkezinde yer almakta ve kurumların çevresel değişimlere uyum sağlamasına yardımcı olmaktadır (Argote ve Ingram, 2000: 151). Örgütsel öğrenme, bireysel öğrenme süreçlerinin yanı sıra, takım ve kurumsal düzeyde de gerçekleşmektedir.

Bilgi paylaşımı ve iş birliği ile ilgili modeller arasında, Nonaka ve Takeuchi'nin (2007) bilgi yaratma modeli dikkat çekmektedir. Bu model, bilgi yaratma sürecini, örtük bilgiden açık bilgiye dönüşüm süreci olarak tanımlamaktadır. Bu model, sosyalizasyon, dışsallaştırma, birleştirme ve içselleştirme aşamalarını içermektedir. Bu süreçler, bilgi paylaşımının dinamik ve sürekli bir döngü olduğunu göstermektedir (Nonaka ve Takeuchi, 2007: 166-168). Bir diğer önemli model, Crossan, Lane ve White'ın (1999: 529) 4I modeli olarak bilinen örgütsel öğrenme modelidir. Bu model, bilgi paylaşımını ve öğrenmeyi dört seviyede ele almaktadır: bireysel, takımsal, örgütsel ve kurumsal. 4I modeli, sezgisel öğrenme, yorumlama, bütünleştirme ve kurumsallaştırma süreçlerini içermekte olup, bilgi paylaşımının bu süreçler arasındaki etkileşimlerle nasıl gerçekleştiğini açıklamaktadır. Kurumlar arası iş birliği ise, genellikle ağ teorisi ve açık inovasyon yaklaşımları ile incelenmektedir. Ağ teorisi, kurumlar arasındaki bağlantıların, bilgi akışını ve iş birliğini nasıl etkilediğini analiz etmektedir. Bu teoriye göre, ağ yapılarının özellikleri, bilgi paylaşımının etkinliğini belirlemektedir (Powell, vd., 1996: 120). Açık inovasyon yaklaşımı, kurumların dış kaynaklardan gelen bilgi ve fikirleri kullanarak inovasyon süreçlerini nasıl geliştirdiğini açıklamaktadır. Bu yaklaşım, kurumlar arası iş birliğini ve bilgi paylaşımını, yenilikçilik ve rekabet avantajı elde etme sürecinin temel bir unsuru olarak görmektedir (Chesbrough, 2003: 36).

Bilgi paylaşımı ve iş birliği, sosyal sermaye teorisi, bilgi tabanlı teori ve örgütsel öğrenme teorisi gibi çeşitli teorik yaklaşımlar ve modellerle açıklanmaktadır. Bu teorik çerçeveler, bilgi paylaşımının kurumlar arasındaki iş birliğini nasıl teşvik ettiğini ve bu süreçlerin kamu kurumlarının stratejik ve operasyonel hedeflerine ulaşmada ne kadar kritik olduğunu ortaya koymaktadır. Kurumların daha etkin ve verimli çalışabilmesi, güvenli ve etkili bilgi paylaşımı ve iş birliği mekanizmalarının oluşturulmasına bağlıdır.

TÜRKİYE'DEKİ KAMU KURUMLARI ARASINDA BİLGİ PAYLAŞIMI

Türkiye'de kamu kurumları arasındaki bilgi paylaşımı, bilgi teknolojilerinin hızlı gelişimi ve dijital dönüşüm süreçlerinin ivme kazanmasıyla birlikte giderek daha önemli hale gelmiştir. Bu süreçler, kamu hizmetlerinin sunumunda verimliliği ve etkinliği artırmak amacıyla birçok yenilikçi proje ve uygulamanın hayata geçirilmesine olanak tanımaktadır. Bilgi teknolojilerindeki ilerlemeler, kamu kurumlarının iş süreçlerini optimize etmelerine ve hizmet sunumunda entegrasyonu sağlamalarına yardımcı olmaktadır. Bu bağlamda yürütülen programlardan birkaçı şöyle açıklanabilir:

e-Devlet Kapısı: Türkiye'de kamu kurumları arasındaki bilgi paylaşımının en önemli örneklerinden biri e-Devlet Kapısı'dır. 2008 yılında kullanıma açılan e-Devlet Kapısı, vatandaşların ve kurumların çeşitli kamu hizmetlerine tek bir noktadan erişimini sağlamaktadır. Bu platform, kamu kurumları arasındaki bilgi paylaşımını kolaylaştırmakta ve kurumların entegre bir şekilde hizmet sunmasına olanak tanımaktadır. E-Devlet Kapısı, 2024 itibarıyla 8,000'den fazla hizmet sunmakta olup, 565 milyondan fazla kayıtlı kullanıcıya sahiptir (T.C. Dijital Dönüşüm Ofisi, 2024).

