DÜZCE ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ISO 27001 BİLGİ GÜVENLİĞİ SİSTEMİ KONULU YAYINLARIN WOS VERİ TABANINA DAYALI BİBLİYOMETRİK ANALİZİ

Gözde AKBALIK KORKMAZ

YÜKSEK LİSANS TEZİ
TOPLAM KALİTE YÖNETİMİ ANABİLİM DALI

DANIŞMAN
Dr. Öğr. Ü. Okan BÜTÜNER

DÜZCE, 2023

DÜZCE ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ISO 27001 BİLGİ GÜVENLİĞİ SİSTEMİ KONULU YAYINLARIN WOS VERİ TABANINA DAYALI BİBLİYOMETRİK ANALİZİ

Gözde AKBALIK KORKMAZ

YÜKSEK LİSANS TEZİ
TOPLAM KALİTE YÖNETİMİ ANABİLİM DALI

DANIŞMAN
Dr. Öğr. Ü. Okan BÜTÜNER

DÜZCE, 2023

JÜRİ ÜYELERİ İMZA SAYFASI

T.C.
DÜZCE ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ISO 27001 BİLGİ GÜVENLİĞİ SİSTEMİ KONULU YAYINLARIN WOS VERİ TABANINA DAYALI BİBLİYOMETRİK ANALİZİ

Gözde AKBALIK KORKMAZ tarafından hazırlanan tez çalışması aşağıdaki jüri tarafından Düzce Üniversitesi Lisansüstü Eğitim Enstitüsü Toplam Kalite Yönetimi Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Dr. Öğr. Üyesi Okan BÜTÜNER

Düzce Üniversitesi Akçakocabey Siyasal Bilgiler Fak. Uluslarası İlişkiler Bölümü

Jüri Üyeleri

Dr. Öğr. Üyesi Okan BÜTÜNER

Düzce Üniversitesi Akçakocabey Siyasal Bilgiler Fak. Uluslarası İlişkiler Bölümü

_____

Doç. Dr. Mehmet Nurullah KURUTKAN

Düzce Üniversitesi İşletme Fak. Sağlık Yönetimi Bölümü

_____

Doç. Dr. Ömer Kürşad TÜFEKÇİ

Isparta Uygulamalı Bilimler Üniversitesi Turizm Fak. Turizm İşletmeciliği Bölümü

_____

Tez Savunma Tarihi: 03/01/2023

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

03/01/2023

Gözde AKBALIK KORKMAZ

İTHAF

Nil Hüma Akbalık'a …

TEŞEKKÜR METNİ

Öncelikle tez çalışmam sırasında kıymetli bilgi, birikim ve tecrübeleriyle bana yol gösteren, desteğini her zaman hissettiğim, öğrencisi olmaktan her zaman gurur duyduğum ve duyacağım çok değerli danışman hocam Dr. Öğr. Üyesi Okan Bütüner'e sonsuz teşekkür ve saygılarımı sunarım.

Yüksek lisans eğitimim boyunca ders aldığım Düzce Üniversitesi Toplam Kalite Yönetimi Yüksek Lisans bölümünün tüm hocalarına, araştırmam esnasında içtenliğini, manevi desteklerini esirgemeyen sabır, sevgi ve güveni ile süreci kolaylaştırdığı için Serhan Balkanal'a teşekkür ederim.

Yüksek lisans eğitimine başlamamda en önemli katkıyı sunan değerli ağabeyim Anıl Akbalık'a, azmiyle her şeyin üstesinden geleceğini gördüğüm ve ilham aldığım değerli Seda Aydın Akbalık'a, eğitim ve öğretim hayatımın idol kişisi annem, bir tanem Nurcan Bulcun Akbalık'a ve çalışması, azmiyle her zaman gurur duyup örnek aldığım canım babam Recep Akbalık'a şükranlarımı ve minnetlerimi sunarım. Bana inandığınız ve ne olursa olsun yanımda olduğunuz için çok şanslıyım.

Hayatımın yol arkadaşı, canım eşim Mert Korkmaz'a anlayışı, güveni, sabrı ve sonsuz sevgisi için çok teşekkür ederim.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

ÖZET

ISO 27001 BİLGİ GÜVENLİĞİ SİSTEMİ KONULU YAYINLARIN WOS VERİ TABANINA DAYALI BİBLİYOMETRİK ANALİZİ

Gözde AKBALIK KORKMAZ

Yüksek Lisans Tezi

Toplam Kalite Yönetimi Anabilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Okan BÜTÜNER

Ocak 2023, 87 Sayfa

Günümüz bilgi toplumunda en önemli konu bilgidir. Hayatın her alanında bilgi en değerli sermaye haline gelmiştir. Bu denli önemli hale gelen bilgi mutlaka iyi bir şekilde yönetilmeli, bundan daha önemlisi çok iyi bir şekilde korunmalıdır. Hem kötü niyet ile hem de kasıtsız olarak bilgi sistemleri çeşitli tehditler ile karşı karşıyadır. Bunları bertaraf etmenin yolu sistematik bir bilgi yönetim sistemi kurulmasıdır. Bu şekilde hem yönetim hem de koruma sağlanabilmektedir. Bunun öneminin farkında olan ülke ve kurumlar konu ile ilgili standartlar oluşturma yolunda çalışmalar yapmaktadırlar.

Çalışmamız konu ile ilgili çalışmaların önemli noktaları ortaya konulmuştur. Literatüre yapılan katkının yanında önemli bir kaynak olmasına gayret edilmiştir. Çalışmamız bu standartlardan ISO 27001 standardını ve bu yönde yapılan yayınları bibliyometrik olarak incelemeyi amaçlamaktadır.

Çalışmanın ilk bölümünde kavramlar incelenmiştir. İkinci bölümde literatür çalışmalarına yer verildikten sonra üçüncü bölümde bilgi güvenliği yönetim sistemleri hakkında bilgiler verilmiştir. Daha sonra bulgular yer almaktadır. Veriler Web of Science veri tabanından elde edilmiş, R ve R Studio programları ile Bibliometrix Biblioshiny paketleri ile analiz edilmiştir. Sonuçlarda en çok yayının yapıldığı yıllar, ülkeler, en etkin yazar, yayın, dergi ve ülkeler, en çok atıf alan yayın,

yazar, dergi ve ülkeler yer almaktadır. Ayrıca zaman içinde yapılan ülke, yazar ve dergi işbirlikleri gösterilmektedir. Çin ve ABD her analiz alanında öne çıkmaktadır. Ayrıca Uzak Doğu ülkelerinin kurumları etkili yayınlara ev sahipliği yapmıştır. Konunun işbirliklerine uygun olduğu görülmüştür. Temaların zaman içindeki evrimi de bulgular kısmında yer almaktadır. Çalışma sonuçların toparlanması ve önerilerin sunulması ile bitirilmiştir.

Anahtar Kelimeler: Bilgi, Bilgi yönetimi, Bilgi yönetim sistemi, BGYS, ISO 27001.

ABSTRACT

BIBLIOMETRIC ANALYSIS OF PUBLICATIONS ON ISO 27001 INFORMATION SECURITY SYSTEM BASED ON WOS DATABASE

Gözde AKBALIK KORKMAZ

DEPARTMENT OF TOTAL QUALITY MANAGEMENT

Master. Thesis

Supervisor: Assist. Prof. Dr. Okan BÜTÜNER

January, 2023, 87 Pages

In today's information society, the most important issue is information. Knowledge has become the most valuable capital in all areas of life. Information that has become so important must be managed well, and more importantly, it must be protected very well. Information systems are faced with various threats, both maliciously and unintentionally. The way to eliminate them is to establish a systematic information management system. In this way, both management and protection can be provided. Countries and institutions that are aware of the importance of this are working to establish standards on the subject.

In our study, the important points of the studies related to the subject have been revealed. It has been tried to be an important source besides the contribution to the literature. Our study aims to bibliometrically examine the ISO 27001 standard and the publications made in this direction.

In the first part of the study, the concepts were examined. After the literature studies are given in the second part, information about information security management systems is given in the third part. Then there are the findings. The data were obtained from the Web of Science database and analyzed with R and R Studio

programs and Bibliometrix Biblioshiny packages. The results include the years of the most publications, countries, the most active authors, publications, journals and countries, the most cited publications, authors, journals and countries. In addition, country, author and journal collaborations over time are shown. China and the USA stand out in every field of analysis. In addition, the institutions of the Far East countries have hosted influential publications. It has been seen that the subject is suitable for collaborations. The evolution of themes over time is also included in the findings section. The study was concluded by summing up the results and presenting the recommendations.

Key Words: Knowledge, Knowledge management, Knowledge management systems, ISMS, ISO 7001

BÖLÜM 1

1. GİRİŞ

1.1 Araştırmanın Problemi

Teknoloji bireysel, kurumsal ve toplumsal yönlerden hayata önemli katkılar sunmaktadır. Teknolojideki hızlı gelişme katlanarak artmaktadır. Bu da hayata yaptığı katkıların her yönden etkilerinin artması anlamına gelmektedir. Günümüzde internetin gelişimi ve hayatın bir parçası haline gelmesi ile birlikte kişiler hemen her işlerini internet ortamından halleder hale gelmiştir. We Are Social 2022 4.Çeyrek raporuna göre internet kullanıcı sayısı 5,07 milyar (dünya nüfusunun %63,5'u) olarak belirtilmektedir. Aynı raporda sosyal medya kullanıcısı sayısı 4,74 milyar (dünya nüfusunun %59'ü) ve mobil kullanıcı sayısı da 5,48 milyar (dünya nüfusunun %68,6'sı) olarak değerlendirmektedir (www.marketingturkiye.com.tr). Bilgiye ulaşmak kolaylaşırken kişisel kazanımlar da ortaya çıkmaktadır. Bunun yanında bu gelişmenin olumsuz yönleri de olmaktadır. Bunların en önemlisi bilgi güvenliği olarak karşımıza çıkmaktadır. Özellikle internet ortamında gerçekleşen bankacılık hizmetleri, sosyal medya paylaşımları, sohbetler, kişilerin en gizli bilgilerini bile sanal ortamda paylaşmaları güvenlik konusundaki zafiyetleri ve buna bağlı kaygıları ortaya çıkarmaktadır. ABD Savunma Bakanlığı ve NASA gibi çok iyi korunduğu düşünülen kurumların sistemlerine bile sızıntılar yapılarken bunu sadece 16 yaşındaki Jonathan James isimli hackerın yapabilmesi kişilerin kendilerini güvende hissetmemeleri durumunu gündeme getirmiştir (Sharma ve Purohit, 2017, 468). Uzun yıllardır internet dünyasının önemli aktörlerinden olan Yahoo'dan Ağustos 2013'de 3 milyar kullanıcı bilgisi çalınmıştır. Sadece 15 yıl sonra aynı şirketten 500 milyon kişi bilgisi sızdırılmıştır. Güvende hissetmeme duygusu bu olaylarla pekişmektedir. Siber suçların büyüklüğünün 2025'te 10,5 trilyon dolara ulaşması ve

dünyanın en büyük 3. ekonomisine denk hale geleceği düşünülmektedir (Yetkin, 2018, 53).

Bilgi güvenliğine konusunda sadece kişiler değil kurumlar da büyük önem vermektedir. Bu kaygılar ve düşünceler bilim insanlarını konu hakkında çalışmalar yapmaya itmektedir. Ancak gene de henüz konu hakkında yeterli sayı ve kapsamda çalışma yapılmamıştır. Gelişen teknoloji ve yazılımlar ile hem tehditler artmakta hem de önlemler geliştirilmektedir. Tüm bu gelişmeler çalışmalara konu edilmelidir.

Bu noktadan hareketle bu çalışmada ISO 27001 bilgi güvenliği yönetim sistemi hakkında yapılan yayınlar bibliyometrik yöntemler ile araştırılması araştırmanın problemini oluşturmaktadır. Bu problem doğrultusunda yayınlar incelenecek ve analizleri yapılacaktır.

1.2. Araştırmanın Amacı

Çalışmanın amacı ISO 27001 bilgi güvenliği yönetim sistemi ile ilgili yayınların bibliyometri yöntemi ile araştırılması ve analizi ile yapılan çalışmaları ortaya koymaktır. Konu ile ilgili yayınların sıklığı, gelişimi ve evrimi, yayın ortamları ve ülkeleri ile bilgiler analizler ile ortaya konulacaktır. Hem mevcut literatür ortaya konulacak hem de bu konuda çalışacak kişilere yol gösterici bir kaynak oluşturulacaktır.

1.3. Araştırmanın Önemi

Bilişim sektörü hem yaygın hem de önemli bir sektör olarak neredeyse herkesi ilgilendiren bir alan olmaktadır. Yurt dışında konu ile ilgili bibliyometrik çalışmalar yapılmış olmasına karşın ülkemizde ve dilimizde böyle bir yayın bulunamamıştır. Çalışma ile yapılmış çalışmaların önemli noktaları ortaya konulacaktır. Konu ile ilgili toplu bir bakış ortaya konulacaktır. Hem sektör çalışanları hem de araştırmacılar için kaynak olacaktır. Literatüre katkı sağlaması yanında özellikle etkili yayın, yazar ve kaynakların, konunun temalarının evriminin çalışma kapsamında incelenmesi yeni yayınlara yön verecektir. Tüm toplumu etkileyen bir konuda katkı sağlayacak olması çalışmanın önemini ortaya koymaktadır.

1.4. Araştırmanın Sayıltıları

Çalışma kapsamında ele alınacak yayınların en çok atıf alanlar arasından seçilmesinde en çok okunan ve en iyi araştırılmış yayınlar olduğu varsayılmıştır.

1.5. Araştırmanın Sınırlılıkları

Araştırma Web of Science veri tabanında yapılacaktır. Çalışmada kullanılacak veriler bu veritabanından "ISO 27011" ve "knowledge management system" anahtar kelimeleri ile elde edilebilecek veriler ile sınırlıdır. Ayrıca en bu yayınlar içinde en çok atıf alanlar araştırmaya dahil edilecektir.

1.6. Tanımlar

ISO 27001: Bilişim teknolojisi güvenlik teknikleri gereksinim standardıdır. Bilgi güvenliğinin sağlanması adına belirlenen standartları içermektedir.

KVKK: Kişisel verilerin korunması sağlamak ve gözetmek amacı ile kurulmuş düzenleyici ve denetleyici kurum.

Bilişim sistemi: Genel olarak işletmelerde karar verme ve kontrolü sağlama adına ihtiyaç duyulan bilgiyi sağlayan sistem olarak tanımlanmaktadır. Bu bilgilerin toplanması, işlenmesi, depolanması ve dağıtılması bu sistem sayesinde gerçekleştirilmektedir.

BÖLÜM 2

2. BİLGİ, BİLGİ GÜVENLİĞİ VE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Bilgi güvenliği, üzerinde her geçen gün daha fazla durulan bir olgu haline gelmiş olup bu durum literatürde sürekli olarak artış gösteren konuya ilişkin çalışma sayısından da anlaşılmaktadır. Bu doğrultuda literatürde yer alan farklı çalışmalarda konunun hangi yönleri ile ele alındığına dair inceleme yapmakta fayda vardır.

Bu çalışmalardan birinde Yılmaz (2015), çalışmasında bilgi güvenliğinin önemine vurgu yapmaktadır. Çalışmada özellikle kurumların yaşadığı bilgi güvenliğini tehditleri ile buna yönelik alınması gereken tehditler incelenmektedir. TS ISO/IEC 27001 Standardı göz önüne alınarak Bilgi Güvenliği Yönetim Sisteminin (BGYS) kurulumu ve süreç tabanlı bir model ile risk analizi bilgileri yer almaktadır. Vardığı sonuca göre çalışanların bilgi güvenliğinin önemi konusunda farkındalıklarının artırılması ve daha fazla bilinçli olmaları en etkili ve en sonuç verici yöntemdir. Bunun yolu da teknolojik yatırımlarla birlikte hizmet içi eğitimlerin daha fazla yapılması olmaktadır. Bu şekilde risklerin azaltılabileceği sonucuna varılmıştır (Yılmaz, 2015: 45).

Konuya ilişkin bir diğer çalışmada Evrin ve Demirer (2011), ISO 27001'i bilgi güvenliği konusunu kurumsal açıdan incelemişlerdir. Hayatın her aşaması ve noktasında teknoloji ve iletişim olanaklarının kullanılması ile bilgi güvenliği konusu her zaman önem arz edecektir. Bundan dolayı teknoloji ve iletişim olanaklarını amacına uygun ve güvenli bir şekilde kullanmak gerekmektedir. Özellikle kurumlar herhangi bir tehdit ile karşı karşıya kalmamak için bilgi güvenliğini bir felsefe olarak kabul ederek, kurumsal bir kültür oluşturmak durumundadırlar. Araştırmacılar BGYS süreçlerinin kurumsal yapıda bir kültür haline getirilmesinin gerekli olduğu sonucuna varmışlardır (Evrin ve Demirer, 2011: 8).

Gencer (2015) araştırmasında bilişim kaynaklarının güvenlik zafiyetlerini ortaya koymaktadır. Alınan önlemlerin sorunları nasıl azaltacağı araştırılmıştır.

Sistemdeki en zayıf halkanın insan olduğu tespiti yapılan çalışmada sistemdeki insan sayısının azalmasının güvenliğe olumlu katkı sunacağı belirtilmektedir. Otomasyonun artması ve yapay zeka ile daha az hata olabileceği çalışmanın sonuçları arasında yer almaktadır (Gencer, 2015: 70).

Bingöl (2010) çalışmasında BGYS sistemlerinin açık kaynak kodları kullanarak oluşturulmasının maliyet düşürücü etkisi incelenmektedir. Bu şekilde işletmeler küçük değişikliklerle sistemleri kendilerine adapte edebilmektedirler. Sonuçta elde edilen sistemin bir başka faydasının da dışa bağımlılığın azaltılması olarak ortaya çıkmaktadır (Bingöl, 2010: 7).

Erdoğan (2020) ise çalışmasında standarda uygun bir bilgi yönetim sistemi oluşturulmasını ve bu sistemin sivil havacılık sektöründe uygulanmasını ele almıştır. Kurum çalışanları ile mülakatlar yapılmış, bilgi güvenliği yönetim sisteminin oluşturulmasında önem arz eden konular tespit edilmiştir.

2.1. Bilgi Kavramı

Tek kesinliğin belirsizlik olduğu bir ekonomide, kalıcı rekabet avantajının tek kesin kaynağı bilgidir. Piyasalar değiştiğinde, teknolojiler çoğalır, rakipler çoğalır ve ürünler neredeyse bir gecede eskiyebilir. Başarılı şirketler sürekli olarak yeni bilgi yaratan şirketlerdir. Bilgiyi geniş çapta yaymak için organizasyonlar teknolojiler ve ürünler geliştirirler. Bilgi yaratan şirketlerin en önemli işi sürekli yeniliktir (Nonaka, 2000: 96).

2.1.1. Bilgi Güvenliği Kavramı

İnsan düşünebilen ve düşüncelerine yorum katabilen bir canlıdır. Yapılan gözlemlerle olaylar, durumlar anlamlandırılmaktadır. Bunlar sonucunda bilgi ortaya çıkmaktadır. Türk Dil Kurumu sözlüğünde bilgi "insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat" ya da "insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf" şeklinde tanımlamıştır (TDK, 2019).

Günümüzde bilgi artık korunması gereken bir değer haline gelmiştir. Drucker (1994)'a göre "Bilgi kavramının anlamı son 250 yılda değişmeye başlamış, bu durum

toplumu ve ekonomiyi değiştirmiştir". Drucker, aynı eserinde, "enformasyon kapitalizmi" kavramını ortaya atmaktadır. Buna göre bilgi sahibi olmak bir üstünlüktür. Dolayısıyla bilgi korunmalıdır. Bunun için de etkin bir bilgi yönetim sistemine ihtiyaç vardır (Drucker, 1994: 46). Bilgi pek çok şekilde karşımıza çıkabilmektedir. Yazılı ortamlar, elektronik ortamlar gibi yerlerde bilgi görülebilirken filmlerde, masalarımızdaki notlarda, sohbetlerimizde, postalarımızda bilgi hep ulaşılabilir haldedir. Yani bir tehdit altındadır. Bu tehditler içerden, dışarıdan, art niyetsiz ya da kötü amaçlı olabilir (Doğantümur, 2009: 6).

Bilgiye erişimin kolaylaşınca bununla birlikte sorunlar da ortaya çıkmaktadır. Bilginin sadece "bilmesi gereken" kişilere ulaşması, yetkisiz kişilerden korunması gerekmektedir. Bu da etkili bir bilgi güvenliği sistemi ile sağlanabilir (Bingöl: 2010: 6).

Bilgi güvenliği tanımında çeşitli boyutlar yer almaktadır. Bunlar bilgiye erişimin sürekli olabilmesi, tam bir gizliliğe sahip olunması, bozulmaması, değişikliğe uğramaması, bütünlüğünün korunması, başkalarının erişimine kapalı olması ve güvenle iletilebilmesi olarak sıralanabilmektedir (Vural ve Sağıroğlu, 2008: 509).

Bireysel bilgi güvenliğinden daha önemlisi kurumsal bilgi güvenliğidir. Kişiler bilgi sistemleri üzerinden mal/hizmet satın alırken veya mal/hizmet sunarken kurumsal bilgi unsurlarını direkt ya da indirekt yöntemler ile kullanmaktadır. İnternet alışverişleri, internet bankacılığı gibi kullanımlarda kişisel veriler kurumlara iletilmektedir. Kurumlar da bu bilgiyi korumak ile yükümlüdür. Bir müşterinin iletişi bilgileri, kredi kartı, banka hesabı bilgileri güvenli bir şekilde toplanmalı ve korunmalıdır. Bu bilgilerin üçüncü kişi ve taraflarca ele geçirilmesi telafisi zor ya da imkansız zararlar verebilmektedir. Kurumun itibar kaybı da çok önemsenmesi gereken bir durumdur (Bingöl, 2010: 6).

Bilgi güvenliğinin temelinde üç boyut yer almaktadır. Gizlilik, bütünlük ve erişilebilirlik bu üç boyutu oluşturmaktadır. Gizlilik bilginin sadece erişim yetkisi olan kişilerce erişilebilir olmasıdır. Bütünlük ise veriye üçüncü kişilerce ekleme yapılmaması, silinen bir kısmının olmaması, değiştirilmemesi ve bozulmamasını

ifade etmektedir. Bilginin her an kullanılabilir olması ise erişilebilirliktir (Aktaş 2020: 7).

Bu temel bileşenleri sağlamak genellikle küçük ölçekli firmalarda çok zor olmamaktadır. Ancak kurum boyutu büyüdükçe, çalışan, şube, ofis, kullanılan cihaz sayısı arttıkça bilgi güvenliğinin sağlanmasını zorlaşmaktadır. Bilgi güvenliği sadece bilgi güvenliği çalışanlarının sorumluluğunda değil, herkesin sorumluğunda olmalıdır. Bilgi güvenliğini bilgi işlem çalışanlarının sorumluğuna bırakılacak teknik bir konu olarak görmek doğru bir yaklaşım değildir. Bu konuda tüm çalışanların belirli sorumlulukları olmalıdır (Erdoğan, 2020: 2).

Bilgi güvenliğindeki en önemli etkenlerin başında insan kaynağı gelmektedir. Bilgi güvenliğini sadece dış kaynaklı tehditler altında değildir. İç kaynaklı tehditler de mevcuttur. Yanlış işlem ve davranışlar sadece hata olabileceği gibi kötü niyet de içerebilmektedir (Thomson, Solms & Louw, 2006: 7). 2018 yılında yapılan bir çalışmada siber saldırıların %46'sı kurum personellerinin hatalarınından kaynaklanmaktadır. Bu çalışmayı ünlü bir siber güvenlik araştırmaları ve uygulamaları geliştirici firmanın yapmış olması sonucunun güvenilmesi gerektirdiğini düşündürebilir (Erdoğan, 2020: 2).

Bilgi güvenliği sadece teknolojik önlemlerle sağlanamamaktadır. Bilgi güvenliği, süreçlerin bir parçası olmalıdır. Bir kültür haline getirilmelidir. Kurumlar hem çalışan bazında hem de kurumsal boyutta bir güvenlik politikası oluşturmalıdır. Bu yazılı bir halde çalışanlara, paydaşlara ve iş ortaklarına aktarılmalıdır. Sorumluluklar belirlenmelidir (Kahraman, 2006: 19).

2.1.2. Bilgi Güvenliğini Tehdit Eden Unsurlar

Bilgi güvenlik tehdidi, kişisel, kurumsal ya da kurumun bilgi kaynaklarına zarar verebilecek potansiyele sahip bir eylem olabilir. Bu tehdit kötü niyete bağlı kasıtlı olabileceği gibi kasıtsız hata veya kaza sonucu da oluşabilmektedir (Raymond ve Schell, 2004: 208).

Tehdit türüne bağlı olarak küçük zararlar olabileceği gibi tüm bilgi sisteminin kaybına varabilecek kayıplar yaşanabilmektedir. Kimi zaman bilgilerin gizliliği kimi

zaman da erişilebilirliği zarar görebilmektedir. Kurumlar bilgi güvenliği tehditlerinin ne olduğunu saptayarak, tümüyle önlenme ya da en azından etkilerini minimize etme yönünde faaliyetler içindedirler.

Öncelikle yapılması gereken tehditleri sınıflandırmak olmalıdır. Tehditlerin kaynakları ve etkileri farklılıklar gösterebilir. Tehdidin kaynağı içerden, dışarıdan ya da hem içeriden hem de dışarıdan olabilir. Önce tehdidi kaynağının başlangıç yerine göre sınıflandırmak gerekmektedir. Kaynak başlangıcı neresi olursa olsun hepsinde üç etken vardır. Bunlar, insan faktörü, çevresel etkenler ve teknolojik etkenlerdir (Jouini, 2014: 490).

Bilgi güvenliğini tehdit eden unsurlar öncelikle iki alt başlıkta ele alınmaktadır. Bu başlıklar ve kapsamları şu şekildedir (Erdoğan, 2020: 6):

- İç Kaynaklı Tehditler: Burada tehdidi oluşturan bilgi sistemine erişim yetkisine sahip bir kullanıcı olmaktadır. Yapılan bir hata ile ya da yetkisini kötüye kullanarak sistemde zafiyet oluşturmaktadır. Ülkemizde önemli bir bankanın bir çalışanı kötü niyet ile müşteri verilerini sızdırmıştır. Bu nedenle, finansal ve belki de ondan daha önemli olarak itibar yönünden kayıpların olmaması için iç kaynaklı olası tehditlere karşı koruyucu önlemler alınmalıdır.
- Dış Kaynaklı Tehditler: Bu durumda tehdidi kurum yerleşim yeri dışında bulunan art niyetli kişiler, gruplar ya da afetler gibi zarar verebilecek doğa olayları olarak gösterilebilir. Ülkemizde önemli iletişim firmalarından biri sel felaketi yüzünden ciddi bir zarar yaşamıştır. Siber saldırılar da bu başlık altında yer almaktadır ve büyük tehlike arz etmektedir.

Bilgi güvenliğini tehdit eden etkenler de kendi içlerinde üç alt başlığa ayrılmaktadır. Bu başlıklar ve kapsamları da şu şekildedir (Erdoğan, 2020: 7):

- İnsan Etkeni: Burada iki grup oluşmaktadır. İstem dışı yapılan hatalar ve oluşan kazalar ile art niyet ile yapılan insan kaynaklı olaylar bu grupları oluşturmaktadır.

- Çevresel Etkenler: Bunları önceden bilebilmek pek mümkün değildir. Deprem, sel, yangın gibi doğal afetler bu başlık altında sayılabilir. Bunlarla ilgili gerekli önlemler alınmalıdır. Hem bilgi kaynaklarının yerleşimi ve saklanması açısından dikkat gerekirken düzenli ve yeterli sıklıkta yedeklemeler yapılmalıdır.
- Teknolojik Etkenler: Kurumsal yapılarda günümüzde iş süreçleri içinde teknolojik araçlar, gereçler ve yazılımlar vazgeçilemez bir hale gelmiştir. Bilgi sistemleri ile yazılımlar ile kullanılıyor olması tehditleri de beraberinde getirmektedir. Art niyetli kişiler sistemlere zarar verebilmektedir. Silme ya da değiştirme işlemleri ve erişilebilirliğe engel olma durumları oluşabilmektedir. Hele ki saldırganlar fark edilemezse zararlar uzun süreli ve kalıcı olabilmektedir. Sadece bir yazılım ile saldırganlık faaliyetleri gerçekleştirilebilir (Shephard, 2002: 126). Bu şekilde çalışan yazılımlara örnek olarak truva atı (trojan horse) denilen programlar, görünürde zararsız ve sadece rutin işleri yaparken aslında arka planda tamamen gizlice zarar verici faaliyetler gerçekleştiren programlardır. Bu tip zararlı yazılımlar özellikle ağ ortamlarında hızlı bir şekilde yayılma özelliğine de sahiptir.

2.1.3. Bilgi Güvenliğinin İhlali

Var olan bilgi güvenliği politikaları ve önlemlerine rağmen veya bir takım aksaklıklar sonucu bilgi güvenliğinin zarar görmesi durumları bilgi güvenliği ihlali olarak tanımlanabilir Yönetim sisteminin tamamı ya da bir bölümü ihlaller sonucunda sekteye uğrayabilir. Hızlıca yapılması gereken meydana gelen olayı saptayabilmek, raporlamak, değerlendirmek ve mevcut prosedürler doğrultusunda tepki verebilmektir. Ayrıca bu durum ileride yapılacak eğitimlere konu edilmelidir (Akay, 2014: 17).

Hiçbir zaman tamamen güvenli ya da hiçbir riskin olmadığı bir durum düşünmek gerçekçi olmayacaktır. Çok güvenilen bir bilgi güvenliği sistemi ile de bu sonuç yaratılamaz. Güvenliği kurum ya da toplum için sürekli kılabilmek, riskleri en

aza indirebilmek ve bu riskleri de kontrol altında tutabilmek gerçekçi bir hadaf olacaktır (Tipton ve Krause, 2008: 85).

Sağlık Bakanlığı bilgi güvenliği ihlal olayları prosedüründe aşağıdaki ihlaller bilgi güvenliği ihlali olayı olarak tanımlanmıştır (Erdoğan, 2020: 8).

- *Var olan bilgi kaynaklarının hırsızlığa uğraması, zayi olması*
- *Bilgi güvenlik unsurlarının ihlalleri (bütünlük, gizlik, erişilebilirlik)*
- *Personel hata ve ihmalleri ile oluşan ihlaller*
- *Genel Müdürlük ve Bakanlık tarafından yayımlanmış Bilgi Güvenliği Yönergesi, Politikalar ve Prosedürlere göre iş ve işlemlerin yürütülmemesi*
- *Fiziksel Güvenlik düzenlemelerinin ihlali*
- *Sistemlerde kontrol dışı değişiklikler*
- *Kullanılan yazılımlarda veya donanımlarda meydana gelen arızaları*
- *Erişim ihlalleri (yetkisiz erişim), yetkisiz bilgi kullanımına izin veren uygun olmayan erişim denetimleri*
- *Siber saldırılar (Virüs, izinsiz giriş, Truva atı, casus yazılım vb. bulgular için, sistem sunucu servis problemleri için)*
- *Gizli bilginin yetkisiz kişilerce ifşa edilmesi*

İhlal durumu oluştuğunda olay incelenmeli, temel sebep tespit edilmeli ve düzeltici faaliyeteler başlatılmalıdır. Tüm bu süreç ayrıca belgelendirilip kayıt altına alınmalıdır. Bakanlık aynı belgede ihlal olayı gerçekleştirildiğinde yapılması gerekenleri şu şekilde listelemiştir (bilgiguvenligi,saglik,gov,tr):

- İhlal durumu gerekli formların doldurulması ile raporlanır.
- Bildirim ilgili mail adreslerine de eş zamanlı olarak yapılır.
- BGYS Birim Sorumlusu durumu tespit eder, analizini yapar, ihlal var ise yayılmaması yönünde faaliyetleri gerçekleştirir. Gerekir ise hukuk ve güvenlik birimleri haberdar edilir.
- Çözüm için eposta ya da telefon ile bildirim yapılır.
- Çözüm için harekete geçilir.

- BGYS ekibi tarafından izlenir ve raporlanır.
- Farkındalık için kurum içi bilgilendirmeler yapılır.

2.2. Bilgi Güvenlik Yönetim Sisteminin Tanımı ve Tarihçesi

Siber saldırılar ve bu yönde oluşan riskler son yıllarda, hem kurumlar hem de toplum açısından önemli bir tehdit oluşturmaktadır. Dünya üzerinde hem mobil teknolojilerin, hem sosyal ağların hem de bulut hizmetlerinin yaygınlaşması sistemlerde zafiyetlerin artmasına neden olmuştur. Bilgi güvenliği pek çok kurum tarafından önemli bir iş riski olarak görülmektedir. Her türlü güvenlik önlemine rağmen halen ciddi kayıplar oluşabilmektedir.

Günümüz örgütlerinde bilgiye verilen önem, transfer ve replikasyonun önünde engellerin olduğu varsayımına dayanmaktadır. Bilgi kuruma stratejik bir önem verir. Birçok kuruluş paylaşımlarını kolaylaştırmak için özel olarak tasarlanmış bilgi sistemleri geliştirmek ve bilginin entegrasyonu sağlayan sistemler geliştirmektedir. Bu tür sistemlere Bilgi Yönetim Sistemi (BYS) denir (Alavi ve Lediner, 1999: 2).

Yetkisi olmayan kişilerin veya kurumların yetkisi olmadığı bilgilere ulaşması gizlilik ihlali oluşturmaktadır. Verilerin bütünlüğü ve sistem bütünlüğü önem arz etmektedir. Veri bütünlüğü, verilerin yetkisiz kişilerce değiştirilmediği ya da yok edilmediği anlamına gelmektedir. Sistem bütünlüğü ise, bir sistemin amaçlanan işlevini, kötü niyetle ya da kazayla yetkisiz müdahalelerden arındırılmış, zarar görmemiş bir şekilde yerine getirmesidir. Uygunluk ise, bir talep anında bilginin hem erişilebilir hem de kullanılabilir olma özelliğidir (Ateş, 2016: 1).

Hayata geçirilmiş pek çok ulusal ve uluslararası BGYS bulunmaktadır. Çok sayıda kişi tarafından bilinen bazı BGYS'leri aşağıdaki şekilde özetlenebilir. (Ateş, 2016: 3).

- Avusturya BT Güvenlik El Kitabı: Avusturya Federal İdari İşleri tarafından 1998 yılında yayınlanan bu el kitabı iki bölümden oluşmaktadır. İlk bölümde yer alan konular BT güvenlik yönetimi sürecinin tanımlanması, risk analizi, güvenlik kavramlarının tanımı, güvenlik planı uygulamaları olarak sıralanabilir. Diğer bölümde ise 230 adet temel güvenlik önlemi yer almaktadır. Yayınlandığında özellikle kamu kurumlarına yönelik olan bu el kitabı günümüzde tüm kurumlara yön vermektedir.
- Hollanda A ve K analizi: 1996'da Hollanda hükümeti A ve K Analizini yayınlamıştır. Yayınlandığı güncen bugüne herhangi bir güncelleme yapılmamıştır. Bu analiz de hem kamu kurumlarınca hem de özel sektörce kullanılmaktadır.
- Bilgi güvenliği değerlendirme ve izleme yöntemi (ISAMM): Bilgi güvenlik yönetim sistemlerini desteklemeyi amaçlayan nitel yönteme

dayalı bir risk analizi yöntemidir. 2002 yılında Belçika'da Telindus Grup tarafından yayınlanmıştır. Bu yöntem ile kurumlara sisteme yönelik varlık ve tehditlerin tanımlanması, varsa tanımlanan güvenlik açıklıklarına göre tehditlerin etkilerinin ve olası zararlarının ölçülmesi, risklerin kabul edilebilirliğinin değerlendirilmesi, kabul edilemez bir risk ise buna yönelik hangi önlemlerin alınacağının kararlaştırılması ve risk oluştuğunda yapılması gereken iletişim sürecinin grafik ve raporlardan yararlanılarak desteklenmesi konularında yol göstermektedir.

- Bilgi teknolojileri temel koruma kılavuzu (IT-Grundschutz): 1993 yılında Almanya Bilgi Güvenliği Bakanlığı tarafından yayınlanmıştır. Kurumlara kendi BGYS'lerini oluşturmaları için tasarlanmış bir yöntemdir. En son 2005 yılında güncelleme yapılan yöntem Almanya için merkezi BT güvenlik hizmeti sağlayıcısıdır. Kurumlara BGYS için genel bir çerçeve sunmaktadır. Detaylı teknik öneriler içermektedir.
- Operasyonel olarak kritik tehdit, varlık ve güvenlik açığı değerlendirmesi (OCTAVE): Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü'nde geliştirilen ileri hesaplama içeren ağır riskli bir risk metodolojisidir. Bu yöntem öncelikle iç tehditlere odaklanmaktadır. Büyük kurum ve kuruluşlar için OCTAVE ve küçük ölçekli kurum ve kuruluşlar için ise OCTAVE-S olmak üzere iki versiyonu mevcuttur. Güvenlik risk yönetimi alanında risk temelli bir stratejik değerlendirme ve planlama tekniğidir. Sistemdeki değişik düzeylerdeki bilgilerden yararlanılarak kritik varlıklar ve tehditler belirlenir. Olası açıklıklar kurumsal ve teknolojik olarak belirlenir.
- Ulusal standartlar ve teknoloji enstitüsü - Özel yayın (NIST-SP 800-30): SP 800-30, 2002 yılında ABD'de National Institute of Standards and Technology (NIST) tarafından yayınlanmıştır. SP 800-30, risk yönetime genel bir bakış ile BT'yi desteklemektedir. Risk denetimi için dokuz temel adım vardır. Bu adımlar, sistemin tanımlanması, tehditlerin tanımlanması, açıklıkların tanımlanması, kontrol analizleri, olasılıkların belirlenmesi, etki analizi, riske karar verilmesi, kontrol önerileri ve raporlama şeklindedir. Riski azaltılması seçenek ve stratejileri içermektedir.
- CCTA risk analizi ve yönetimi metodu (CRAMM): Central Communication and Telecommunication Agency (İngiltere Merkez Bilgi İşlem ve Telekomünikasyon Ajansı, CCTA) tarafından geliştirilen nitel bir güvenlik risk yönetimi yaklaşımıdır.
- Harmonize risk analizi yöntemi (MEHARI): MEthod for Harmonized Analysis of RIsk (Harmonize Risk Analizi Yöntemi, MEHARİ) Risk analizi ve risk yönetimini içeren Fransız Bilgi Güvenliği Uzmanları Birliği tarafından geliştirilen bir yöntemdir. Beş aşamada risk analizi yapılmaktadır. Bağlam kuruluşu, destek analizi ve varlık sınıflaması,

risk tanımlaması, risk analizi ve Risk denetlemesi. Risk yönetimi ise dört aşamada tamamlanır. Bu aşamalar risk değerlendirmesi, risk çözümü, risk kabulü ve risk iletişimi şeklindedir.