Ulusal Yargı Ağı Bilişim Sistemi (UYAP): Adalet Bakanlığı tarafından geliştirilen UYAP, yargı süreçlerinin dijital ortamda yürütülmesini sağlayan bir bilgi sistemi olup, kamu kurumları arasındaki bilgi paylaşımını desteklemektedir. UYAP, mahkemeler, savcılıklar, ceza infaz kurumları ve diğer adalet hizmeti sunan birimler arasında etkin bilgi paylaşımı ve koordinasyonu sağlamaktadır. Bu sistem sayesinde, yargı süreçleri hızlanmakta ve adalet hizmetlerinin kalitesi artmaktadır (UYAP Bilişim Sistemi, 2024).

Sağlık Bilgi Sistemleri (SBS): Sağlık Bakanlığı'na bağlı olarak çalışan Sağlık Bilgi Sistemleri Müdürlüğü, sağlık kurumları arasındaki bilgi paylaşımını ve entegrasyonu sağlamaktadır. Bu sistem kapsamında Merkezi Hekim Randevu Sistemi (MHRS), Halk Sağlığı Yönetim Sistemi (HSYS) ve e-Nabız gibi çeşitli alt sistemler yer almaktadır. Sağlık Bilgi Sistemleri sayesinde, hasta verileri elektronik ortamda tutulmakta ve sağlık hizmetlerinin etkinliği artırılmaktadır. Ayrıca, bu sistemler aracılığıyla sağlık kurumları arasında bilgi paylaşımı kolaylaşmakta

ve hastaların tedavi süreçleri daha etkin bir şekilde yönetilmektedir (T.C. Sağlık Bilgi Sistemleri Genel Müdürlüğü. 2024).

Kamu Entegre Veri Merkezi (KEVM): KEVM, kamu kurumları arasındaki veri paylaşımını ve iş birliğini artırmak amacıyla kurulmuş bir veri merkezi olup, çeşitli kamu hizmetlerinin daha entegre ve verimli sunulmasını sağlamaktadır. KEVM, farklı kamu kurumlarının verilerini tek bir platformda toplamakta ve bu verilerin güvenli bir şekilde paylaşılmasına olanak tanımaktadır. KEVM, veri güvenliği ve gizliliği konularında da önemli bir rol oynamaktadır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024).

Merkezi Nüfus İdaresi Sistemi (MERNİS): Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü tarafından geliştirilen MERNİS, Türkiye'deki tüm vatandaşların nüfus bilgilerinin elektronik ortamda tutulduğu bir sistemdir. MERNİS, kamu kurumları arasında nüfus verilerinin güvenli ve hızlı bir şekilde paylaşılmasını sağlamakta olup, kamu hizmetlerinin daha etkin ve verimli sunulmasına katkıda bulunmaktadır. MERNİS sayesinde, kamu kurumları arasındaki iş birliği ve koordinasyon artırılmakta, bürokratik işlemler hızlanmaktadır (T.C. Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, 2024).

Türkiye'de kamu kurumları arasındaki bilgi paylaşımı, çeşitli projeler ve sistemler aracılığıyla geliştirilmektedir. Bu projeler, kamu hizmetlerinin kalitesini artırmakta, kurumlar arası iş birliğini ve koordinasyonu güçlendirmekte ve vatandaşlara daha etkili hizmet sunulmasını sağlamaktadır. Mevcut uygulamalar, Türkiye'deki dijital dönüşüm sürecinin önemli bir parçası olarak, kamu kurumları arasındaki bilgi paylaşımını ve iş birliğini sürekli olarak geliştirmeyi amaçlamaktadır.

Türkiye'de kamu kurumları arasında bilgi paylaşımını engelleyen çeşitli bürokratik engeller bulunmaktadır. Bu engeller, kurumsal yapılar, yasal düzenlemeler, teknik uyumsuzluklar ve kültürel bariyerler gibi faktörlerden kaynaklanmaktadır. Bu bürokratik engellerin detaylı bir analizi yapılmakta ve bu engellerin aşılması için önerilen yöntemler tartışılmaktadır.