2.3. ISO 27001 Bilgi Güvenliği Yönetim Sistemi

2.3.1. ISO 27001 Tanımı

Kurumların yaşadıkları bilgi güvenliği tehditleri ile başa çıkabilmeleri için süreç yönetim standartları oluşturmaya yönelik olarak 1995 yılında İngiliz Standartları Enstitüsü (British Standards Institutition-BSI) tarafından BS-7799 standardının ilk bölümü olan BS7799-1 yayınlanmıştır. 1999 yılında ise ikinci bölümü olan BS7799-2, İngiliz Standardı olarak yayımlanmıştır. 2000 yılında ISO küçük bir takım düzenleme ve uyumlulaştırma çalışmaları yapılarak ISO/IEC–17799 adıyla uluslararası bir standardı paylaşmıştır. Bu arada 2002 yılında BSI'nin yapmış olduğu çalışma sonunda BS7799-2 revize edilerek bir kez daha yayımlanmıştır. ISO 2005 yılında ISO/IEC–17799 standardında değişiklikler yaparak ISO/IEC–17799:2005 versiyonunu yayımlanmıştır. Aynı yılın sonlarında BSI BS7799-2 standardında bir takım ilaveler yapınca ISO kendi standardında bu konulara da yer vermiş ve ISO/IEC:27001 olarak bilinen uluslararası standart ortaya çıkmıştır (Bingöl, 2010: 9).

Bilgi güvenliği için oluşturulan ilk standart BS-7799 olmuştur. İki bölüm halindedir. Birinci bölümünde bilişim güvenliği ile ilgili çalışma kuralları (Information Technology – Code of Practice for Information Security Management) mevcuttur. Bu bölümde 10 alt bölüm vardır. 36 kontrol ve 127 alt kontrol maddesi bulunmaktadır. Standardın diğer bölümünde ise bilgi güvenliği yönetimi sisteminin planlanması, kurulması ve sürdürülebilirliği için gereken süreçler anlatılmaktadır. Ayrıca bu bölümde belgelendirme ve sertifikasyon konuları ele alınmaktadır. Standart ile sadece kurum prosedürleri oluşturulmamakta, beraberinde paydaşlar ve ortaklar da sürece dahil edilebilmektedir (Erdoğan, 2020: 26).

ISO/IEC:27001:2005 standardı Uluslararası Standartlar Organizasyonu (International Organization for Standardization-ISO) ve Uluslararası Elektroteknik Komisyonu (The International Electrotechnical Organization-IEC) tarafından BS-

7799 standardının uluslararası bir standart haline getirilmiş halidir. Halen teknik çalışma grupları ile geliştirmeler devam etmektedir. Bu çalışmaların ele alındığı SC27 komisyonu Bilişim Teknolojileri Güvenlik Teknikleri Alt Komisyonudur. Bu alt komisyon JTC-1 Bilişim Teknolojileri Komitesine bağlıdır ve 41 ülkenin katılımıyla oluşturulmuştur. Bu komisyonun sorumluluklarından bazıları aşağıda belirtilmiştir. Buna Göre;

- Bilgi teknolojileri sistemlerine dair ihtiyaçların ve güvenlik hizmetlerinin tanımlanması
- Güvenliğe yönelik teknik ve mekanizmalarının geliştirilmesi
- Güvenlik kılavuzlarının oluşturulması
- Yönetim destek dokümanlarının ve standartların geliştirilmesidir.

SC27 alt komisyonu içinde 5 ayrı çalışma grubu bulunmaktadır. Çalışma Grubu–1 (JTC 1/SC 27/WG 1) çalışma alanı BGYS standartları ile ilgili çalışmalardır. ISO/IEC 17779 standardı 2005 yılında yapılan bir düzenleme ile yerini 27000 serisini bilgi güvenliği ile ilgili standartlara bırakmıştır. 2013 yılında bir güncelleme daha yapılmıştır. En son olarak 2022 yılında yeni bir versiyon yayınlanmıştır (ISO, 2022: 2). Tablo 1'de ISO 27000 serisinin hazırlanan standartları gösterilmektedir.

Tablo 1. Yayımlanan ISO 27000 Serisi

Standart Adı	**Açıklaması**
ISO / IEC 27007 – 27059	Bilgi güvenliği ile ilgili standartlar için ayrılmış aralık
ISO / IEC 27000	BGYS standartları için genel sözlük (İlk Yayımlanma Tarihi: 2009)
ISO / IEC 27001	BGYS için kurulum, uygulama, kontrol ve geliştirme ile ilgili standart (İlk Yayımlanma Tarihi: 2005)
ISO / IEC 27002	BGYS uygulama ilkeleri ve tavsiyeleri (İlk Yayımlanma Tarihi: 2007)
ISO / IEC 27003	BGYS uygulama rehberi (İlk Yayımlanma Tarihi: (2010)
ISO / IEC 27004	BGYS ölçüm ve metrikleri (İlk Yayımlanma Tarihi: 2009)
ISO / IEC 27005	BGYS risk yönetim sistemi (İlk Yayımlanma Tarihi: 2008)
ISO / IEC 27006	BGYS belge kaydı ve belgelendirme süreçleri kılavuzu (İlk Yayımlanma Tarihi: 2007)
ISO / IEC 27011	Telekomünikasyon endüstrisi için BGYS rehberi

Kaynak: Vural, 2007.

Tablo 1'de yer alan halen yürürlükte olan standartlardır. Tablo 2'de ise önümüzdeki dönemde yayınlanması planlanan ve üzerinde çalışmaların sürdüğü ISO 27000 serisi yer almaktadır.

Tablo 2. Planlanan ISO 27000 Serisi

Standart Adı	Açıklaması
ISO / IEC 27007 – 27008	BGYS izleme rehberi
ISO / IEC 27000	BGYS standartları için genel sözlük
ISO / IEC 27013	ISO / IEC 20000-1 ve ISO / IEC 27000 standartlarını birleşik olarak uygulama rehberi
ISO / IEC 27014	Bilgi güvenliği yönetişimi çerçevesi
ISO / IEC 27015	Finans ve Sigorta sektörlerinde BGYS uygulama rehberi
ISO / IEC 27031	BGYS iş güvenliği standart rehberi
ISO / IEC 27032	İnternet için siber güvenlik rehberi
ISO / IEC 27033	ISO / IEC 18028: 2006 temel alınarak bilişim sistemleri ağ güvenliği rehberi
ISO / IEC 27034	Uygulama güvenliği rehberi

Kaynak: Vural, 2007

Ülkemizde bilgi güvenliği ile ilgili standartlaştırma ve belgelendirme faaliyetleri Türk Standartları Enstitüsü tarafından yapılmaktadır. Bu doğrultuda ISO/IEC 17799:2000 standardı tercüme edilerek 2002 yılında TS ISO/IEC 17799 Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi için Uygulama Prensipleri Türk standardı yayınlanmıştır. Bununla birlikte 2005 yılında BS-7799-2 de tercüme edilmiş ve "Bilgi güvenliği yönetim sistemleri–Özellikler ve kullanım kılavuzu" ismiyle TS 17799–2 standardı olarak yürürlüğe girmiştir. Bu standart 2006'da TS ISO/IEC 27001:2006 "Bilgi teknolojisi–Güvenlik teknikleri-Bilgi güvenliği yönetim sistemleri ve Gereksinimler" standardının yayınlanması ile kaldırılmıştır (Erdoğan, 2020: 28).

2.3.2. ISO 27001 Standartları

ISO 27001, düzenleyici makamlarca kabul görmüş bir standarttır. Kurumların nasıl bilgi güvenliği yönetim süreçlerini oluşturmaları gerektiği yönünde yol göstericidir. Riskleri en aza indirme yönünde yapılması gereken faaliyetler standart içinde yer almaktadır (Korucu, 2021: 65).

ISO 27001 ile bilgi varlıkları konusunda farkındalık sağlanmaktadır. Kurum güvenirliğine katkı sağlamasının yanında çalışan motivasyonunu arttırmaktadır.

Belgelendirilmesi ile kurumun kanun ve sertifikasyon gerekliliklerine uyduğunu göstererek itibar artışını beraberinde getirmektedir. Tüm bunlar kurumun rekabetçi yapısını güçlendirmektedir. Standardın ana maddeleri şu şekilde sıralanabilir (Doğantimur, 2009: 15):

- Güvenlik politikası: Yönetime destek ve sürdürülebilirlik alanlarında bir politika uygulanmaktadır.
- Bilgi güvenliği organizasyonu: Temel uygulama ekibi bu başlık altında oluşturulur. Bu aşamada kurumun imkanları ve ihtiyaçları göz önünde bulundurulur. Ekip içinde tecrübe ve yetenek sahibi bilgi işlem birim yöneticileri arasından seçilen sistem, ağ ve yazılım ekip liderleri ile bunların bağlı olduğu bir teknik yönetici bulunur.
- Varlık yönetimi: Bu aşamada her türlü bilgi değeri taşıyan varlıklar bir envanter şeklinde listelenir.
- İnsan kaynakları güvenliği: Kökeninde insan kaynaklı art niyet ve kazaları engellemeye yönelik tedbirlerden ibarettir.
- Fiziksel ve çevresel güvenlik: Önemli noktalara erişim yetkisi olmayanların girişini engellemek üzerinde alınan tedbirlerdir.
- Haberleşme ve iletişim yöntemi: Kurumda ağ üzerinden yapılan iletişimin güvenlik unsurları ile bütünlüğünün ve doğruluğunun korunduğu bilgi kaynaklarının düzenlemesini içerir.
- Erişim kontrolü: Erişimin kısıtlanması ve yetkilendirmeyi içerir.
- Bilgi sistemleri edinimi, geliştirme ve bakımı: Sistemlerde bütünlük ve güvenlik unsurlarının kurulması veya geliştirilmesini, daha sonraki geliştirme süreçlerinde ise yine bu unsurların artırılarak devamının sağlanmasını içerir.
- Bilgi güvenliği ihlal olayı yönetimi: İhlal durumlarındaki davranış ve tepkileri içerir.
- İş sürekliliği yönetimi: Felaket kurtarma istasyonu oluşumu en önemli örneklerdendir.
- Uyum: Yasal düzenlemelere uygun bir sistem kurulumu ve işletimi olmalıdır

2013 versiyonunda 114 olan kontrollerin sayısı 2022'de 93'e indirilmiştir. Bu versiyon ile birlikte kontroller 14 maddede değil 4 ana başlık halinde gruplandırılmıştır (ISO, 2022: 11-18). Bunlar;

- İnsanlar (8 kontrol)
- Organizasyonel (37 kontrol)
- Teknolojik (34 kontrol)
- Fiziksel (14 kontrol)

2.3.3. ISO 27001'in Önemi

Bu standart, bir kurum/kuruluşta bilgi güvenliği yönetim sistemi için elzem olan kurulum, uygulama, sürdürülmesi ve sürekli iyileştirilmesi için mecburiyetleri belirlemek amacıyla geliştirilmiştir. Kurum içinden ya da dışından art niyetli ve doğru olmayan kullanımlara karşı bilginin muhafaza edilmesi gerekliliklerini tanımlar. TSE tarafından yayınlanma amacı "Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek amacıyla geliştirilmiştir." şeklinde belirtilmiştir (Ersoy, 2012: 14-15). Sektör ya da işletme büyüklüğü ayırt etmeksizin (ticari işletmeler, devlet kurumları, kar amacı gütmeyen kuruluşlar, mikro işletmeler, çokuluslu şirketler, perakendecilik, bankacılık, savunma, sağlık, eğitim kurumları vb.) tüm kuruluşların yararlanabilmesi üzerine geliştirilmiştir. (Gündoğan, 2016: 20). ISO 27001 ile sadece bilişim güvenliği sağlanmamış, kağıt üzerindeki hatta sohbet anındaki bilgiler bile korunabilir hale gelmektedir (Çetinkaya, 2008: 512).

Bu belge sahip olan kuruma bir takım ayrıcalıklar sağlamaktadır. Bunları şu şekilde sıralayabiliriz (Çubukçu, 2018: 21):

- Tüm dünyada geçerli bir yönetim sistemini kullandığınızı gösterir.
- Kurum için korunması önem arz eden bilgisayar, dosyalar, sözleşmeler, e-posta gibi tüm önemli unsurların farkında olmayı ve düzenli bir şekilde korumalarını öngörür.
- Herhangi bir afet durumunda minimum kayıp yaşamayı sağlar.
- Çalışanların, müşterilerin ve tedarikçilerin bilgilerini güven altına alır.

- Bilgi varlıklarını siber saldırılardan korur.
- Bilgi güvenliği ihlallerinde hukuka uygun kanıtların hazırlanmasını sağlar.
- Sistemde görülebilecek açıklıkları ve bunların yaratacağı riskleri azaltır.
- Bilgisayar sistemlerinin daha düzenli ve sistematik kullanımını sağlar.
- Bilgilere erişimin ve aktivitelerin kayıt edilmesini sağlar.

2.4. Bilgi Güvenliği Yönetim Sisteminin Kurulumu, Aşamaları ve Faydaları

Bilgi sadece elektronik ortamlarda bulunan bir şey değildir. Kağıt üzerinde, ortamda bulunan bir yazı tahtasında hatta kurum içi sohbetlerde bilgi ortalıkta bulunmaktadır. Bu nedenle ISO/IEC 27001 standardı yalnızca kullanılan bilgisayarlar ya da bilişim güvenliği ile ilgilenmez. Bilgi ile ilgili her türlü süreçte güvenliğin sağlanması amaçlanmaktadır. Standart dahilinde bir BGYS kurulur ya da geliştirilir. Bu sistemi işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere bu standart hazırlanmıştır. BGYS'nin amacı, bilgi varlıklarını korumak ve ilgili tüm taraflara güven vermek, güvenlik kontrollerini sağlamak olarak sıralanabilir. Tüm dünyada olduğu gibi ülkemizde de ISO/IEC 27001 standardı kapsamında bir kurumda BGYS kurulumunu gerçekleştirmek üzere pek çok çalışmalar yapılmıştır ve günümüzde de yapılmaya devam edilmektedir. TÜBİTAK/UEKAE tarafından yapılan çalışmalar bu alanda ülkemizdeki en önemli çalışmaların başında gelmektedir. Yapılan çalışmalar www.bilgiguvenligi.gov.tr sitesinde yayımlanmakta ve konu ile ilgili çalışma yapan ve yapacak olan kişi ve kurumların hizmetine sunulmaktadır (Altınpulluk, 2016: 24).

2.4.1. Bilgi Güvenliği Organizasyonunun (Komisyonunun) Oluşturulması

BGYS kurulumu aşamasında çalışmaları organize edecek, uygulayacak ve yönetebilecek bir ekibin oluşturulması ilk başta yapılması gereken bir eylemdir. Standart, bilgi güvenliği organizasyonlarını iç organizasyon ve dış taraflar olmak üzere iki bölüm halinde ele almaktadır. İç organizasyon, isminden de anlaşılacağı üzere kurum içinde bilgi güvenliği uygulamalarını idare eden organizasyon, dış taraflar ise bahsi geçen iç organizasyonun dışında kurumun ürettiği bilgiye erişen ve

bu bilgileri işleyen gruplardır. İç Organizasyonun temel sorumlulukları (Aydın, 2012: 15);

- Bilgi güvenliği hedeflerini kurumun ihtiyaçları doğrultusunda tanımlamak, bu hedeflere ulaşmak için gereken yeterli kaynak kullanımını sağlamak ve kurumun süreçlerine BGYS'nin doğru entegre edilmesini sağlamak,
- Kurum BGYS politikasının oluşturulmasını ve uygulanmasını, BGYS kapsamının belirlenmesini, BGYS plan ve hedeflerinin saptanmasını ve BGYS politikasına göre kurum içindeki bilgi güvenliği ile ilgili rollerin ve sorumlulukların belirlenmesini sağlamak,
- Yeterli kaynak tahsisi ile BGYS'nin kurulmasını, uygulanmasını, işletilmesini ve güncellenmesini sağlamak,
- Kurumsal amaçlar ile bilgi güvenliği ihtiyaçlarını uyumlaştırarak BGYS ile en yüksek verimi almaya çalışmaktır (Calder, 2006: 72).

Belirlenen ve görev tanımı yapılan BGYS ekibi konu ile ilgili mutlaka iyi bir eğitim almalıdır. Bunun yanında dış paydaşların da mutlaka bilgi güvenliği konusunda bilgilendirilmesi gerekmektedir. Ayrıca özellikle risk yönetimi, politika oluşturma, güvenlik prosedürlerinin hazırlanması ve uygun kontrollerin seçilerek uygulanması konuları ve aşamalarında etkin ve yetkin uzman desteği alınmalıdır. Önceden bu süreçleri yaşamış kurumlarla görüşmeler yapmak ve bilgi almak da faydalı olacaktır.

2.4.2. Kapsamın Belirlenmesi

Kurumda BGYS kapsamı belirlenirken sistem dahilinde yer alacak tüm alt organizasyonlar, bölgeler ve aktiviteler açıkça belirlenmelidir. Kapsam dışında kalan diğer tüm öğelerin neden kapsam dışı tutulduklarına dair gerekçeler açıklanmalıdır. Zaman içinde yaşanan gelişmeler ve farklılaşan ihtiyaçlarla birlikte kapsamın içeriği revize edilebilir. Ancak bu değişiklikler yönetilebilir boyutta olmalıdır. Organizasyonun fiziksel yapısı ve süreçler göz önünde bulundurulmalıdır.