Kurumsal Yapılar: Kamu kurumları arasındaki bilgi paylaşımını zorlaştıran önemli faktörlerden biri, kurumsal yapılar arasındaki hiyerarşik ve silo temelli organizasyonlardır. Bu yapıların neden olduğu iletişim kopuklukları ve koordinasyon eksiklikleri, bilgi akışını engelleyebilmektedir. Genellikle belediyeler arasındaki bilgi paylaşımında yaşanan sorunlar, yerel yönetimlerin bağımsız yapıları ve merkezi idare ile olan ilişkisinden kaynaklanmaktadır. Bu sorunun aşılması için, kurumlar arası daha yatay ve ağ temelli bir yapı benimsenmesi önerilmektedir. Ayrıca, kurumlar arasında ortak çalışma gruplarının oluşturulması ve düzenli toplantılarla bilgi alışverişinin teşvik edilmesi, iletişimi ve iş birliğini artıracaktır.

Yasal Düzenlemeler: Bilgi paylaşımını engelleyen bir diğer önemli faktör, yasal ve düzenleyici engellerdir. Kamu kurumları arasında bilgi paylaşımı, genellikle veri koruma ve gizlilik yasaları tarafından kısıtlanmaktadır. Örneğin, Kişisel Verilerin Korunması Kanunu (KVKK), kamu kurumlarının veri paylaşımını belirli kurallar ve sınırlamalar dâhilinde yapmalarını zorunlu kılmaktadır (Resmî Gazete, 2016). Bu durum, bilgi paylaşımının yasal çerçevede güvenli bir şekilde yapılmasını zorlaştırmaktadır. Bu engelin aşılması için, bilgi paylaşımına yönelik yasal düzenlemelerin gözden geçirilmesi ve güncellenmesi gerekmektedir. Özellikle, veri paylaşımı ve gizliliği ile ilgili yasaların, bilgi güvenliğini sağlarken bilgi paylaşımını da teşvik edecek şekilde düzenlenmesi önem arz etmektedir.

Teknik Uyumsuzluklar: Kamu kurumları arasında bilgi paylaşımını zorlaştıran teknik uyumsuzluklar da önemli bir engel teşkil etmektedir. Farklı kurumların kullandığı bilgi teknolojileri ve yazılımlar arasındaki uyumsuzluklar, veri paylaşımını ve entegrasyonunu zorlaştırmaktadır. Örneğin, Türkiye'de sağlık sektörü ile adalet sistemi arasındaki bilgi paylaşımında yaşanan teknik sorunlar, farklı yazılım ve veri formatlarının kullanılması nedeniyle ortaya çıkmaktadır. Bu sorunun aşılması için, standartlaştırılmış bilgi teknolojileri ve protokollerinin benimsenmesi gerekmektedir. Kurumlar arasında ortak veri formatlarının ve standartlarının belirlenmesi, teknik uyumsuzlukların giderilmesine yardımcı olacaktır.

Kültürel Bariyerler: Bilgi paylaşımını engelleyen bir diğer faktör ise, kurumsal kültür ve çalışanların bilgi paylaşımına yönelik tutumlarıdır. Kurumlar arasında rekabetçi bir kültürün hâkim olması, bilgi paylaşımını olumsuz etkilemektedir. Bu sorunun aşılması için, kurumlar arasında güvenin tesis edilmesi ve bilgi paylaşımının teşvik edilmesi gerekmektedir. Çalışanların bilgi paylaşımının önemini anlamaları ve bu konuda teşvik edilmeleri için eğitim programları düzenlenmelidir. Ayrıca, bilgi paylaşımını teşvik eden ödül ve tanıma sistemlerinin oluşturulması da bu konuda olumlu bir etki yaratacaktır.

Önerilen Yöntemler: Bilgi paylaşımını engelleyen bürokratik engellerin aşılması için çeşitli yöntemler önerilmektedir. Öncelikle, kurumlar arasında ortak bilgi paylaşım politikalarının ve protokollerinin geliştirilmesi gerekmektedir. Bu politikalar, bilgi paylaşımının yasal, güvenli ve etkin bir şekilde yapılmasını sağlayacaktır. Ayrıca, bilgi paylaşımını kolaylaştırmak için teknolojik altyapının güçlendirilmesi ve entegrasyonun artırılması

önemlidir. Kurumlar arasında güvenin artırılması ve bilgi paylaşımının teşvik edilmesi için düzenli iletişim ve iş birliği platformlarının oluşturulması da önemli bir adımdır (Cummings, 2004: 355).