2.4.3. Bilgi Güvenliği Politikasının Oluşturulması

- BGYS kurulumunda, ekibin belirlenmesinden sonraki aşama kurumsal bilgi güvenliği politikasının oluşturulmasıdır. Bu politikaları kurumun bilgilerinin yönetimini ve güvenliğini düzenleyen uygulamalar ve bu uygulamalar için hazırlanan kurallardan ibarettir. Kısa, anlaşılabilir ve uygulanabilir olan,, farklılaşan durumlara ve iş stratejilerine göre esneyebilen bir bilgi güvenliği politikası iyi hazırlanmış demektir. Olabildiğince az sayıda teknik ifade kısaltmalar kullanılmalıdır. Kurumda her seviyede çalışan personel politika dokümanını anlayabilmelidir. Bilgi güvenliği politikasının ISO/IEC 27002 BGYS uygulama ilkeleri ve tavsiyeleri standardına bağlı olarak içermesi gereken maddeler şu şekilde sıralanabilir (Altınpulluk, 2016: 28);
- BGYS kapsamının ve bilgi güvenliğinin kurum için gerekliliği ve önemi,
- Bilgi güvenliğine dair hedefleri,
- Yönetimin Bilgi Güvenliğini Sağlama Sözü ve Politika Dokümanının Onayı,
- Bilgi güvenliği açısından belirlenen sorumluluklar,
- Kurumun Risk Yönetim çerçevesinin tanıtımı,
- Bilgi güvenliği ile ilgili ilkeler, genel kurallar ve olası ihlal durumlarında uygulanacak olan yaptırımlar,
- Yasal mevzuatlar ve standartlar ile uyumun belirtilmesi ve koordinasyonu,
- Gelişen ve farklılaşan durumlar ve stratejiler, aynı zamanda olağan yapılacak olan gözden geçirme faaliyetleri ve bunlara yönelik tarihleri belirtilmelidir.

2.4.4. Risk Yönetimi Süreci

"TS ISO/IEC 27001:2005 Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler" standardında risk yönetimi, kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler olarak tanımlanmıştır. Sözlük anlamında göre risk kayıp ve/veya zarar neden olabilecek, beklenen veya beklenmeyen olayların meydana gelme olasılığıdır. Bu durumda riskin iki temel bileşeni ortaya çıkmaktadır. Bunlar;

- Belirlenen bir sonuca ulaşamama olasılığı ve istenmeyen bir olayın oluşma olasılığı

- Sonuca ulaşamama veya riskin gerçekleşmesi durumunda meydana gelen olay (Etki)

Riski tanımladıktan sonra risk analizi kavramını ele almakta fayda vardır. Risk değerlendirme aşamasında öncelikle risk analizi kapsamında kurumun risk tahminleri yapılır ve olası riskler tanımlanır. Bunlar ile risk değerlendirmesi yapılır. Risk analizinde genel olarak iki yöntem kullanılır. Bunlardan biri olan Nicel risk Analizinde risk analizinin girdileri sayısal değerlere aktarılarak matematiksel hesaplamalar gerçekleştirilir. girdilerin sayısal değerler yerine "yüksek", "düşük" gibi tanımlayıcı değerlere aktarılarak yapılan analize ise Nitel Risk Analizi denir. Tüm kurum ve kuruluşlar her zaman bilgi güvenliği hususunda pek çok risk ile karşı karşıya kalabilirler. Kurum hem bilgi güvenliği risklerini kontrol altında tutmak hem de bu riskleri bertaraf etmek amacı ile risk yönetimine dair süreç çalışması yapmalıdır. Risk analizi ile amaçlanan kurumda oluşabilecek tehlikelerin en uygun şekilde yanıtlanabilmesini sağlayacak her türlü tehdidin oluşumunu ve etkilerini azaltabilecek çeşitli prosedürlerin ve kontrol mekanizmaların oluşması için incelemeler yapmaktır (Erdoğan, 2020: 45).

Risk yönetim planlarında dört temel hedef yer almaktadır bulunmaktadır. Bunlar;

- Risklerin ortadan kaldırılması,
- Risk oluşturabilecek nedenlerin yok edilmesi,
- Kontroller ve önleme faaliyetleri ile risklerin varlığını bilerek hayata devam edilmesi,
- Risklerin diğer kurumlara yollanması

İlk olarak kurumlar kapsam belirleyerek risk analizine başlamalıdır. Kapsam dahilinde olacak bilişim sistemlerinin sınırları oluşturulur. Bilgi varlıkları belirlenir. Varlıklar tanımlanırken donanım ve yazılım varlıkları dışında kağıt üzerinde olan bilgiler, belgeler, süreçler, ürünler, çalışanlar ve kurumsal itibar da birer varlık olarak düşünülmelidir. Bunlar belirlenirken anket yönteminden, mülakatlardan faydalanılabilir. Bu yönde bir ekip oluşturmak ve bunların tarama faaliyetleri yapmaları yerinde olacaktır. Bundan sonra bu varlıkların kriterler belirlenerek sınıflandırılması gerekir. Bu kriterler maddi değer, ya da niteliksel özellikler olabilir. (Aydın, 2012: 48).

Sonraki adım saptana varlıklara yönelik olası tehditlerin belirlenmesi olmalıdır. Bu tehditler afetler gibi doğal kaynaklı olabileceği gibi kazalar çevresel etkiler ya da kasıtlı ya da kasıtsız insan kaynaklı tehditler olabilir.

Kurum bilgi varlıklarında açıklık var ise bunlar saptanmalıdır. Bu açıklıklar ihlallere sebebiyet verebilir. Bu konuya azami önem gösterilmelidir. Riskleri yönetmeyle ilgili oluşturulan komisyon çeşitli yöntemler ile açıkları tespit etmelidir. Farklı tarama ve testlerin uygulanması gelişmiş teknolojik imkanlar ile mümkün olabilmektedir. Yine bu açıklıkların tespitine yönelik anket ve mülakatlar da yapılabilir. (Doğantimur, 2009: 60).

Bir sonraki aşamada tehditler ile oluşabilecek açıkların meydana gelebilme olasılıkları hesaplanmalıdır. Bunlar derecelendirilmeli ve bunlara karşı yapılan kontroller gözden geçirilmelidir. Daha sonra bu tehditler sonucunda oluşabilecek olumsuzlukların analizi yapılmalıdır. Gizliliğin bozulması, bütünlüğe zarar gelmesi ve erişilebilirliğin sekteye uğraması durumlarının oluşup oluşmayacağı ve bunlarla ilgili mali kayıpların meydana gelebilme durumları incelenmelidir. Bu etkiler derecelendirilir.

Risk faktörleri de saptanır ve bunlar da derecelendirilir. Bunun için bir matris oluşturulması faydalı olacaktır. Risklerin belirlenmesinden sonra önleyici ve düzeltici faaliyetler planlanmalıdır. Bunun için risk işlemesi yapılır. Risklerin işlenmesinde kurumun belirlenen risklere karsı uygulayacağı kontroller belirlenir. ISO/IEC 27001 standardının EK-A dokümanında belirlenmiş olan kontroller yapılabileceği gibi kurum kendi kontrol mekanizmalarını da oluşturabilir. Bunlar oluşturulurken hukuki olmalarına dikkat edilmelidir. (Aydın, 2012: 50).

Tüm kontroller gerçekleştirildikten sonra sonuçlar raporlanmalıdır. Bu süreç sürekli bir şekilde döngüsel olarak devam etmelidir. Zaman içinde farklılaşan durumlar göre güncellemeler yapılmalı, gereksiz hale gelen kısımlar atılmalı, yeni ihtiyaçlara yönelik yeni kısımlar eklenmelidir.

Bunlar tamamlandıktan sonra ilgili ekip yönetim tarafından BGYS kurulumu amacı ile yetkilendirilmelidir. Bu yetki alındıktan sonra ISO/IEC 27001 standardı

uygulanabilirlik bildirgesi yayınlanmalıdır. Bu yayında seçilen kontrol mekanizmaları yer almalıdır. Neden seçildikleri açıklanmalıdır. Amaçları anlatılmalıdır. Seçilmeyen kontrol mekanizmalarının hangileri oldukları ve neden seçilmedikleri de bildiride yer verilmesi gereken konulardandır. (Aydın, 2012: 60).

2.4.5. BGYS'nin Gerçekleştirilmesi ve İşletilmesi

Gelinen bu noktada oluşturulan BGYS komisyonuna bağlı risk yönetimi çalışma ekibi bir risk işleme planı hazırlamalı ve komisyona sunmalıdır. Plan içinde olası risk durumlarında yapılması gerekenleri yapılma sıraları ve gerektirdiği kaynakları yer almalıdır (Bingöl, 2010: 26).

Plan hazırlandıktan sonra tanımlanmış olan risklerin ortadan kaldırılması ya da en azından azaltılması için tercih edilen kontrol mekanizmalarının uygulanması ve ne derece etkin olduklarının ölçülmesi gerekmektedir. Bu işlem seçilen kontrollerin hedeflenen amaca uygunluğunu görme fırsatını sunacaktır. Burada hedeflenen amaç hem risklerden kurtulmak ya da etkilerini azaltabilmek, bunu da en az maliyet ile gerçekleştirebilmektir. Eğer planlanan kontrol mekanizması uzun süre gerektiriyorsa süreç içinde durumu değerlendirmek için ara toplantılar yapılmalıdır. Etkinlik ölçümü için ISO/IEC 27004 BGYS ölçüm ve metrikleri standardını kaynak olarak kullanmak yerinde olacaktır. Ölçeceğimiz göstergeler önce-sonra durumunu yansıtabilmelidir. Bu işlemlerle eş zamanlı olarak çalışanlara eğitimler verilmeli ve farkındalık yaratılmalıdır (Bingöl, 2010: 26).

İnsan faktörü aslında bilgi güvenliğinde en fazla zafiyet yaratan unsurdur. Burada insan faktöründen kast edilen sadece konu ile doğrudan ilgili çalışanlar değil tüm kurum çalışanlarıdır. Her çalışanda konu ile ilgili farkındalığın oluşturulması gerekmektedir. Bilgi ve farkındalık olmaz ise kişiler sorumluluklarını tam anlamıyla yerine getiremezler. Bu yüzden bunun ön şartı etkili bir eğitim faaliyetidir. Eğitimler zaman içinde tekrarlanmalı, yeni bilgiler konu açıklamalarına eklenmelidir. Bu konuda kurum içi insan kaynaklarından yararlanabileceği gibi konuya hakim uzman kişilerden de eğitim hizmeti alınabilir.

Teknolojideki değişim ve gelişim sürekli olduğundan gerektiğinde yeni kontrollerin öğrenilmesi için yeni eğitimler düzenlenmeli, eğitimlerin etkinlikleri ölçülmelidir (Çelik, 2021: 26). BGYS'nin işleme süreçlerinde her durumun kayıt altın alınması ve belgelenmesi çok önemlidir. Bunlar kurumsal hafızada yer almalıdır. Kurum üst yönetimi tüm bu süreçler için gereken kaynağı komisyonun kullanımına sunmalıdır. (Şen ve Yerlikaya: 2013).

2.4.6. BGYS'nin İzlenmesi ve Gözden Geçirilmesi

BGYS işleme başladıktan sonra yapılan kontrollerin ne derece etkin olduğu gözlenmelidir. Eksiklikler, başarısızlıklar ve başarılı mekanizmalar tespit edilmelidir. Önleme faaliyetlerinin sonuçları değerlendirilmelidir. Kurum iş ortamları değişebilir, yeni hedefler konulabilir, bir takım yeni yasal mecburiyetler ortaya çıkabilir. Bu gibi durumlarda yeni kontrol mekanizmaları gerekecektir. Bunlar hızlı bir şekilde tanımlanmalıdır. Düzenli aralıklarla sistem başarısı iç kaynaklarca değerlendirilmelidir. Bu denetimlerle sistemin güncelliği sağlanabilir (Marttin ve Pehlivan, 2010: 51).

2.4.7. ISO 27001 BGYS Dokümantasyon Sistemi

Bir yandan BGYS süreçleri yürütülürken eş zamanlı olarak ISO/IEC 27001 standardına ilişkin dokümantasyonlar da yapılmalıdır. Bu kapsamda (Kahraman, 2006: 61);

- BGYS politikası ve kontrol amaçları dokümanı
- BGYS kapsam dokümanı
- BGYS'yi destekleyici prosedürler ve kontrol dokümanları
- Risk değerlendirme metodolojisi
- Risk değerlendirme raporu
- Risk isleme planı
- Kuruluş tarafından, bilgi güvenliği proseslerinin etkin planlanmasını, işletilmesini ve kontrolünü sağlamak için ihtiyaç duyulan dokümante edilmiş prosedürler ve kontrollerin etkinliğinin ölçüm dokümanı
- Bu standart tarafından gerek duyulan kayıtla

- Uygulanabilirlik Bildirgesi.

Bunlara bir takım ek dokümanlarda ilave edilmelidir. Yönetimin BGYS'nin işlemesi yönünde aldığı kararlar ve bu karaların yer aldığı toplantı tutanakları, mutlaka zorunlu belgelere eklenmelidir. Tüm belgeler ve kayıtlar sürekli ve düzenli bir şekilde güncel halde tutulmalıdır. (Kahraman, 2006: 62).

2.4.8. Yönetimin Sorumluluğu

Yönetim BGYS için mutlaka bir politika belirlemeli, gerekli kaynağı ayırmalıdır. Politika belirlenirken hangi düzeyde risklerin kabul edilebilir olduğu kararı verilmelidir. Eğitim faaliyetleri düzenlemesine fırsat sağlamak, denetimleri planlamak ve denetim sonuçlarını değerlendirmek yönetimce mutlaka yapılması gereken işlemlerdir.

2.5. Bilişim Sistemi

2.5.1. Bilişim Sisteminin Tanımı

Bilişim sistemleri, kullanılacak olan bilgilerin toplanmasında, daha sonra işlenmesinde, kullanım anı ve sonrasında depolanmasında ve gerektiğinde ağlar üzerinde paylaşılmasında kullanılan iletişim ve bilgisayarlar dâhil bütün teknolojileri kapsar. Bu teknolojiler kurum ve kullanıcılara karar verme desteği de sunmaktadır. Böylece kontrol ve koordinasyon sağlanabilirken personelin problem çözümüne, karışık durumların algılanabilmesine ve yeni ürün/hizmetlerin oluşturulmasında da rol oynamaktadır.

Bilişim akla ilk olarak kişilere yararlı ve anlamlı hale getirilmiş bilgiler akla gelmektedir. Veri ise, bilgi verir. Bu bilgi ile var olan bir sorunu çözebilir ya da karar verebiliriz Bilişim sistemindeki üç aktivite yer almaktadır. Bunlar girdi, işlem ve çıktı olarak sayılabilir. Kurumun dışından elde edilen ya da toplanan bilgiler girdileri oluşturmaktadır. Ham haldeki veriler işlem aşamasında anlamlı duruma getirilir. İşlenmiş olan bilginin kişilere ya da kullanacak birimlere aktarılması ise çıktıdır (Güner ve Altuğ, 2019: 15).

Bilişim sistemleri yetkilendirilmiş kişilerin girdileri doğrulamasına ve değerlendirmesine destek veren geri besleme kısımlarını da içerir. Resmi olarak bilişim sistemleri elle ya da bilgisayar tabanlı olarak iki ayrı kategoride incelenebilmektedir. Çok önceden beri var olan, kağıt ve kalem kullanarak oluşturulan sistemler el sistemleri olarak adlandırılmaktadır. Diğeri ise her gecen gün akıl almaz bir hızla gelişen bilgisayar tabanlı sistemlerdir (BTBS). El sistemlerine göre çok daha fazla hızlı ve büyük boyutlardaki işlemleri halledebilen sistelerdir.

Modern bilişim sistemlerinin temelinde bilgisayarlar ve bunlarda kullanılan yazılım programları yer almaktadır. Bilgisayarların görevi bilgileri saklamak ve işlemektir. Bilgisayarlarda işlemleri yöneten ve kontrol eden programlar ya da yazılımlar bulunmaktadır. Yine de bilgisayarlar bilişim sistemlerinin tek bir parçasıdır, tamamını ihtiva etmezler.

2.5.2. Bilişim Sektörünün Gelişimi

İlk bilgisayar diyebileceğimiz ENIAC yaklaşık 50 yıl önce faaliyete geçmiştir. Son 30 yılda ise bilgisayarlar hem hız hem de kapasite yönünden çok büyük aşamalardan geçmiştir. BU gelişmelerle birlikte ağ yapıları ve internet tüm dünyada yaygın bir hale gelmiştir. Zaman içinde ana bilgisayarlar ile kişisel bilgisayar ağlarının bağlantılı hale gelmesi merkezden kontrol ve idare edilebilen gelişmiş sistemlerin ortaya çıkmasını sağlamıştır. Yazılım teknolojileri aynı dönemde donanım teknolojisi kadar olmasa da önemli bir gelişim yaşamıştır. Başta programlama dilleri olmak üzere, pek çok sistem ve uygulama yazılımları pazarlara girmiştir (Güner ve Altuğ, 2019: 16).

Pek çok şirketin çok uluslu hale gelmesi ve farklı lokasyonlarda birimlerinin olması merkez ile dış bağlantılar arasında iletişim ihtiyacını doğurmuştur. Bu ihtiyaca yönelik alt yapılar oluşturulmuştur. İlk dönemlerde altyapıyı kurmak pahalı olduğundan telefon hizmetleri devlet kurumları tarafından verilmiştir. Yatırım maliyetlerinin yüksek olması ve güvenlik yönündeki endişeler iletişimin kamu tekelinde olmasına neden olmuşsa da bu değişmeye başlamıştır. Gelişen fiber optik teknoloji ile incecik fiber lifleri üzerinde eş zamanlı olarak yüzbinlerce telefonun kullanılabilmesine olanak vermiştir. Dijital teknolojilerin Telekom alt yapılarında yer

alması ile iletişim kapasiteleri ve hızları büyük bir ilerleme kaydetmiştir. Ayrıca hem bakım maliyetleri hem de işletme maliyetlerinde önemli düşmeler yaşanmış, bu da tüketicilerin yararına olmuştur (Güner ve Altuğ: 2019, 16).

1980'li yıllarda başlayan bilgi ve iletişim teknolojileri (BİT) ilerlemeleri beraberinde iş dünyası için pek çok fırsat yaratmıştır. Departmanların daha etkin olabilmesi için neredeyse tüm işlemler için bilgi e iletişim teknolojileri süreçlere dahil edilmiştir.

Başlangıçta askeri bir proje olan internet yıllar içinde günlük hayatın bir parçası olmuştur. İnternetteki gelişmeler e-ticaret gibi alanların doğmasına, edevlet gibi hayatı kolaylaştıran yapıların oluşmasını sağlamıştır İletişim ağları yoğun bir şekilde kullanılınca sektörde kaynak ve sermaye fırsatları oluşmuştur. Özel sektör ve finansman dünyasında yaşanan hızlı gelişmeler ve globalleşme önemli bir sermaye birikimi yaratmış, yatırma dönüşen bu birikim ile devletlerin tekel yapıları ortadan kalkmaya başlamıştır. İletişimde kamu-özel rekabeti başlamıştır. Sonuçta bu gelişme kullanım maliyetlerini düşürmüştür (Çokmutlu, 2014: 66).

Globalleşen dünya ekonomisindeki bunun sonucu olarak büyük boyutları verilerin de aktarmak bir zorunluluk olarak ortaya çıkmıştır. Başlarda hem kapasitenin düşük olması hem de maliyetlerin yüksek oluşu buna fırsat vermese de hat kapasitelerinde artış ile makul ücretli bir şekilde mümkün hale gelmiştir. İletişim olanakları arttıkça daha da fazla iletişim talebi oluşmuştur.

Bilginin ağlar üzerinde paylaşımı ve yönetimi küresel standartların oluşması ile daha kolay hale gelmiştir. Telekomünikasyon teknolojilerinde yaşanan ilerleme bilgilerin hem daha hızlı iletilmesini hem de daha büyük veri paketlerinin iletilmesi sağlamıştır. Bu da özellikle ekonominin globalleşmesine fırsat vermiştir. Dijital teknolojilerin gelişmesi bu fırsatı daha da üst noktalara taşımıştır. Globalleşmeye diğer katkıları TV yayınlarının yaygınlaşması, mobil teknolojilerin gelişmesi, kişisel bilgisayar ve internet kullanım oranlarında artış kaynaklı olmuştur (Kılınç, 2012: 47).