Türkiye'de kamu kurumları arasında bilgi paylaşımını engelleyen bürokratik engeller, çeşitli yöntemler ve stratejilerle aşılabilir. Bu engellerin üstesinden gelmek, kamu kurumlarının daha etkili ve verimli çalışmasını sağlamakta ve vatandaşlara daha kaliteli hizmet sunulmasına olanak tanımaktadır

KURUMLAR ARASI İŞ BİRLİĞİNİN GELİŞTİRİLMESİNE YÖNELİK POLİTİKA ÖNERİLERİ

Bilgi paylaşımının etkinliğini artırmak ve kamu kurumları arasındaki iş birliğini güçlendirmek amacıyla çeşitli politika önerileri inşa etmek gerekmektedir. Bu öneriler, bilgi güvenliği, yasal düzenlemeler, eğitim ve farkındalık artırma gibi çeşitli alanlarda stratejik adımlar içermelidir. Ancak, kamu kurumları arasında etkin bir bilgi paylaşımının önündeki teknik, hukuki ve kurumsal engeller, koordinasyon eksikliği ve güvenlik riskleri gibi faktörler, sürecin optimal düzeyde işlemesini zorlaştırmaktadır. Bu bağlamda, Türkiye'de kamu kurumları arasındaki bilgi paylaşımının etkinliğini artırmak amacıyla on temel politika önerisi geliştirilmiştir. Bu öneriler, veri entegrasyonu ve bilgi paylaşım altyapısından ortak risk yönetimi çerçevesine, insan kaynakları kapasitesinin artırılmasından yasal düzenlemelerin güncellenmesine kadar geniş bir perspektif sunmaktadır. Bu politika önerilerinin amacı, kamu kurumlarının daha koordineli, güvenli ve verimli bir şekilde çalışmasını sağlamak, vatandaş odaklı hizmet sunumunu güçlendirmek ve kamu yönetiminde dijital dönüşüm sürecini hızlandırmaktır. Türkiye'deki kamu kurumları için bilgi paylaşımının etkinliğini artırmak amacıyla önerilen bu politika ve stratejiler aşağıda detaylandırılmaktadır.

1- Veri Entegrasyonu ve Bilgi Paylaşım Altyapısı: Kamu kurumları arasındaki veri entegrasyonu, hizmetlerin etkinliğini artırmanın yanı sıra vatandaşlara daha hızlı ve kesintisiz hizmet sunulmasını sağlamaktadır. Türkiye'de bu alanda çeşitli kurumlar tarafından yürütülen projeler bulunmaktadır. Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, vatandaşların kimlik, adres ve aile bilgilerini içeren MERNİS (Merkezi Nüfus İdaresi Sistemi) ile tüm kamu kurumlarına temel bir veri kaynağı sağlamaktadır. Gelir İdaresi Başkanlığı (GİB), vergi mükelleflerinin bilgilerini içeren VEDOP (Vergi Daireleri Otomasyon Projesi) sistemi ile çeşitli kamu ve özel sektör kurumlarına güvenli veri paylaşımı imkânı sunmaktadır. Sosyal Güvenlik Kurumu (SGK), MEDULA ve e-Nabız sistemleri ile hastaneler, eczaneler ve sağlık kurumları arasındaki bilgi paylaşımını sağlamaktadır. Türkiye'de kamu kurumlarının bilgi paylaşımı büyük ölçüde e-Devlet Kapısı üzerinden entegre edilmektedir (https://cbddo.gov.tr). Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yönetilen bu platform, farklı kamu kurumlarının hizmetlerini tek bir çatı altında toplayarak vatandaşların tek noktadan erişimini kolaylaştırmaktadır. Adalet Bakanlığı tarafından geliştirilen Ulusal Yargı Ağı Projesi (UYAP), mahkemeler, emniyet, ceza infaz kurumları ve noterler arasında veri entegrasyonunu sağlayarak yargı süreçlerini hızlandırmaktadır (https://uyap.gov.tr/).

Bu entegrasyon süreçlerinde ortak veri standartlarının geliştirilmesi gerekmektedir. Türkiye Bilişim Derneği (TBD) ve TÜBİTAK BİLGEM, kamu kurumlarının veri yönetimi alanındaki stratejik yaklaşımlarına katkı sağlayan yapılar olarak öne çıkmaktadır. Kamu kurumları, ortak veri paylaşım protokolleri belirleyerek, veri akışını düzenlemeli ve hizmetler arası uyumluluğu artırmalıdır. Kamu Sertifikasyon Merkezi (KSM) tarafından sağlanan elektronik imza altyapısı, kamu kurumları arasında güvenli kimlik doğrulama süreçlerini desteklemekte ve veri bütünlüğünü sağlamaktadır. Türkiye'de veri entegrasyonu süreçlerinde, siber güvenlik tehditlerine karşı uçtan uca şifreleme, çok faktörlü kimlik doğrulama ve merkezi güvenlik izleme sistemlerinin geliştirilmesi büyük önem taşımaktadır. Bilgi Teknolojileri ve İletişim Kurumu (BTK), kamu kurumlarının bilgi güvenliği politikalarını düzenleyen ve denetleyen bir yapı olarak kritik bir rol üstlenmektedir. Türkiye Siber Olaylara Müdahale Merkezi (USOM), kamu kurumlarında tespit edilen siber tehditleri analiz ederek önleyici tedbirlerin alınmasını sağlamakta, böylece kurumlar arası veri entegrasyonunun güvenli bir şekilde yürütülmesine katkı sunmaktadır.

Türkiye'de veri paylaşımı ve entegrasyonu süreçlerinin başarıya ulaşması için, blok zinciri tabanlı veri doğrulama sistemleri gibi yeni teknolojiler uygulanmalı, kamu kurumları arasında entegre bir veri güvenliği politikası benimsenmelidir. Sanayi ve Teknoloji Bakanlığı tarafından desteklenen Dijital Dönüşüm Projeleri, kamu kurumlarının veri yönetimi süreçlerinde inovatif yaklaşımlar benimsemesini teşvik etmektedir. T.C. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, merkezi kimlik doğrulama ve veri entegrasyonu konularında geliştirdiği projelerle, diğer kamu kurumları için referans bir yapı oluşturmaktadır.

2- Ortak Risk Yönetimi Çerçevesi: Türkiye'de siber güvenlik tehditlerine karşı kurumlar arasında ortak hareket edilmesi zorunludur. Bilgi Teknolojileri ve İletişim Kurumu (BTK), kamu kurumlarının siber güvenlik politikalarını denetleyen bir yapı olarak risk yönetimi süreçlerini belirlemektedir. Türkiye Siber Olaylara Müdahale Merkezi (USOM), kamu kurumlarında tespit edilen güvenlik açıklarını analiz ederek önleyici tedbirlerin alınmasını sağlamaktadır. Kamu kurumları için ortak bir siber tehdit erken uyarı sistemi kurulmalı ve veri güvenliği konusunda sürekli güncellenen protokoller benimsenmelidir.

3- Süreç Optimizasyonu ve Hizmet Entegrasyonu: Bütünleşik hizmet yönetimi, vatandaşlara kesintisiz ve verimli hizmet sunumu hedefini gütmektedir. Örneğin, belediyeler, Ticaret Bakanlığı, Çevre, Şehircilik ve İklim Değişikliği Bakanlığı ve Gelir İdaresi Başkanlığı, işyeri açma süreçlerinde koordineli çalışmalıdır. Tapu ve Kadastro Genel Müdürlüğü ile Bankalararası Kart Merkezi (BKM), tapu işlemlerinin dijitalleşmesini sağlayarak finansal süreçlerle entegrasyonu hızlandırmalıdır.

4- İnsan Kaynakları ve Yetkinlik Paylaşımı: Siber güvenlik alanında uzman personelin her kurumda bulunması yerine, ortak bir uzman havuzu oluşturulmalıdır. Siber Olaylara Müdahale Ekibi (SOME), kritik kamu kurumlarında saldırılara hızlı yanıt verebilmek için genişletilmelidir. TÜBİTAK BİLGEM, kamu kurumlarına siber güvenlik danışmanlığı sağlamakta olup, bu desteğin yaygınlaştırılması gerekmektedir.

5- Kriz Yönetimi ve İş Sürekliliği: Siber güvenlik tehditleri karşısında kurumların tek başlarına hareket etmeleri yerine, koordineli bir kriz yönetimi yaklaşımı benimsemeleri gerekmektedir. Bu kapsamda; BTK ve USOM koordinasyonunda, kamu kurumlarının siber güvenlik tatbikatları yapması zorunlu hale getirilmelidir. Kamu Bulut Bilişim Altyapısı, veri yedekleme süreçlerinde kullanılmalı ve olası krizlerde iş sürekliliğini sağlamalıdır.