Hızla gelişen internet ve iş dünyasının buna hızlı adaptasyonu geleneksel ticaretten e-ticarete geçişi hızlandırmış fiziksel değiş tokuşun yerini elektronik

ortamda ticaret yapılması almıştır. İçeriği sayısallaştırılmış görüntü, ses, metin, yazılım ve benzeri hizmetlerin uluslararası ticarette, tanıtım, sipariş, satın alma, ödeme, dağıtım ve satış sonrası servis işlemlerinin tümünün ağlar üzerinden yapılması mümkün olabilmektedir. Böylece ortaya çıkan e-ticaret önemli bir yenilik olmuştur. Kamu sektörü de hem iç ortamlarında hem de dış ortamlar ile ilişkilerinde bilişim teknolojisi imkanlarından yoğun bir şekilde yararlanmaktadır. (Çokmutlu, 2014: 72).

E-Ticaret ile hem bireysel müşteriler hem de küçük ve orta ölçekli işletmeler geleneksel yöntemlere göre daha kolay ve daha az maliyetli ticaret yapma şansı bulmuşlardır. Bu sisteme ne kadar çok kullanıcı ve işletme dahil olursa o kadar kullanım hızı artacaktır. İnternet ortamına taşınan ticaret zaman tasarrufu sağlayarak pazarların da yapısını değiştirecektir. Paralama ve dağıtım sistemleri değişim gösterecektir. Ürünler ve hizmetler daha fazla müşteri odaklı hazırlanacaktır. Toplumsal refah hem satıcı hem de alıcının tam rekabete daha yakın bir ortamda bir araya gelmesi ile artacaktır. Bununla birlikte mevcut istihdam yapısında da değişim yapacaktır. Kaybolan meslekler olabileceği gibi yeni meslekler de ortaya çıkacaktır. Bu yeni alanlara iyi eğitimli çalışanlar gerekecektir.

Yazılım sektörü donanım ve iletişim sektörleri kadar yatırım gerekmemektedir. İnsan zekası ve yaratıcılık yazılım sektörünün en önemli girdisidir. Eğitilmiş, zeki ve yaratıcı kullanıcı kolaylıkla sektörün ve pazarın bir parçası olabilmektedir. Girişimci bir kişi sadece bir modem olması durumda tüm dünyaya ulaşabilir bir hale gelebilmektedir. Bu yönleri ile yazılımların üretilmesi ve sonrasında ticaretinin yapılması geleneksel ticari yöntemlerden çok farklıdır. Yazılımların üretildikten sonra kopyalanması ve bu şekilde çoğaltılması maliyetleri düşürmektedir (Kılınç, 2012: 68).

İlk üretim sürecinde kullanılan yaratıcı zeka ve zihinsel emek başlangıçta bir maliyet yaratsa da ürün ortaya çıktıktan sonra kopyalama ile çoğaltma herhangi bir maliyet unsuru oluşturmamaktadır. Yazılımların artması üretimde çok önemli ilerlemeler sağlamış ve verimli üretim süreçleri oluşturmuşlardır. Yazılımlar üreticilerin rekabet gücüne de katkı sağlamıştır. Böylece hem yazılım sektörü hem de hizmet ettiği diğer sektörlerde gelir artışları yaşanmıştır.

Yazılım sektöründe ilk önce yer alan ülkeler büyük kazanımlar elde etmişlerse de halen tüm ülkeler için yeni fırsatlar mevcuttur. Bu sektörde gelişme ve yaratıcılığın sonu olmadığı söylenebilir. Doğru kurgulanmış yeni yazılımlar ülkelere daha fazla istihdam imkanı ve daha çok gelir getirebilir. Verimlilik ve refah düzeyinde artış yaşanacaktır. Günümüzde yazılım sektöründe Hindistan, İsrail ve İrlanda önemli bir yere sahip ülkeler olarak öne çıkmaktadır. Çin, Rusya ve Filipinler de bu konuda atak yapan ülkeler arasındadır (Çokmutlu, 2014: 77).

Daha önceki dönemlere kıyasla bilgi toplumunda fiziki ve kültürel çevredeki değişim çok hızlı olmuştur. Genel olarak her alanda çok hızlı bir değişim yaşanması daha önceki dönemler ile bilgi toplumu döneminin arasındaki çok önemli ir fark olarak ortaya çıkmaktadır. Bu dönemde başarıya ulaşmanın en önemli yolu en güncel bilgi ve teknolojiye en hızlı şekilde ulaşmaktan geçmektedir.

Hızlı değişim dışında önemli bir konu da bilginin pazarlanabilen ve paylaşılabilen bir hal almasıdır. Günümüzde bilgi kendisine alıcı bulabilmektedir. Bu alıcılar işleri ile ilgili üretim, yöntem vs gibi konularda yenilik, uygunluk, uygulanabilirlik ve hız arayan kişilerdir. Bilginin alıcıları olduğu gibi satıcıları da vardır. Bilgiyi üreten bu satıcılar tecrübeli, satışa sundukları bilgiyi daha önce kendisi kullanmış kişilerdir. Bu ticarette elbette aracılar da vardır. Belirli bir fiyatlandırma sistemi oluşmuştur (Güner ve Altuğ, 2019: 18).

Bilgi toplumunda aynı zamanda teknoloji toplumudur. Teknolojinin en yeni araçları bilgi toplumunda hizmete sunulmuştur. Bu dönemde bilişim teknolojisine sahip olmak bir zorunluluktur. Bilgisayar olmadan bilgi toplumu var olamazdı.

Yeni teknolojilerin geliştirilmesi uzun dönemde ülkelerin en önemli refah artış kaynağıdır. Bu noktada yetişmiş ve yaratıcı insan kaynağı çok önemli hale gelmiştir. Bunun yerini sermaye alamamaktadır. Teknoloji üreten ve kullanan nitelikli insan gücü ülkelerin en önemli refah getirici unsuru haline gelmiştir.

Günümüzde hem bilişim ve iletişim sektörlerinde hem de elektronik cihaz üretiminde yaşanan hızlı ilerleme sanayi ekonomisinden bilgi ekonomisine geçişi de hızlandırmıştır. Bu ortamda üretim, tüketim ve dağıtım ilişkileri de değişim

göstermektedir. Artık bilgi rekabette en önemli unsurlardan biri olmuştur. Yeni ekonomi beraberinde yeni kavramları da getirmiştir. Bunları e-devlet, e-ticaret, e-pazaryerleri, mobil iş, e-bankacılık (internet bankacılığı), gibi kavramlardır (Güner ve Altuğ, 2019: 19).

2.6. Kişisel Verilerin Korunması Kanunu

2.6.1. Türkiye'de Kişisel Verilerin Korunması Kanunun Gelişimi

Bilginin pek çok ortamda paylaşılıyor olması korunması için yasal düzenlemeler yapılmasını zorunluluk haline getirmiştir. Kişisel Verilerin Korunması Kanunu (KVKK) yayınlanmadan önce de kişisel verilerin korunmasına dair bir takım düzenlemeler yapılmıştır.

KVKK'dan çok daha önce kişisel verilerle ilgili toplama, saklama ve işlenmeleri hakkında mevzuat düzenlemeleri bulunmaktaydı. Hukuk devletlerinde kişisel verilerin korunması önem arz etmektedir. Kişilere ait resimlerin, seslerinin, hayat alanlarının, şeref ve haysiyetlerinin korunması kişisel haklar içerisindedir (Kılınç, 2012: 15). KVKK'ya zemin hazırlayan ve bu kişisel hakları koruyan hükümler aşağıda incelenmektedir.

2.6.1.1. 1982 Anayasası'nda Kişilik Hakkı ve Kişisel Veriler

Kişisel verilerin korunması hakkındaki düzenlemelerin alt yapısını Anayasa oluşturmaktadır. 1982 Anayasasında kişisel verilerin korunmasına yönelik bazı maddeler yer almaktadır. Bunlar; özel hayatın gizliliği hakkını düzenleyen 20. Madde ile başlamaktadır. 21. Madde haberleşme gizliliğini, 22. Madde konut dokunulmazlığını, 24. Madde din ve vicdan özgürlüğünü korumayı 25. Madde ise düşünce ve kanaatleri açıklamaya zorlanamama hakkını içermektedir (Kılınç, 2012: 16).

2.6.1.2. 4721 Sayılı Türk Medeni Kanunu'nda Kişilik Hakkı

Anayasanın ikinci bölümünde kişisel verilerin korunmasını isteme hakkı bulunmaktadır. Bu hak ile Türk Medeni Kanunu'nun (TMK) kişilik hakkını koruyan hükümleri, kişisel verilerin korunması için kullanılmaktadır (Çokmutlu, 2014: 125).

TMK belirli bir ölçüde de olsa kişisel verilerin korunmasına ilişkin hükümler içermektedir. Hangi kişilik haklarının korunduğuna dair kesin sınırlar olmamasından dolayı kişisel verilerin korunması yönünde tek başına yeterli olamamaktadır (Çokmutlu, 2014: 127). Olan hükümler de ihlalleri önlemeye değil olduktan sonra yapılabilecek yaptırımlarla ilgilidir.

2.6.1.3. 6098 Sayılı Türk Borçlar Kanunu'nda Kişilik Hakkı

6098 Sayılı Türk Borçlar Kanunu'nda (TBK) da kişilik hakkının korunmasına yönelik hükümlere yer verilmiştir. Bu hükümler kişisel verilerin korunması yönünde değerlendirilebilmektedir. Türk Borçlar Kanununda kişilik hakkının korunması hakkında 27., 49. ve 58. maddeler öne çıkmaktadır.

TBK'nın 27. Maddesi; bu maddeye göre bir sözleşme kişilik haklarına aykırı bir şekilde düzenlenmiş ise kanun bu sözleşmeyi kesin hükümsüz olarak kabul etmektedir. Bu hükmün KVKK'da var olan rızanın geçerli olabilmesinin bazı koşullara bağlı olması suretiyle rızaya rağmen kişinin verilerini korumaya yönelik düzenleme ile aynı doğrultuda olduğu söylenebilir.

TBK'nın 49. Maddesinde haksız fiil sonucunda oluşan zararların tazminine dair bir hükümdür. Kişisel verilerin hukuka aykırı olarak işlenmesi haksız bir fiil olduğundan bu işlemler sonucunda kişinin uğradığı zararın tazminini isteme hakkı TBK ile düzenlenmiştir (Çokmutlu, 2014: 127).

TBK 58. Madde ise; kişiye kişilik hakkı zarara uğradığında karşılaştığı zararlarını talep etme hakkı vermektedir. Günümüzde internet ortamında kişilik hakkı ihlallerinin daha kolay ve yaygın olduğu düşünüldüğünde bu maddenin halen daha yoğun uygulandığını söylenebilir.

Borçlar Kanunu da tıpkı Medeni Kanun gibi hak ihlallerinin önüne geçen değil olduktan sonra uygulanacak yaptırımları içeren bir yapısı vardır ve bu kanun da kişisel verilerin korunmasında yeterli değildir.

2.6.1.4. 5237 Sayılı Türk Ceza Kanunu'nda Kişilik Hakkı

5237 Sayılı Türk Ceza Kanunu'nun (TCK) 132. ve devam maddeleri özel hayatın gizliliği hakkının ihlali neticesinde oluşan suçların tanımlarını ve bu durumlarda uygulanacak cezaları içermektedir.

134. madde özel hayatın gizliliğini ihlal suçunu düzenlerken, 135. Madde kişisel verilerin işlenmesi suçunu ele almaktadır. 136. Madde bilgilerin hukuka aykırı bir şekilde elde edilmesi ve kullanılmasını düzenlemektedir. 138. madde ise verileri yok etmeme suçunu konu almaktadır.

2.6.1.5. 5809 Sayılı Elektronik Haberleşme Kanunu

Elektronik Haberleşme Kanunu 2008 yılında yürürlüğe girmiştir. Bir kurum elektronik haberleşme hizmeti sunmakta ise bu kanunun 4. Maddesine göre bilgi güvenliği ve haberleşme gizliliğinin korunmasını sağlamak mecburiyetindedir. Kişisel verilerin gizliliğinin korunması açısından ek yükümlülükler getirileceği ise 12. Maddede yer almaktadır.

51. Maddede ise kişisel verilerin işlenmesinde uyulması gereken ilkelere yer verilmiştir. KVKK'daki aynı ilkeler bulunmaktadır. Yine bu maddede verilerin yurt dışına çıkarılması, işlenmesinin hukuka uygunluğu konusunu ele almaktadır.

2.6.1.6. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

6698 Sayılı KVKK'nın kapsamına iki grup dahildir. Kanunun ikinci maddesinde tanımlanan bu gruplar verileri işlenen gerçek kişiler ve bu verileri işleyen gerçek ve tüzel kişileredir. Aynı maddeye göre KVKK'nın uygulanması için kişisel verileri işleme faaliyetlerinin kısmen ya da otomatik olması veya otomatik olmasa bile bir veri kayıt sisteminin parçası olması zorunluluğu vardır.

2.6.2. Avrupa Birliği'nde Kişisel Kişisel Verilerin Korunmasına Yönelik Düzenlemeler

Veri gizliliğinin önce hayatta yer almış daha sonra kanunlara girmiştir. Avukat-müvekkil, doktor-hasta ilişkilerinde olduğu gibi kişisel bilgiler alan kişiler

tarafından korunmak zorundadır. Bu zorunluluk önce etik bir kural olarak uygulanmış zaman içinde hukuksal mevzuatta kendilerine yer bulmuşlardır (Calder, 2016: 28).

2.6.2.1. Avrupa İnsan Hakları Sözleşmesi

İkinci Dünya Savaşı bittikten sonra, Avrupa ülkeleri hukukun, demokrasinin, insan haklarının ve sosyal gelişimin öncelendiği bir düşünce ile Avrupa Konseyini kurmuşlardır. Avrupa İnsan Hakları Sözleşmesi (AİHS) de bu amaca yönelik olarak 1950 yılında kabul edilmiş, üç yıl sonra 1953 yılında yürürlüğe girmiştir. AİHS hükümleri, taraf devletler için bağlayıcı özelliktedir. Üye ülkeler zaman içinde bu hükümleri ya kendi hukuk mevzuatlarının bir parçası haline getirmiş veya sözleşmeyi ulusal hukuklarında etki gösterecek şekilde tanımışlardır. Taraf devletler, ulusal güvenlik nedeni ile kullanılan yetkiler de dahil olmak üzere yetki ve güçlerini kullanırken sözleşme ile sağlanmış haklara saygı göstermek zorundadırlar. Bazı emsal kararlarında Avrupa İnsan Hakları Mahkemesi (AİHM) buna vurgu yapmıştır (Solmaz, 2019: 8).

Avrupa İnsan Hakları Sözleşmesinin (AİHS) 8. maddesi aile ve özel yaşama saygı duyulmasını isteme hakkını kapsamaktadır. Kişisel verilerin korunması hakkı da bu maddeye dayanmaktadır. AİHM kişisel verilerin korunmasına dair ihlal iddiası ile gelen dosyaları bu maddeye göre karara bağlamaktadır. Bahsi geçen madde özel alan kavramını tanımlamaktadır. Mahkeme aynı maddenin ikinci fırkası açısından bu alana yapılan müdahaleleri değerlendirmektedir. Müdahalenin gerçekleşip gerçekleşmediği konusunu bu madde ile kabul veya reddetmektedir.

AİHM'in kararları arasında iletişimin dinlenmesi, özel veya kamu kuruluşları tarafından gerçekleştirilen çeşitli izleme faaliyetleri, kamu yetkililerince kişisel verilerin depolanması da dahil olmak üzere veri güvenliğini ilgilendiren kararlar yer almıştır. AİHM vermiş olduğu kararlar ile devletlere sadece hak ihlali yapmamalarını belirtmeyi değil bundan öte olarak hakların güvence altına alınması yönünde çaba göstermeleri gerektiğini de ortaya koymuştur (Solmaz, 2019: 9).

2.6.2.2. Kişisel Verilerin Korunması Sözleşmesi

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi 108 numaralı sözleşme olarak da bilinmektedir. Bu sözleşme 1960'lardan sonra teknolojide yaşanan gelişmeler doğrultusunda ülkelerin ve uluslararası kuruluşların kişisel verilerin gizliliği ve korunması kavramlarıyla tanışmaları sonucunda ortaya çıkmıştır. Sözleşme Avrupa Konseyi tarafından 1985 yılında kabul etmiştir. Bağlayıcı niteliği ile bu sözleşme, özel olarak kişisel verilerin toplanması ve işlenmesine karşı uluslararası bir sözleşmedir.

Kişilerin ırk, siyasi görüş, din ve adli kayıt gibi hassas bilgilerinin işlenmesi il kez bu sözleşme ile hukuka aykırı kabul edilmiştir. Bu sözleşme kapsamında değerlendirilen veriler hem özel sektör tarafından toplanan hem de kamu kesimince toplanan ve işlenen tüm verilerden oluşmaktadır. 108 No'lu sözleşme ile vatandaşların yetkisiz veri toplanması ve işlenmesi gibi kötüye kullanımlara karşı korunması amaçlanmıştır. Ayrıca verilerin sınır ötesi aktarılmasını da düzenlemektedir. Doğru bir şekilde anonimleştirilen veriler 108 No'lu sözleşme ile kişisel veri olarak kabul edilmediği için sözleşme kapsamında değillerdir (Güner ve Altuğ, 2019: 18).

Kişisel verilerin hukuka aykırı olarak toplanması ve işlenmesine karşı 108 No'lu sözleşme bazı standartlar getirmiştir. Bu sözleşmenin ile yaklaşık olarak aynı zamanlarda OECD, Özel Yaşamın Korunması Ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri yayınlamıştır. Bu iki çalışma ile pek çok Avrupa ülkesi kişilerin veri güvenliği düzenlemeleri için faaliyete geçmişlerdir (Tikkinen, vd. 2018: 12).

108 No'lu sözleşmeden sonra Avrupa Birliği 95/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifini yayınlamıştır ve bu direktifin temelinde 108 Nolu sözleşme yer almaktadır.

2.6.2.3. Bireylerin Korunması

1990'ların başına kadar Avrupa Birliği içinde kişisel verilerin işlenmesine dair düzenlemeler birbirleri ile tam uyumlu olamamıştır. Buna yönelik olarak yapılan çalışmalar neticesinde 108 No'lu sözleşmeyi temel alan bu çalışma neticesinde 95/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi 1995 yılında kabul edilmiştir. Bu direktif ile kişilerin verilerinin işlenmesi faaliyetlerine karşı korunmasını ve bu verilerin Avrupa Birliği içerisindeki dolaşımının düzenlenmesi gerçekleştirilmiştir (Elgesem, 1999: 12).