6- Yasal ve İdari Çerçeve: Kamu kurumları arasındaki bilgi paylaşımının önündeki yasal engellerin kaldırılması için, mevcut yasal düzenlemelerin gözden geçirilmesi ve güncellenmesi gerekmektedir. Özellikle, Bilgi Edinme Hakkı Kanunu gibi yasaların bilgi paylaşımını teşvik edecek şekilde düzenlenmesi önemlidir (Resmî Gazete, 2003). Yasal düzenlemelerin esnek ve açık olması, veri paylaşımının yasal ve güvenli bir şekilde gerçekleştirilmesine olanak tanıyacaktır. Türkiye'de kamu kurumlarının veri paylaşımını düzenleyen Kişisel Verileri Koruma Kurumu (KVKK) ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, yasal düzenlemeleri yönlendiren iki önemli yapıdır. Bu kurumların gözetiminde; Veri Paylaşım Protokolleri yasal altyapıya kavuşturulmalıdır. Dijital Hizmetlerin Hukuki Çerçevesi, Türkiye Büyük Millet Meclisi (TBMM) tarafından revize edilerek günümüz dijital ihtiyaçlarına uyarlanmalıdır.

7- Ortak Bilgi Paylaşım Protokollerinin Geliştirilmesi: Kamu kurumları arasında standartlaştırılmış bilgi paylaşım protokollerinin geliştirilmesi ve uygulanması, bilgi akışını kolaylaştıracaktır. Bu protokoller, veri formatları, güvenlik standartları ve paylaşım yöntemleri gibi konularda net yönergeler sağlamalıdır. Sağlık Bilgi Sistemleri (SBS) ve Ulusal Yargı Ağı Bilişim Sistemi (UYAP) gibi mevcut sistemlerin entegrasyonu ve standartlarının harmonize edilmesi, bilgi paylaşımını daha etkin hale getirecektir.

8- Teknolojik Altyapının Güçlendirilmesi: Bilgi paylaşımının etkinliğini artırmak için güçlü ve güvenilir bir teknolojik altyapı oluşturulmalıdır. Kamu kurumlarının bilgi sistemleri arasında uyumluluğun sağlanması ve veri güvenliğinin artırılması için gerekli yatırımlar yapılmalıdır. Özellikle, siber güvenlik önlemlerinin güçlendirilmesi, veri sızıntıları ve yetkisiz erişimlere karşı koruma sağlayacaktır. Bu bağlamda, kamu kurumları arasında veri merkezlerinin entegrasyonu ve bulut bilişim çözümlerinin kullanımı teşvik edilmelidir.

9- Eğitim ve Farkındalık Programları: Bilgi paylaşımının önemini ve gerekliliğini anlamak için kamu kurumlarının çalışanlarına yönelik eğitim ve farkındalık programları düzenlenmelidir. Bu programlar, çalışanların bilgi güvenliği, veri koruma ve paylaşım protokolleri konularında bilgi sahibi olmalarını sağlayacaktır. Ayrıca, bilgi paylaşımını teşvik eden ödül ve tanıma sistemlerinin oluşturulması, çalışanların bu konudaki motivasyonunu artıracaktır.

10- Kurumlar Arası Güvenin Artırılması: Kamu kurumları arasında güvenin tesis edilmesi, bilgi paylaşımının etkinliği açısından kritik bir öneme sahiptir. Kurumlar arası güveni artırmak için, düzenli iletişim ve iş birliği platformları oluşturulmalı ve ortak projeler teşvik edilmelidir. Ayrıca, güven artırıcı önlemler arasında şeffaflık, hesap verebilirlik ve ortak hedeflerin belirlenmesi de yer almaktadır. Güven ortamının sağlanması, kurumların birbirlerine karşı açık ve işbirlikçi bir tutum sergilemelerini kolaylaştıracaktır.

Sonuç olarak, Türkiye'de bütünleşik hizmet yönetimi, kamu kurumlarının veri entegrasyonu, siber güvenlik ve hizmet sunumunda daha etkin ve koordineli çalışmasını sağlayan kritik bir yaklaşımdır. Bu model, vatandaş odaklı, verimli ve güvenli bir kamu hizmeti yapısı oluşturmayı hedeflemektedir. Bilgi paylaşımının etkinliğini artırmak için geliştirilen bu politika önerileri, kamu kurumlarının daha verimli ve koordineli bir şekilde çalışmasını sağlayacaktır. Yasal düzenlemelerin güncellenmesi, teknolojik altyapının güçlendirilmesi, eğitim ve farkındalık programlarının uygulanması ve kurumlar arası güvenin artırılması, bilgi paylaşımının başarısını önemli ölçüde artıracaktır. Bu stratejiler, Türkiye'deki kamu kurumlarının modernizasyonunu destekleyerek vatandaşlara daha kaliteli hizmet sunulmasına katkıda bulunacaktır.