2.6.2.4. Sınırdışı Veri Protokolü

İnternetin yaygın olarak kullanılmaya başladığı ve bilginin Web 2.0 uygulamaları ile dünya çapında paylaşılabilir olduğu interaktif ortamların oluştuğu 1990'larda kişisel verilerin gizliliği ve korunması konularında bir takım yeni ihtiyaçlar doğmuştur. Arama motorları, yer belirleme sistemleri, güvenlik kameraları, nesnelerin interneti ve biyometrik veriler gibi araçlarla doğan bu ihtiyaçlar giderek artmaktadır (De Terwangne, 2014: 13).

2001 yılında oluşan yeni ihtiyaçlara cevap verebilmek için Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar Ve Sınıraşan Veri Akışına İlişkin Protokol (181 Sayılı Ek Protokol) ile sözleşme uyumlulaştırma çalışması yapılmıştır. Bu protokol ile sözleşmede belirlenen prensiplerin daha kolay uygulanabilmesi amaçlanmıştır. Zaman içinde oluşan gereklilikler ile yeni eklemeler de yapılmaktadır.

Çalışmaların başlamasının üzerinden uzun yıllar geçmesine rağmen birlik üyesi devletlerde kişisel verilerin korunması düzenlemelerinde tutarlılık ve uyum yakalanamamıştır. Bundan dolayı geçerli sistemler güncellenmiş ve General Data Protection Regulation (GDPR) düzenlemesi yayınlanmıştır.

2.6.2.5. General Data Protection Regulation

GDPR kapsamı ikinci maddesine göre belirlenmiştir. Düzenleme kişisel verilerin tamamen veya kısmen otomatik araçlarla ya da dosyalama sisteminin

parçasını oluşturan veya bir dosyalama sisteminin parçası olması amaçlanan araçlarla işlenmesine uygulanır.

Ancak bu maddenin devamında GDPR'nin uygulama alanı olmayacak istisnai durumlar belirtilmiştir. GDPR aşağıdaki durumlarda;

- Avrupa Birliği hukuku kapsamına girmeyen faaliyetlerde,
- Üye devletler tarafından Avrupa Birliği Anlaşması'na uygun olarak dış güvenlik politikasına ilişkin hükümler uygulanırken,
- Tümüyle kişisel ya da ev faaliyetleri sırasın gerçek bir kişi tarafından, kamu güvenliğine karşı tehditlere yönelik güvence sağlanması ve bunlara bağlı suçların önlenmesi, soruşturulması, saptanması ve kovuşturulması veya cezaların infaz edilmesi ile ilgili yetkili makamlar tarafından kişisel verilerin işlenmesi durumlarında,

uygulanmaz.

GDPR; Avrupa Birliği tabanlı kontrolör ve işleyicilere uygulanmanın yanında, Birlik içerisinde yer alan veri sahibinden mal veya hizmet sunulması ya da veri sahibinin davranışlarının izlenmesi durumlarında, veri işleme işleminin nerede gerçekleştiğine bakılmaksızın, uygulanmaktadır (Tikkinen, vd. 2018: 14).

GDPR, üye ülke vatandaşlarının dışında Birlik içerisinde yaşayan ancak vatandaş olmayan göçmenler, çalışma ve turist vizesi ile Birlik sınırları içerisinde bulunanlar, yaşama izni olanlar gibi Birlik içerisinde yer alan tüm kişileri kapsamaktadır. Kişi bu kapsamda olmasa da verileri Birlik sınırları içinde depolanıyor ya da işleniyorsa GDPR'nin korumasından faydalanabileceklerdir (Anı, 2018: 49).

2.6.2.6. Elektronik Haberleşmede Gizlilik

E-Gizlilik Direktifi olarak da bilinen 2002/58/EC Sayılı Elektronik Haberleşme ve Gizlilik Direktifi, Avrupa Birliğinde yürürlükte olan veri gizliliği hükümlerine ek olarak, elektronik haberleşme alanında gizliliği düzenlememektedir. GDPR'nin 95. Maddesi ile elektronik haberleşme alanında gösterdiği faaliyetler

sebebi ile 2002/58/EC Sayılı Direktif'e tabi olan ve bu konuda yükümlülük altında bulunan gerçek ve tüzel kişilere ek yükümlülük getirmeyeceği düzenlenmiştir.

2.7. Kişisel Verilerin Korunması

Öncelikle kanuna yönelik kavramları ele alınmalıdır. Bu nedenle bu başlık altında ilk olarak kişisel verilerin korunmasına yönelik kavramlara yer verilecektir.

2.7.1. Kişisel Verilerin Korunmasına İlişkin Kavramlar

2.7.1.1. Açık Rıza

Rıza ve açık rıza, hukuka uygun olarak verilerin elde edilmesi ve işlenmesi konuları açısından önemlidir. Kanun ile açık rıza "Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" şeklinde tanımlamıştır. Rızanın açık rıza olarak sayılabilmesi için gerekli şartlar;

- Belirli br konuya dair rıza alınmış olması
- Uygun bir bilgilendirme faaliyetin var olması ve
- Özgür irade ile rıza verilmiş olmasıdır.

Kişilerin verileri üzerindeki hakimiyetlerinin artırılması ve veri işleme faaliyetlerinde şeffaflığın sağlanması amacı ile kişisel verilerin korunmasına yönelik düzenlemeler yapılmaktadır. Kişi bir kere rıza verdiğinde ileride yapılacak başka işleme faaliyetlerine de izin vermiş sayılmaz. Verilen rızanın hangi işleme faaliyetlerini kapsadığı net bir şekilde göstermeyen bilgilendirmeler olduğunda rıza açık rıza olarak kabul edilemez.

Veri toplayan kişi ya da kurumların kişinin verileri üzerinde hak sahibi olabilmeleri için işleme faaliyetlerine rıza almadan önce kişisel verileri hangi amaçla, ne kadar süre ile, hangi nitelik ile işleneceği ve hangi amaçlarla kullanılacağı konusunda kişileri bilgilendirilmesi gerekir (Korkmaz, 2016: 29).

Cebir, tehdit, hata ve hile gibi durumların varlığında kişinin iradesi sakatlanmış sayılacağı için verilen rıza açık rıza olarak değerlendirilemez. Özgür irade şarttır. Tarafların eşit durumda olmadıkları (işçi-işveren ilişkisi gibi) veya bir

ürün/hizmetin sunulması için rızanın ön şart olduğu hallerde verilen rızanın özgür iradeye dayandığı kabul edilemez (Gözüküçük, 2014: 62).

2.7.1.2. Anonim Hale Getirme

Kişisel verilerin işlenmesi her zaman kötü bir durum değildir. Hatta kimi durumlarda günlük hayatımızı kolaylaştıran faydalı yanları da olabilmektedir. Sağladığı yararlar ile hak ve özgürlükler arasında bir denge kurmak gerekmektedir. Verilerin anonimleştirilmesi buna hizmet etmektedir. Bu durumda kişisel gizlilik korunmuş olacaktır.

Anonim hale getirme kavramı; KVKK'da "Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi" şeklinde tanımlanmıştır. Önemli olan anonimleştirme sonrası verilerin bir kişiyi işaret edip etmemesidir. Kişinin adı yerine takma isim kullanılması ya da her kişiye bir numara verilmesi anonimleştirme için yeterli değildir. Çünkü bazenbu uygulama yapılsa bile kişinin kimliğinin tespiti mümkün olabilmektedir. Hiçbir şekilde kişilerin kimlikleri açık edilmeden veriler saklanmalıdır (Çekin, 2016: 21).

2.7.1.3. İlgili Kişi Kavramı

Kanun, "ilgili kişi"yi "Kişisel verisi işlenen gerçek kişi" olarak tanımlamıştır. Kişisel veri kavramı ülkemiz hukuk sisteminde gerçek kişilerin verilerini ifade etmektedir. Ancak tüzel kişiye ait bir veri ile gerçek bir kişinin kimliği belirlenebiliyor ise o zaman bu veri kişisel veri kapsamına girmektedir (Yücedağ, 2017: 11).

Tüzel kişilerin verilerinin kapsam dışı kalmasının nedeni kişisel verilerin genellikle kişinin manevi varlığı ile ilgili olması ve tüzel kişilerin manevi tazminat talep etme haklarının tartışmalı olmasıdır. Tüzel kişiler haklarının ihlal edildiği durumlarda önceki bölümde bahsedilen ikincil kanun hükümleri çerçevesinde haklarını arayacaklardır.

Gerçek kişi sınırlaması, kişisel verilerin korunmasının, Türk Medeni Kanunu'na uygun olarak sağ ve tam doğum ile başladığı ve kişinin ölümü ile son bulduğu anlamına gelmektedir. Türk Medeni Kanunu'na göre kişinin ölümü ile kişiliği de son bulacağından, ölülerin de ilgili kişi olarak değerlendirilmeleri mümkün değildir (Yücedağ, 2017: 12).

2.7.1.4. Kişisel Veri

KVKK'nın 3. Maddesinin 1. Fıkrasının d bendine göre "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi" kişisel veri niteliğindedir. Kanun bir önceki başlıkta belirtildiği üzere gerçek kişilerin verilerini kapsadığı için tüzel kişilerin verileri kişisel veri sayılmamaktadır ayrıca bir verinin kişisel veri olarak değerlendirilebilmesi için ilgili kişiyi belirlenebilir kılması gerekmektedir.

2.7.1.5. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi kavramı; KVKK'nın m 3./1-e ile tanımlanmıştır. Buna göre:

"Kişisel verilerin işlenmesi; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi kapsar."

Kişisel verilerin işlenmesi kavramı belirli işlemlerin yazılması yoluyla tanımlanmamış, her somut olaya özel bir şekilde değerlendirilmek üzere geniş ve yoruma açık olarak tanım yapılmıştır. Verilerin sadece kaydedilmesi bile bir işleme faaliyeti olarak değerlendirilmektedir (KVKK, 2018).

Kanun otomatik yollarla yapılan tüm işlemeleri kapsarken, verilerin otomatik olmayan yollarla işlenmesini yalnızca bu faaliyetlerin bir veri kayıt sistemi aracılığıyla yapılması hallerinde kapsar. Burada veri kayıt sistemi, elektronik veya

fiziki ortamda oluşturulan ve verilerin sınıflandırılabildiği her türlü sistemi kapsar (KVKK, 2018).

2.7.1.6. Kurum

KVKK, 19. ve devam maddeleri ile idari ve mali özerkliğe sahip bir veri koruma otoritesi kurmaktadır. KVKK'ya göre; Kişisel Verileri Koruma Kurumu, yani Kurum, merkezi Ankara olan, kamu tüzel kişiliğine haiz ve Cumhurbaşkanının görevlendireceği bakan ile ilişkili olan bir kamu tüzel kişiliğidir.

Kurum'un bakanlık ile hiyerarşik bir bağı yoktur ancak bakanlığın idari vesayet denetimine sınırlı şekilde tabiidir. 15 Temmuz 2018 tarihli ve 30479 sayılı Resmi Gazetede yayımlanan "Bakanlıklara Bağlı, İlgili ve İlişkili Kurum ve Kuruluşlar ile İlgili 2018/1 Sayılı Cumhurbaşkanlığı Genelgesi" ile Kurum Adalet Bakanlığı ile ilişkilendirilmiştir. Kurumun görev ve sorumlulukları KVKK'nın 20. Maddesi ile belirlenmiştir. Bunlar;

- Görev alanı ile ilgili ulusal ve uluslararası gelişmeleri takip etmek, iş birlikleri kurmak,
- Yıllık faaliyet raporu sunmak ve kanunlarla verilen diğer görevleri yerine getirmek olarak özetlenebilir (Gürsel ve Düğmeci, 2018, 320).

2.7.1.7. Kurul

Kurul, Kişisel Verileri Koruma Kurumunun dokuz üyeden oluşan bağımsız karar organıdır. Kurul;

- Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamaktan,
- Hak ihlali şikâyetlerini karara bağlamaktan,
- Bir şikayet anında ya da bir şekilde ihlal iddiası öğrenildiğinde resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almaktan,

- Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemekten,
- Veri Sorumluları Sicilinin tutulmasını sağlamaktan,
- Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmaktan,
- Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmaktan,
- Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmaktan,
- KVKK'da öngörülen idari yaptırımlara karar vermekten,
- Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmekten,
- Kurumun; stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemekten,
- Kurumun stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamaktan
- Kurumun performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konulardan hakkında hazırlanan rapor taslaklarını onaylamaktan ve yayımlamaktan,
- Kanunlarla verilen diğer görevleri yerine getirmekten sorumludur. Kurul içeresindeki toplantılar aksi kararlaştırılmadıkça gizlidir.

İdarenin kanuniliği ilkesi gereği, Kurul'un Kurum adına alacağı kararlara ve yapacağı işlemlere karşı yargı denetimi yolu açıktır. Kurul'un verdiği idari para cezaları hariç diğer işlemlerine karşı İdari Yargılama Usul Kanundaki esaslara göre İdari dava açmak mümkündür. Kurulca kesilen idari para cezalarına ise 5326 sayılı Kabahatler Kanunu hükümlerine göre itiraz edilebilir (Gürsel ve Düğmeci, 2018: 322).

2.7.1.8. Başkan

KVKK'nın 24. Maddesine göre Kurul ve Kurumun Başkanı, Kurumun en üst amiridir ve kurum hizmetlerinin mevzuata ve kuru stratejine uygun olarak

yürütülmesini sağlar. Başkan aynı zamanda, kurul toplantılarını idare eder, kurul kararlarının kamuoyuna duyurularını sağlar, kurumun yönetim ve işleyişine ilişkin bütçe ve personel atamaları dahil olmak üzere idari görevleri yerine getirir.

2.7.1.9. Veri Sorumlusu

Kişisel verilerin hangi amaçlarla ve araçlarla işleme tabi tutulacağının kararını veren, verilerin kaydı için sistemlerin kurulmasından ve yönetilmesinden sorumlu olan kişi, "veri sorumlusu"dur. Burada kişi; özel hukuk tüzel kişisi de kamu tüzel kişisi de olabilir. Altı çizilmesi gerekli başka bir husus; veriler bir tüzel kişi tarafından işleme tabi tutulduğunda, veri sorumlusunun o tüzel kişinin çalışanları değil, bizzat tüzel kişiliğin kendisi olduğudur (Pekmez, 2019: 28).

Kanun'un lafzında veri sorumlusunun, kişisel verilerin işlenmesine dair kararları vermesinin yanı sıra veri kayıt sisteminin kurulmasından ve yönetilmesinden de sorumluğu olduğunun belirtilmesi; kişinin yalnızca bu iki şartı aynı anda sağlaması halinde mi veri sorumlusu sıfatına haiz olabileceği yönünde bazı tartışmalara sebebiyet vermiştir. Ancak doktrinde bunun zorunlu değil tanımlayıcı bir etken olduğu, bu yüzden kişisel verilerin işleme ve araçlarını belirleyen kişinin veri sorumlusu olduğu yönündedir. Bu bağlamda veri sorumlusunun belirlenmesinde temel kıstas işlevi yani verilerin işleme tabi tutulacağı amaçlar ve hangi yöntemler ile bu işleme faaliyetlerinin yürütüleceğine karar vermek konusunda yetkili olmasıdır.

İşlev odaklı yapılan tanım sebebiyle veriye sahip olan herkes veri sorumlusu sayılmayacaktır olamaz. Örneğin bir şirket verilerini saklamak ve depolamak için bir başka şirketten hizmet satın alıyorsa, depolama hizmetini veren şirket veriye sahip olduğu halde verinin kimlerle ne şekilde paylaşılacağını veya ne şekilde işleneceğini belirleyen otorite olmadığından veri sorumlusu olarak değerlendirilmeyecektir. Bunun en güzel örneği, verilerin saklanması için bir bulut depolama çözümü tercih edildiğinde şayet bulut altyapısını sunan şirket ile ayrıca bir veri işleme anlaşması yapılmazsa, bu şirketin veri sorumlusu olmayacağıdır (Memiş, 2017: 12).

KVKK veri sorumlusuna bir takım sorumluluklar yüklemektedir. Bu sorumluklara aykırı hareket edilmemesi veya ilkelere bağlı kalınması gerekmektedir. Aksi halde kişiden oluşan zarar tazmin edilebilir

2.7.1.10. Veri İşleyen

Yine 6988 Sayılı KVKK'nın m. 3/1-ğ'ye göre veri işleyen kavramı; "veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi" anlatmakta kullanılır. Burada önemli olan kıstas; veri işleyenin faaliyetlerini, veri sorumlusunun talimatına bağlı olarak gerçekleştirmesidir. Bu nedenle veri işleyenin görevinin daha çok teknik kısımlar ile ilgili olduğunu söylemek yanlış olmayacaktır. Ancak veri sorumlusu ve veri işleyen kavramlarının tanımları, kişiye göre değil icra edilen faaliyetlerin niteliğine göre yapıldığından, aynı kişi farklı faaliyetleri ile hem veri sorumlusu hem de veri işleyen olabilir.

Yukarıda verilen bulut bilişim sistemleri örneğinden devam etmek gerekirse, günümüzde birçok bulut depolama hizmeti sağlayıcısının aynı zamanda depolanan verilerin anlamlı biçimde işlenebilmesi ve analiz edilebilmesi için çeşitli araçlar da sağladığı görülmektedir.

Veri işleyen kavramının en önemli özelliği veriyi, veri sorumlusunun talimatları doğrultusunda işlemesidir. Veri İşleyen, veri sorumlusunun talimatları ile bağlı olduğundan veri işlenmesine ilişkin yükümlülüklerin yerine getirilmesinde asıl sorumlu veri sorumlusu olacaktır. Veri sorumlusunun talimatlarının aşılması durumunda veri işleyenin sorumluluğu doğacaktır ve o aşamada veri işleyen "de facto" veri sorumlusu kabul edilecektir. Diğer bir deyişle talimatları aşan veri işleyen de veri sorumlusuymuş gibi değerlendirilerek ortaya çıkan zarardan sorumlu tutulacaktır (Anı, 2018: 44).

2.7.1.11. Veri Kayıt Sistemi

KVKK m.3'e göre veri kayıt sistemi, kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder. Dikkat edilmesi gereken nokta, kanun özel olarak bir belirleme yapmadığından sistemin elektronik ortamda bulunması şart değildir.

2.7.1.12. Veri Sorumluları Sicili

Kişisel verileri işleyen gerçek ve tüzel kişilerce veri işlemeye başlanmadan önce kayıt olması gereken, Kurulun gözetiminde Başkanlık tarafından kamuya açık olarak tutulan sicildir. Kural olarak veri işleme faaliyeti icra edecek olan herkesin sicile kaydolması gereklidir ancak Kurul kaydolma zorunluluğuna istisnalar getirebilir.

BÖLÜM 3

3. YÖNTEM

Araştırmanın bu bölümünde araştırmanın modeli, veri toplama araçları ve bununla ilgili süreç ile elde edilen verilerin analizine yer verilmiştir.

3.1. Araştırma Modeli

Bu araştırmada bibliyometrik analiz yöntemi kullanılmıştır. Bibliyometrik analiz alanla ilgili araştırmaların objektif olmasını sağlamaktadır. Ayrıca alanda çalışan diğer araştırmacılara, alan ve araştırmacıların çalıştığı konular ve odaklandığı noktaları göstermektedir. Alandaki yayınların değerlendirilmesine yardımcı olmaktadır (Zupic ve Cater, 2015, 430).

Bu çalışmanın ana amacı, bilgi yönetim sistemi alanında yapılan bilimsel yayınların ISO 27001 ile ilişkisini ortaya koymak ve bu bilimsel çalışmaların bibliyometrik analiz yöntemiyle profillerini çıkarmasıdır. Çalışma nitel bir yapıdadır ve ikincil veri kaynakları kullanarak betimleyici bir yapıyla doküman incelmesi analizidir.

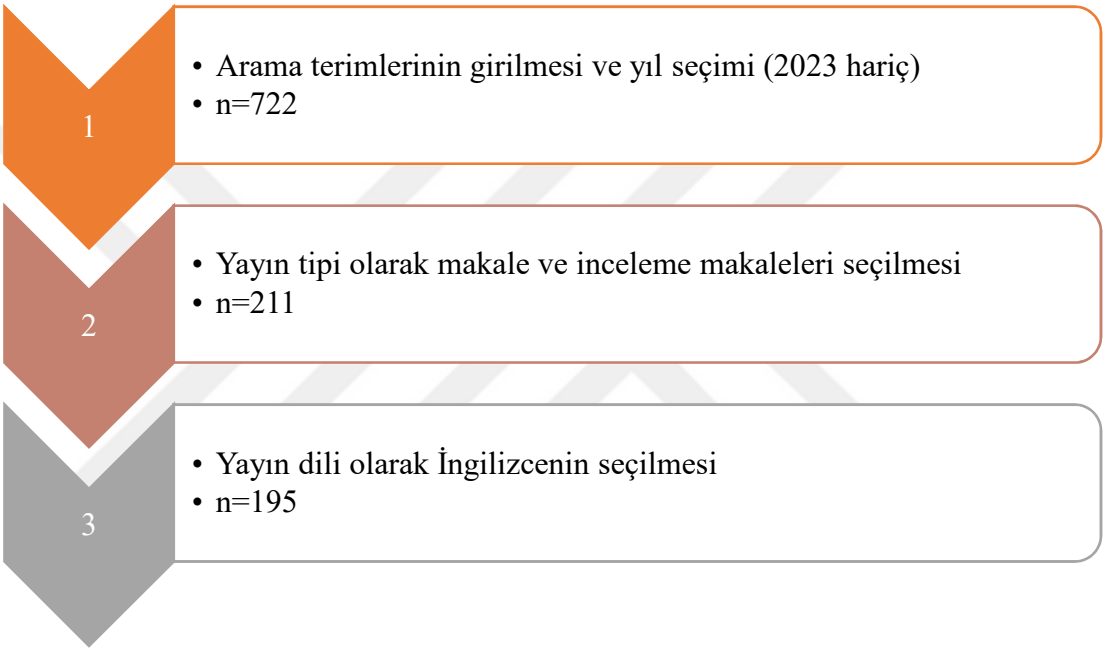
Web of Science veri tabanında arama kodlaması şu şekilde yapılmıştır; "ISO 27001" (Title) or "knowledge management system" (Title) and 2023 (Exclude – Publication Years) and Article or Review Article (Document Types) and English (Languages) and Book Chapters or Proceeding Paper (Exclude – Document Types).

3.2. Veri Toplama Araçları ve Veri Analizi

Araştırmada öncelikle Web of Science veri tabanında yayın başlıklarında “ISO 27001” ve “knowledge management system" anahtar kelimeleri taratılmıştır. Veri tabanı olarak Web of Science’ın seçilmesi içeriğinde dünyanın birçok ülkesinden yüksek etki faktörüne sahip dergiler ve akademik ürünleri bulunduran, SCI, SSCI ve A-HCI gibi bibliyometride önem arz eden dizinlere sahip olmasıdır.

Web of Science'ın dünyanın en güvenilir, multidisipliner ve küresel veri tabanlarından biri olması bu çalışmada tercih edilmesinde önemli bir etkendir. Bu taramada henüz başlangıcında olduğumuzdan dolayı 2023 yılı hariç tutulmuştur. Uluslararası yayınlarda en yaygın dil olması sebebi ile tazı dili İngilizce seçilmiştir. Yayın tipi olarak makale ve inceleme makaleleri dahil edilmiştir. Bildiri ve kitap bölümleri hariç tutulmuştur.

Şekil 1. Araştırma Verilerinin Elde Edilmesinde İzlenen Yol Haritası



Tarama sonucu elde edilen 195 makale R ve R Studio programları ile analize tabii tutulmuştur. Analizlerin yapılmasında Biblıometrix Biblioshiny paketi kullanılmıştır.

BÖLÜM 4

4. BULGULAR VE YORUM

Bulgular ve yorum bölümünde elde edilen veriler ile yapılan analiz sonuçlarına yer verilmiştir. Analiz sonuçları için R ve R Studio programları ile bibilometrix sitesi ve biblioshiny uygulaması kullanılmıştır.

4.1. Yayınlar ile İlgili Temel Bilgiler

Web of Science veri tabanından elde edilen verilerin R programı ile analizi sonucunda elde edilen temel bilgiler Tablo 3'de yer almaktadır.

Tablo 3. Yayınlar ile İlgili Temel Bilgiler

Zaman aralığı	1993:2022
Kaynaklar (Dergiler, Kitaplar, vb.)	132
Yayın sayısı	195
Yıllık yayın artış oranı %	7,87
Yayın ortalama yaşı	9,4
Yayın başına ortalama alıntı sayısı	20,08
Referanslar	7494
YAYIN İÇERİĞİ	
Anahtar Kelimeler Artı (ID)	336
Yazarın Anahtar Kelimeleri (DE)	654
YAZARLAR	
Yazarlar	563
Tek yazarlı yayınların yazarları	33
YAZARLAR İŞBİRLİĞİ	
Tek yazarlı yayınlar	34
Yayın Başına Ortak Yazarlar	3,09
Uluslararası ortak yazarlık %	17,44

Veriler incelendiğinde yayınların 1993 yılında başladığı görülmektedir. 1993-2022 yılları arasında 132 ayrı dergide 195 yayın saptanmıştır. Yayın sayısında yıllık artış ortalaması %7,87 olarak görülmektedir. Yayın başına ortalama atıf sayısı 20,08 olmuştur. Yayınlarda 7.494 referans kullanılmıştır. 654 farklı anahtar kelime seçilmiştir. 33 yazar 34 adet yayını tek başlarına hazırlamışlardır. Yayınlardaki

toplam yazar sayısı ise 563'tür. Yayın başına ortak yazar sayısı 3,09 olarak görülmektedir.

4.2. Yayınların Yayınlandığı Dergilerin Dağılımı

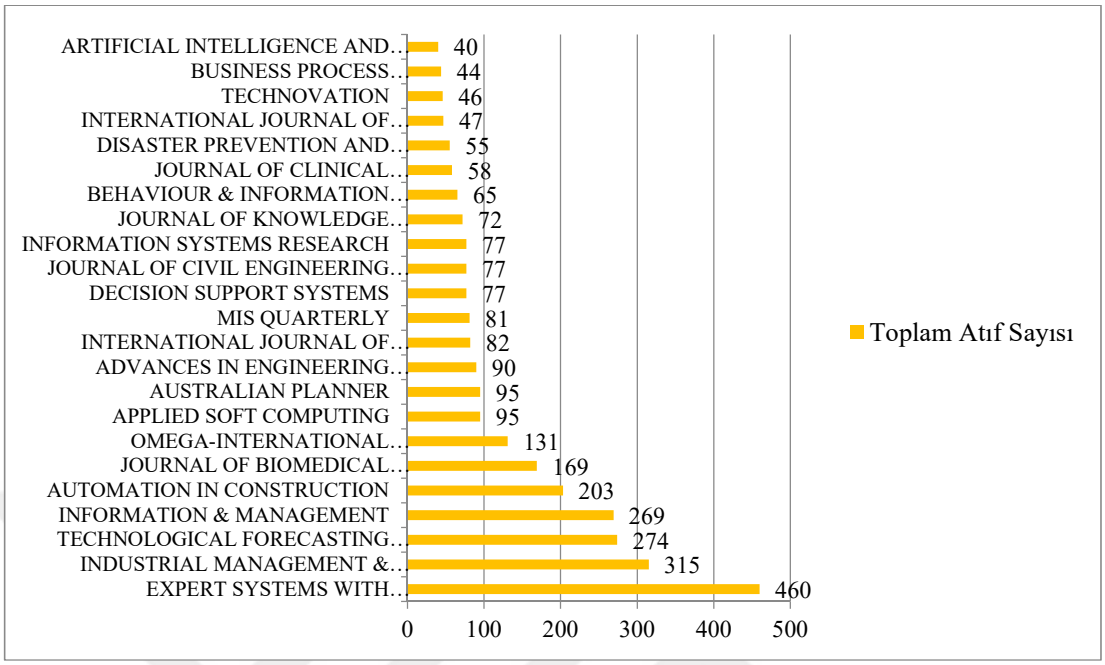
Tespit edilen yayınların yayınlandığı dergilerin dağılımı Tablo 4'de görülmektedir. Yayın sayısı 1 olan dergilere tabloda yer verilmemiştir.

Tablo 4. Yayınların Yayınlandığı Dergiler

Dergi	Makale Sayısı
EXPERT SYSTEMS WITH APPLICATIONS	8
INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY	8
INTERNATIONAL JOURNAL OF KNOWLEDGE MANAGEMENT	8
JOURNAL OF INFORMATION & KNOWLEDGE MANAGEMENT	5
KNOWLEDGE MANAGEMENT RESEARCH & PRACTICE	5
VINE JOURNAL OF INFORMATION AND KNOWLEDGE MANAGEMENT SYSTEMS	5
AUTOMATION IN CONSTRUCTION	4
INDUSTRIAL MANAGEMENT & DATA SYSTEMS	4
JOURNAL OF KNOWLEDGE MANAGEMENT	4
DECISION SUPPORT SYSTEMS	3
HUMAN SYSTEMS MANAGEMENT	3
INTERNATIONAL JOURNAL OF SOFTWARE ENGINEERING AND KNOWLEDGE ENGINEERING	3
JOURNAL OF BIOMEDICAL INFORMATICS	3
JOURNAL OF CIVIL ENGINEERING AND MANAGEMENT	3
BUSINESS PROCESS MANAGEMENT JOURNAL	2
INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS	2
INTERNATIONAL JOURNAL OF PRODUCTION RESEARCH	2
INTERNATIONAL JOURNAL OF TECHNOLOGY MANAGEMENT	2
JOURNAL OF CASES ON INFORMATION TECHNOLOGY	2
KYBERNETES	2
MIS QUARTERLY	2
PERTANIKA JOURNAL OF SOCIAL SCIENCE AND HUMANITIES	2
QUALITY-ACCESS TO SUCCESS	2
TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE	2
TEM JOURNAL-TECHNOLOGY EDUCATION MANAGEMENT INFORMATICS	2

Tablodan görüldüğü üzere 25 dergide 2 ve daha fazla makale yayınlanmıştır. En çok yayın yapılan dergiler Expert Systems with Applicatıons, International Journal of Computer Science and Network Security ve International Journal of Knowledge Management olmuştur. Bu dergilerde 8'er makale yayınlanmıştır.

Şekil 2. Dergilerin Toplam Atıf Sayıları

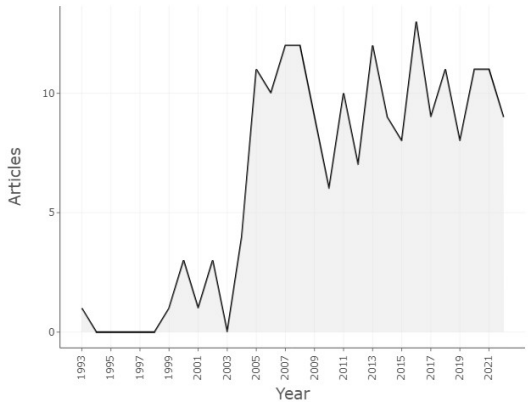


Biblioshiny paketi ile yapılan analizde toplam atıf sayılarında 460 ile Expert Systems with Applications dergisi ilk sırada yer almaktadır. Bu dergiyi 315 atıf ile Industrial Management & Data Systems ve 274 atıf ile Technological Forecasting and Social Change dergileri izlemektedir.

4.3. Yıllara Göre Yayın Sayıları

Tespit edilen 195 yayının yıllara göre dağılımı Şekil 2 ve Tablo 5'de görülmektedir. Çalışmalar 1993-2022 yılları arasında yayınlanmıştır.

Şekil 3. Yayınların Yıllara Göre Dağılımı



Tablo 5. Yayınların Yıllara Göre Dağılımı

Yıl	Yayın Sayısı	Yıl	Yayın Sayısı
1993	1	2008	12
1994	0	2009	9
1995	0	2010	6
1996	0	2011	10
1997	0	2012	7
1998	0	2013	12
1999	1	2014	9
2000	3	2015	8
2001	1	2016	13
2002	3	2017	9
2003	0	2018	11
2004	4	2019	8
2005	11	2020	11
2006	10	2021	11
2007	12	2022	9

Tablo incelendiğinde en çok yayının 2016 yılında yapıldığı (13 yayın) görülmektedir. 2007, 2008 ve 2013 yıllarında ise 12'şer yayın yapılmıştır. Bu yılları 11'er yayın ile 2005, 2018, 2020 ve 2021 yılları takip etmektedir. İlk yayın 1993 yılında yapılmıştır. 1994-1998 yılları arasında ve 2003 yılında konu ile ilgili yayın yapılmamıştır. Son yıllarda konu hakkında daha fazla yayın yapılması konunun güncelliğini göstermektedir.

Tablo 6. Yıllık Ortalama Atıf Dağılımı

Yıl	Yayın Sayısı	Makale Başına Toplam Atıf Ortalaması	Yıl Başına Ortalama Atıf Sayısı	Yıllık Atıf Sayısı
1993	1	7,00	0,24	29
1994	0	0,00	0,00	0
1995	0	0,00	0,00	0
1996	0	0,00	0,00	0
1997	0	0,00	0,00	0
1998	0	0,00	0,00	0
1999	1	0,00	0,00	23
2000	3	3,67	0,17	22
2001	1	9,00	0,43	21
2002	3	55,33	2,77	20
2003	0	0,00	0,00	0
2004	4	42,25	2,35	18
2005	11	37,82	2,22	17
2006	10	21,60	1,35	16

2007	12	22,67	1,51	15
2008	12	48,83	3,49	14
2009	9	24,22	1,86	13
2010	6	26,33	2,19	12
2011	10	31,20	2,84	11
2012	7	7,43	0,74	10
2013	12	14,50	1,61	9
2014	9	33,78	4,22	8
2015	8	8,25	1,18	7
2016	13	8,46	1,41	6
2017	9	14,44	2,89	5
2018	11	33,45	8,36	4
2019	8	6,13	2,04	3
2020	11	7,00	3,50	2
2021	11	3,18	3,18	1
2022	9	0,44		0

Tablo incelendiğinde yıl başına ortalama atıf sayısının en fazla olduğu yılın 2018 yılı olduğu görülmektedir. Bunu 2014 ve 2020 yılları takip etmektedir. İlk on sıraya bakıldığında 8'inin 2011 ve sonrası yıllar olduğu görülmektedir. Bu da konunun giderek daha fazla incelendiğini gösteriyor denilebilir.

4.4. En Çok Çalışması olan Yazarlar

Araştırma kapsamında incelenen 195 yayında 563 yazar katkı sağlamıştır. Yayınların tek veya çok yazarlı olması durumunun dağılımı Tablo 7'de görülmektedir.

Tablo 7. Yayınların Tek/Çok Yazar Durumu Dağılımı

Yazar Sayısı	**Makale Sayısı**	**Yüzde**
Tek Yazar	36	18,46
Birden Çok Yazar	159	81,54

Tabloda görüldüğü üzere 195 yayının 159'u (%81,54) birden çok yazar tarafından hazırlanmıştır. 36 yayın (%18,46) ise tek yazarlı yayındır. Bu 36 yayın 33 yazar tarafından yazılmıştır. Bu oranlar konunun ortak çalışmaya uygunluğunu göstermektedir.

Yayınlarda en etkin olan yazarların sıralaması Tablo 8'de görülmektedir. Tabloya 2 ve daha fazla yayında yer alan yazarlar dahil edilmiştir.

Tablo 8. En Etkin Yazarlar ve Yayın Sayıları

Yazar	Yayın Sayısı
LIN YC	5
SELAMAT MH	5
ABDULLAH R	4
LAM HY	3
LI M	3
TSANG YP	3
TSERNG HP	3
WU CH	3
ABDULLAH RH	2
ALIAS RA	2
BARBER KD	2
CHANG PL	2
CHAU KW	2
CHIH IL	2
CHOY KL	2
HUANG CC	2
KIM S	2
LEE GG	2
LIAO CN	2
LIN TC	2
PARK Y	2
SCHMITT U	2
TANG V	2
TSENG SM	2
XU X	2
YU WD	2
ZHANG XJ	2

Tablo incelendiğinde 5'er yayın ile en çok yayın yapan yazarların Lin YC ve Selamat MH olduğu görülmektedir. Bu iki yazarı 4 yayın ile Abdullah R takip etmektedir. 2 ve daha fazla yayın yapan yazar sayısı ise 28 olarak saptanmıştır.

Lin YC araştırma kapsamındaki beş yayınında daha çok inşaat sektöründe bilgi yönetim sistemleri konularını ele almıştır. Yayınlarında sistem önerileri sunmaktadır. Selamat MH ise özellikle eğitim alanında bilgi yönetim sistemleri konusunda çalışmalar yapmıştır. Bunun yanında yazılımlarla ilgili yayınları da mevcuttur. Abdullah R, daha çok şirketler için bilgi yönetim sistemleri konusunda araştırmalar yapmış bir yazardır.

4.5. En Etkin Dergiler

Çalışmada incelenen 195 yayın 132 ayrı dergide yayınlanmıştır. Bu yayınların aldıkları atıfların dergilere göre dağılımı Tablo 9'da görülmektedir. Tabloya en çok atıf alan ilk 20 dergi dahil edilmiştir.