SONUÇ VE DEĞERLENDİRME

Bu çalışmada, Türkiye'de kamu kurumları arasındaki bilgi paylaşımının önemi ve bu süreci etkileyen faktörler ayrıntılı bir şekilde incelenmiştir. Araştırma bulguları, bilgi paylaşımının siber güvenlik tehditleriyle mücadelede ve kamu hizmetlerinin etkinliğini artırmada stratejik bir rol oynadığını ortaya koymaktadır. Bilgi paylaşımı, kamu kurumlarının daha iyi kararlar alabilmesi, hizmet kalitesini artırabilmesi ve kaynakları verimli kullanabilmesi için kritik bir süreçtir. Türkiye'de, e-Devlet Kapısı, UYAP ve Sağlık Bilgi Sistemleri gibi projeler, kamu kurumları arasında bilgi paylaşımını teşvik ederek kurumlar arası iş birliğini ve koordinasyonu güçlendirmektedir. Bu projeler, bilgi paylaşımının etkinliğini artırmakta ve kurumların karşılaştıkları zorlukları daha hızlı ve etkili bir şekilde aşmalarına olanak tanımaktadır.

Siber güvenlik tehditleri, çeşitli formlarda ortaya çıkmakta ve kamu kurumlarına yönelik ciddi riskler taşımaktadır. Kötü amaçlı yazılımlar, fidye yazılımları, hizmet aksatma saldırıları ve oltalama gibi tehditler, kurumların operasyonel sürekliliğini ve veri güvenliğini tehdit etmektedir. Bu tehditlere karşı alınan önlemler, bilgi paylaşımının etkinliği açısından kritik öneme sahiptir. Bilgi paylaşımı ve iş birliği süreçlerinin, sosyal sermaye teorisi, bilgi tabanlı teori ve örgütsel öğrenme teorisi gibi yaklaşımlarla desteklenmesi, kurumlar arası güvenin artırılmasına ve iş birliğinin teşvik edilmesine katkı sağlamaktadır.

Bu çalışmanın bulguları doğrultusunda, kamu kurumları arasındaki bilgi paylaşımının etkin bir şekilde gerçekleştirilmesi için bütünleşik hizmet yönetimi anlayışının benimsenmesi gerektiği sonucuna ulaşılmaktadır. Veri entegrasyonu, bilgi güvenliği, yasal çerçevenin güncellenmesi, insan kaynağı kapasitesinin artırılması ve kurumlar arası güvenin tesis edilmesi, bilgi paylaşımını destekleyen temel unsurlar olarak öne çıkmaktadır. Bu süreçte, dijital dönüşüm projelerinin yaygınlaştırılması, ortak veri paylaşım protokollerinin oluşturulması ve siber güvenlik risklerine karşı koordineli bir yaklaşım benimsenmesi kritik öneme sahiptir. Ayrıca, kamu kurumları arasındaki güven eksikliğini gidermek ve yasal engelleri aşmak için, ilgili düzenlemelerin bilgi paylaşımını teşvik edecek şekilde revize edilmesi ve kamu çalışanlarına yönelik eğitim ve farkındalık programlarının yaygınlaştırılması gerekmektedir. Sonuç olarak, bütünleşik hizmet yönetimi anlayışı çerçevesinde bilgi paylaşımının güvenli, etkin ve sürdürülebilir bir şekilde gerçekleştirilmesi sağlanmalı ve vatandaş odaklı kamu hizmetlerinin kalitesi artırılmalıdır. Bu bağlamda, kamu kurumlarının veri paylaşımı konusunda yasal mevzuata uyum sağlamaları ve eğitim programlarına katılmaları teşvik edilmelidir.

Gelecekteki araştırmalar için, bilgi paylaşımının etkinliğini artırmak amacıyla daha fazla ampirik çalışmanın yapılması ve bu çalışmalarda farklı sektörlerin ve kurumların deneyimlerinin incelenmesi önerilmektedir. Ayrıca, teknoloji altyapısının güçlendirilmesi ve standartların belirlenmesi, bilgi paylaşımının etkinliğini artırmak için önemli adımlar olacaktır. Kamu kurumları, güvenlik ve gizlilik önlemlerini güçlendirerek ve iş birliğini teşvik eden mekanizmalar oluşturarak, bilgi paylaşımını daha etkili hale getirebilirler. Bu stratejiler, kamu yönetiminin modernizasyonunu destekleyerek siber güvenlik tehditlerine karşı daha dirençli ve hazırlıklı bir yapı oluşturulmasına katkı sağlayacaktır.

KAYNAKÇA

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643.

Argote, L., & Ingram, P. (2000). Knowledge transfer: A basis for competitive advantage in firms. *Organizational Behavior and Human Decision Processes, 82*(1), 150-169.

Chesbrough, H. W. (2003). *Open Innovation: The new imperative for creating and profiting from technology*. Harvard Business School Press.

Crossan, M. M., Lane, H. W., & White, R. E. (1999). An organizational learning framework: From intuition to institution. *Academy of Management Review, 24*(3), 522-537.

Cummings, J. N. (2004). Work groups, structural diversity, and knowledge sharing in a global organization. *Management Science, 50*(3), 352-364.

Çelik, S., & Çeliktaş, B. (2018). Güncel siber güvenlik tehditleri: Fidye yazılımlar. *CyberPolitik Journal, 3*(5), 105-132.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business Press.

ENISA, (European Union Agency for Cybersecurity) (2019). Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity Erişim tarihi: 11.05.2024.

Fung, A. (2015). Putting the public back into governance: The challenges of citizen participation and its future. *Public administration review*, *75*(4), 513-522.

Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, *17*(S2), 109-122.

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., & Hohimer, R. E. (2012, January). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. In *2012 45th Hawaii International Conference on System Sciences* (pp. 2392-2401).

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39-53.

Nahapiet, J., & Ghoshal, S. (1998). Social capital, intellectual capital, and the organizational advantage. *Academy of management review*, *23*(2), 242-266.

NIST, (National Institute of Standards and Technology). (2018). Framework for improving critical infrastructure cybersecurity. https://complexdiscovery.com/wp-content/uploads/2019/10/Framework-for-Improving-Critical-Infrastructure-Cybersecurity.pdf Erişim tarihi: 28.06.2024.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, *5*(1), 14-37.

Nonaka, I., & Takeuchi, H. (2007). The knowledge-creating company. *Harvard business review*, *85*(7/8), 162.

Powell, W. W., Koput, K. W., & Smith-Doerr, L. (1996). Interorganizational collaboration and the locus of innovation: Networks of learning in biotechnology. *Administrative Science Quarterly*, *41*(1), 116-145.

Resmî Gazete, (2003). "4982 sayılı Bilgi Edinme Hakkı Kanunu. Resmî Gazete", 24 Ekim 2003, Sayı: 25269. https://www.resmigazete.gov.tr/eskiler/2003/10/20031024.htm Erişim tarihi: 18.06.2024.

Resmî Gazete, (2016). "6698 sayılı Kişisel Verilerin Korunması Kanunu", Resmî Gazete, *07 Nisan 2016, Sayı: 29677* https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5, Erişim tarihi: 22.06.2024.

Symantec. (2019). "Internet Security Threat Report" https://docs.broadcom.com/doc/istr-24-2019-en Erişim tarihi: 21.07.2024.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2024). "e-Devlet Kapısı Kullanım İstatiskitkleri", https://cbddo.gov.tr/ Erişim tarihi: 09.07.2024.

T.C. Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, "Merkezi Nüfus İdaresi Sistemi (MERNİS)" https://www.nvi.gov.tr/mernis Erişim tarihi: 14.07.2024.

T.C. Sağlık Bilgi Sistemleri Genel Müdürlüğü. (2024). "Hzimetler", https://sbsgm.saglik.gov.tr/?_Dil=1 Erişim tarihi: 04.07.2024.

T.C. Ulaştırma ve Altyapı Bakanlığı, "Kamu Entegre Veri Merkezi Projesi", https://hgm.uab.gov.tr/kamu-entegre-veri-merkezi-projesi Erişim tarihi: 20.07.2024.

Tsai, W. (2002). Social structure of "coopetition" within a multiunit organization: Coordination, competition, and intraorganizational knowledge sharing. *Organization Science*, *13*(2), 179-190.

UYAP, (2024), "UYAP Bilişim Sistemi" https://uyap.gov.tr/, Erişim tarihi: 09.07.2024.

Wang, & Noe, R. A. (2010). Knowledge sharing: A review and directions for future research. *Human Resource Management Review*, *20*(2), 115-131.

Yang, T. M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, *28*(2), 164-175.

Yılmaz, O. (2017). Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik. *Cyberpolitik Journal*, *2*(4), 22-43.