Tablo 9. En Çok Atıf Yapılan 20 Dergi

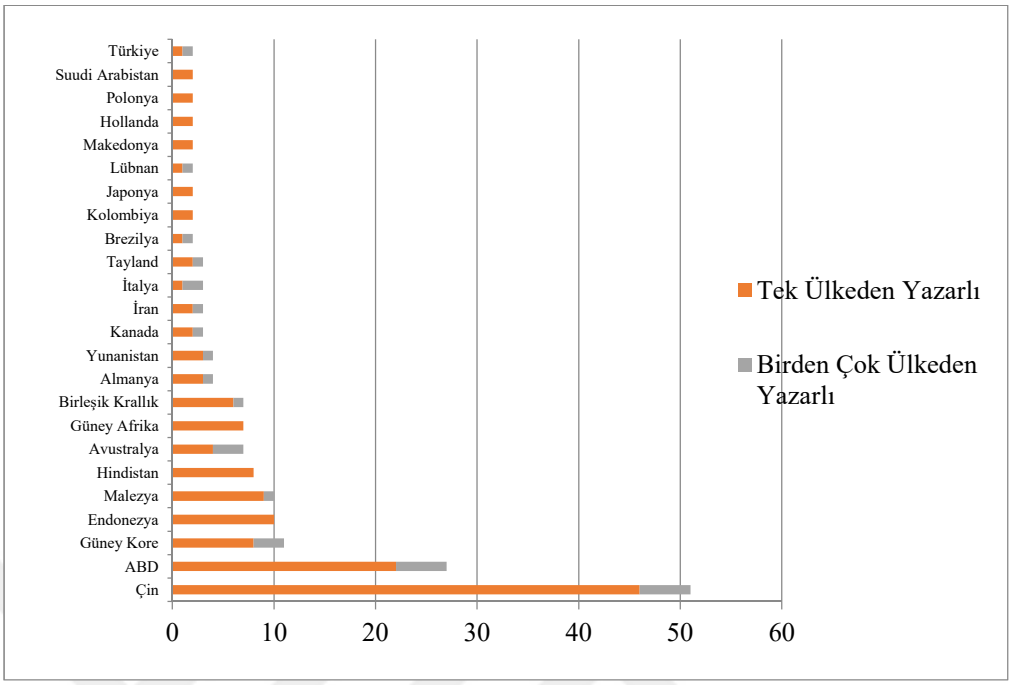
Dergi	Yayın Sayısı
MIS QUART	264
KNOWLEDGE MANAGEMENT	162
J KNOWL MANAG	135
INFORM MANAGE-AMSTER	126
EXPERT SYST APPL	123
JOURNAL OF KNOWLEDGE MANAGEMENT	111
J MANAGE INFORM SYST	83
INFORM SYST RES	81
ORGAN SCI	77
DECIS SUPPORT SYST	76
IND MANAGE DATA SYST	63
MANAGE SCI	62
INT J INFORM MANAGE	59
J KNOWLEDGE MANAGEME	56
ACAD MANAGE J	55
AUTOMAT CONSTR	55
HARVARD BUS REV	53
COMPUT HUM BEHAV	52
SLOAN MANAGE REV	50
STRATEGIC MANAGE J	47

Tablo incelendiğinde en etkin derginin 264 atıf ile MIS Quarterly olduğu görülmektedir. Bu dergiyi 162 atıf ile Knowledge Management ve 135 atıf ile Journal of Knowledge Management dergileri izlemektedir.

4.6 En Etkin Ülkeler

Araştırma kapsamında incelenen 195 yayında 42 ülkeden yazarlar katkı sunmuştur. Yayınların ülkelere göre dağılımı Şekil 3 ve Tablo 10'da görülmektedir.

Şekil 4. Yayınların Ülkelere Göre Dağılımı

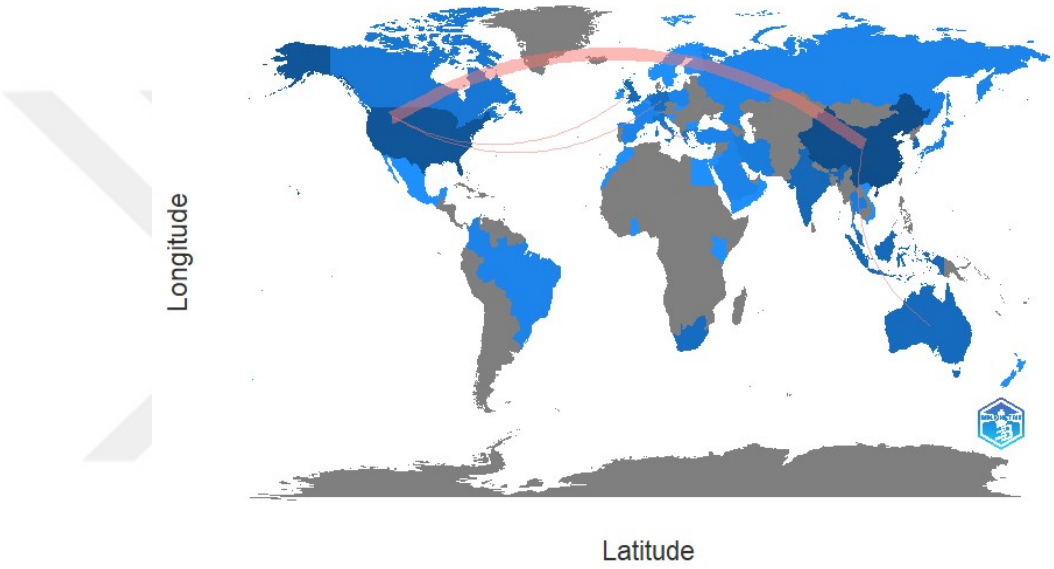


Tablo 10. Yayınların Ülkelere Göre Dağılımı

Ülke	Yayın Sayısı	Tek Ülkeden Yazarlı Yayın	Birden Çok Ülkeden Yazarlı Yayın
Çin	51	46	5
ABD	27	22	5
Güney Kore	11	8	3
Endonezya	10	10	0
Malezya	10	9	1
Hindistan	8	8	0
Avustralya	7	4	3
Güney Afrika	7	7	0
Birleşik Krallık	7	6	1
Almanya	4	3	1
Yunanistan	4	3	1
Kanada	3	2	1
İran	3	2	1
İtalya	3	1	2
Tayland	3	2	1
Brezilya	2	1	1
Kolombiya	2	2	0
Japonya	2	2	0
Lübnan	2	1	1
Makedonya	2	2	0
Hollanda	2	2	0
Polonya	2	2	0
Suudi Arabistan	2	2	0
Türkiye	2	1	1

Tablo incelendiğinde en etkin ülkenin Çin olduğu (51 yayın) görülmektedir. Çin'i 27 yayın ile ABD ve 11 yayın ile Güney Kore izlemektedir. Endonezya ve Malezya'dan da 10'ar yayın yapılmıştır. Tüm bu ülkelerde tek ülkeden yazarlı yayınlar çoğunluktadır. Görüldüğü üzere halen ülkeler arası işbirliği ile çıkan yayın sayısı azdır. Çin en fazla yayına sahip ülke iken uluslararası işbirliği oranı düşük görülmektedir.

Şekil 5. Ülkelerin Bilimsel Etkinliği



Şekil 4'deki haritada ülkelerin yayın sayıları renkler ile gösterilmektedir. Gri renkte olan ülkeler konu ile ilgili yayın yapmamış ülkelerdir. Yayın ne kadar çok ise ülke o kadar koyu bir mavi renk ile işaretlenmiştir. Şekil ile ilgili sayısal veriler Tablo 11'de gösterilmektedir. Tabloya ilk 20 ülke dahil edilmiştir.

Tablo 11. Ülkelerin Yayın Sayıları

Ülke	**Yayın Sayısı (n)**
Çin	96
ABD	62
Endonezya	19
Birleşik Krallık	18
Güney Kore	17
Hindistan	16
Avustralya	15

Malezya	14
Almanya	12
İtalya	11
Güney Afrika	10
Yunanistan	9
İran	9
Hollanda	9
Brezilya	7
Lübnan	6
Bulgaristan	4
Kanada	4
Irak	4
Japonya	4

Tablo incelendiğinde konu ile ilgili en çok yayın yapılan ülkenin Çin (n=96) olduğu görülmektedir. Bu ülkeyi sırası ile ABD (n=62) ve Endonezya (n=19) izlemektedir. Yayınlara yapılan atıfların ülkelere dağılımı ise Tablo 12'de gösterilmektedir. Tabloya ilk 20 ülke dahil edilmiştir.

Tablo 12. En Çok Atıf Alan Yayınların Ülkelere Göre Dağılımı

Ülke	**Toplam Atıf Sayısı**	**Yayın Başına Ortalama Atıf Sayısı**
Çin	1676	32,86
ABD	815	30,19
İtalya	303	101,00
Avustralya	173	24,71
Güney Kore	168	15,27
Slovenya	102	102,00
Malezya	88	8,80
Yunanistan	83	20,75
Singapur	82	82,00
Birleşik Krallık	79	11,29
Yeni Zelanda	37	37,00
Kanada	36	12,00
Mısır	35	35,00
Endonezya	30	3,00
İspanya	28	28,00
Ürdün	24	24,00
Irak	20	20,00
Bulgaristan	18	18,00
Almanya	18	4,50
Hindistan	12	1,50

Tablodan görüleceği üzere en çok yayını yapan Çin aynı zamanda en çok atıf alan ülke durumundadır. Çin'i ABD ve İtalya izlemektedir. En çok yayın yapılan ülkelerde onuncu sırada olan İtalya'nın en çok atıf alan ülkelerde üçüncü sırada olması yaptıkları yayınların ilgi gördüğünün bir göstergesi olarak değerlendirilebilir.

4.7. En Etkin Yayınlar

Araştırma kapsamında 195 yayın incelenmiştir. Bu yayınlar içinde en etkin olanları görebilmek için Dünya çapında en çok atıf alan yayınlar Tablo 13'de gösterilmiştir. Tabloya 60 ve üzeri atıf alan yayınlar dahil edilmiştir.

Tablo 13. En Çok Atıf Yapılan Yayınlar

Yayın	Toplam Atıf Sayısı
LIN TC, 2008, INFORM MANAGE-AMSTER	269
SANTORO G, 2018, TECHNOL FORECAST SOC	260
HUNG YC, 2005, IND MANAGE DATA SYST	139
KING WR, 2008, OMEGA-INT J MANAGE S	131
LEE SM, 2002, IND MANAGE DATA SYST	113
REVERE D, 2007, J BIOMED INFORM	107
NATEK S, 2014, EXPERT SYST APPL	102
LI M, 2014, APPL SOFT COMPUT	95
STEWART RA, 2010, AUST PLAN	95
CHAU KW, 2007, ADV ENG SOFTW	90
CHUA A, 2004, INT J INFORM MANAGE	82
DURCIKOVA A, 2011, INFORM SYST RES	77
TSENG SM, 2008, EXPERT SYST APPL	71
KUO RZ, 2011, BEHAV INFORM TECHNOL	65
LIN C, 2005, IND MANAGE DATA SYST	63
LIN YC, 2006, AUTOMAT CONSTR	62
ZHANG XQ, 2009, AUTOMAT CONSTR	60
JUANG YS, 2008, EXPERT SYST APPL	60

Tablo incelendiğinde en etkin yayının 269 atıf ile Lin TC ve Huang CC isimli yazarların Information & Management adlı dergide 2008 yılında yayınladıkları "Understanding knowledge management system usage antecedents: An integration of social cognitive theory and task technology fit" adlı yayın olduğu görülmektedir. Bu yayını 260 atıf ile Santoro vd. Technological Forecasting and Social Change dergisinde 2018 yılında yayınladıkları "The Internet of Things: Building a knowledge management system for open innovation and knowledge management capacity" adlı yayın takip etmektedir. En çok atıf alan üçüncü yayın ise Hung vd.'nin 2005 yılında Industrial Management & Data Systems dergisinde yayınlanan "Critical

factors in adopting a knowledge management system for the pharmaceutical industry" adlı yayın olmuştur. İlk on yayın ile ilgili bilgiler kısaca şu şekildedir.

1. Lin ve Huang, Information & Management dergisinde 2008 yılında yayınladıkları "Understanding knowledge management system usage antecedents: An integration of social cognitive theory and task technology fit" adlı makalede bilgi yönetim sistemi kullanım öncüllerini açıklamaya çalışmışlardır. Araştırmacılar çalışmaları sonucunda bilgi yönetim sistemi öz yeterliliğinin ve kişisel sonuç beklentilerinin bilgi yönetim sistemi kullanımı üzerinde önemli etkileri bulunduğu sonucuna varmışlardır (Lin ve Huang, 2008: 410).
2. Santoro ve arkadaşları 2018 yılında Technological Forecasting and Social Change adlı dergide yer alan "The Internet of Things: Building a knowledge management system for open innovation and knowledge management capacity" isimli makalelerinde nesnelerin interneti konusunu ele almışlardır. Çalışmanın amacı bilgi yönetim sistemi, açık inovasyon, bilgi yönetimi kapasitesi ve inovasyon kapasitesi arasındaki ilişkiyi incelemek olarak belirlenmiştir. Çalışma ile rekabet avantajının temeli olarak hem iç hem de dış bilgi kaynaklarını dikkate alan bilgi yönetimi ve açık inovasyona kapsamlı bir bakış açısı sunulmaktadır (Santoro vd., 2018: 347).
3. Hung ve arkadaşları 2005 yılında Industrial Management & Data Systems dergisinde yayınlanan "Critical factors in adopting a knowledge management system for the pharmaceutical industry" adlı makalelerinde maliyetleri minimumda tutarken bir firmanın rekabet gücünü artırmak için bir bilgi yönetim sisteminin uygulanmasında yer alan kritik başarı faktörlerini tartışmayı amaçlamışlardır. Çalışma sonucunda BGYS'nin benimsenmesinde strateji ve organizasyon kültürünün önemi ortaya çıkmıştır. Bu çalışma, ilaç endüstrisinin kıyaslama stratejisine özel önem verdiğini belirlemiştir. Sistemin düzgün çalışması için tam katılımın sağlanması gerektiği çıkan sonuçlar arasındadır (Hung vd, 2005: 164).
4. King ve Marks, 2008 yılında Omega dergisinde yayınlanan "Motivating knowledge sharing through a knowledge management system" adlı

makalelerinde kullanıcıların bilgi yönetim sistemine katkıda bulunma sıklıklarını ve çabalarını araştırmışlardır. Sistem kullanımında değişkenlerin kullanım motivasyonu üzerine etkili olduğu sonuçlar arasında yer almaktadır. Ödüllendirmenin önemi de çalışmada ortaya konulmuştur (King ve Marks, 2008: 131).

5. Lee ve Hong, 2002 yılında Industrial Management & Data Systems dergisinde yayınlanan "An enterprise-wide knowledge management system infrastructure" adlı makalelerinde bilgi yönetimi yaşam döngüsü kavramını, bilgi yakalama, bilgi geliştirme, bilgi paylaşımı ve bilgi kullanımı açılarından incelemişlerdir (Lee ve Hong, 2002: 17).
6. Revere ve arkadaşları 2007 yılında Journal of Biomedical Informatics dergisinde yayınlanan "Understanding the information needs of public health practitioners: A literature review to inform design of an interactive digital knowledge management system" adlı makalelerinde halk sağlığı profesyonellerinin bilgi gereksinimlerine odaklanan bir literatür taraması yapmışlardır. Çalışma sonucunda halk sağlığı faaliyetlerinin çeşitliliğini yansıtmak, insan iletişimini mümkün kılmak ve kritik bilgi kaynaklarına çoklu erişim noktaları sağlamak için tasarlanmış halk sağlığı dijital bilgi yönetim sistemlerine kritik bir ihtiyaç olduğu görülmüştür (Revere vd, 2007: 410).
7. Natek ve Zwilling, 2014 yılında Expert Systems with Applications dergisinde yayınlanan "Student data mining solution–knowledge management system related to higher education institutions" adlı makalelerinde öğrenci veri madenciliği konusuna odaklanmışlar ve yüksek öğretim kurumlarıyla ilgili bilgi yönetim sistemlerini incelemişlerdir. Çalışma yükseköğretim kurumlarında veri madenciliği faaliyetlerinin bilgi yönetim sistemlerinin ciddi bir parçası olma konusunda gerçek bir potansiyele sahip olduğu yönünde sonuç vermiştir (Natek ve Zwilling, 2014: 6400).
8. Li ve arkadaşları 2014 yılında Applied Soft Computing dergisinde yayınlanan "A new MCDM method combining QFD with TOPSIS for knowledge management system selection from the user's perspective in

intuitionistic fuzzy environment" adlı makalelerinde kullanıcının bakış açısından bilgi yönetim sistemlerinin değerlendirilmesine ve seçilmesine yardımcı olacak bir yöntem sağlamayı amaçlamışlardır. Sezgisel bulanık ortamda kullanıcının bakış açısından bilgi yönetim sistemi değerlendirmesi ve seçimi için kalite fonksiyon yayılımı ile sezgisel bulanık ortamda ideal bir çözümü birleştiren yeni bir çok kriterli karar verme yöntemi önermektedirler (Li vd, 2014: 28).

9. Stewart ve arkadaşları 2010 yılında Australian Planner dergisinde yayınlanan "Web-based knowledge management system: linking smart metering to the future of urban water planning" adlı makalelerinde su planlamasında güncel konulara, özellikle akıllı ölçüm sistemlerine genel bir bakış sağlamayı amaçlamışlarıdır. Çalışma sonucunda Avustralya şehirlerinde su planlaması ve yönetiminin geleceği için akıllı ölçümün potansiyel rolünü araştırmışlar ve web tabanlı bir bilgi yönetim sistemi önerisinde bulunmuşlardır (Stewart vd, 2010: 66).
10. Chau, 2007 yılında Advances in Engineering Software dergisinde yayınlanan "An ontology-based knowledge management system for flow and water quality modeling" adlı makalesinde mühendislere akış ve su kalitesi modellemesi hakkında bilgi paylaşma, arama ve yönetme konusunda yardımcı olabilecek ontoloji tabanlı bir bilgi yönetim sistemi sunulmaktadır. Mimari, geliştirme, uygulama ve uygulamanın yanı sıra problem çözme sırasında bilgi temsili ve görselleştirme ayrıntılı olarak açıklanmaktadır. Çalışma sonucunda ontoloji tasarımı için üç aşamalı bir yaşam döngüsü ve bilgi arama bileşenlerini otomatik olarak oluşturmak için Java/XML tabanlı bir şema kullanan ontoloji tabanlı bir bilgi yönetim sistemi önermektedir (Chau, 2007: 172).

4.8. En Etkin Kurumlar

Bu bölümde incelenen yayınların üretilmesinde katkısı olan kurumlar listelenmiştir. Tabloya 3 ve daha fazla yayına katkı sunan kurumlar dahil edilmiştir.

Tablo 14. En Fazla Yayın Yapılan Kurumlar

Kurum	Yayın Sayısı
HONG KONG POLYTECH UNIV	7
UNIV PUTRA MALAYSIA	7
CHUNG HUA UNIV	5
NATL TAIWAN UNIV	5
UNIV WASHINGTON	5
ISLAMIC AZAD UNIV	4
NATL TAIPEI UNIV TECHNOL	4
NEWCASTLE UNIV	4
GEORGE WASHINGTON UNIV	3
GRIFFITH UNIV	3
HANYANG UNIV	3
HONG KONG UNIV SCI AND TECHNOL	3
KING SAUD UNIV	3
MIDDLESEX UNIV	3
NATL CENT UNIV	3
NATL CHIAO TUNG UNIV	3
NATL INST TECHNOL	3
NATL TAIWAN UNIV SCI AND TECHNOL	3
RUSSIAN STATE VOCAT PEDAG UNIV	3
SEOUL NATL UNIV	3
SHENZHEN UNIV	3
UNIV INDONESIA	3
UNIV IOANNINA	3
UNIV MASSACHUSETTS	3
UNIV WOLLONGONG	3
YUAN ZE UNIV	3

Tabloda görüleceği üzere yayınların yapıldığı kurumların başında Hong Kong Polytechnic Üniversitesi ve Malezya Putra Üniversitesi (7'şer yayın) bulunmaktadır. Bu kurumları 5'er yayın ile Chung Hua Üniversitesi, National Taiwan Üniversitesi ve Washington Üniversitesi takip etmektedir. İlk 5 üniversite içinde Çin ve Uzak Doğu üniversiteleri çoğunluktadır.

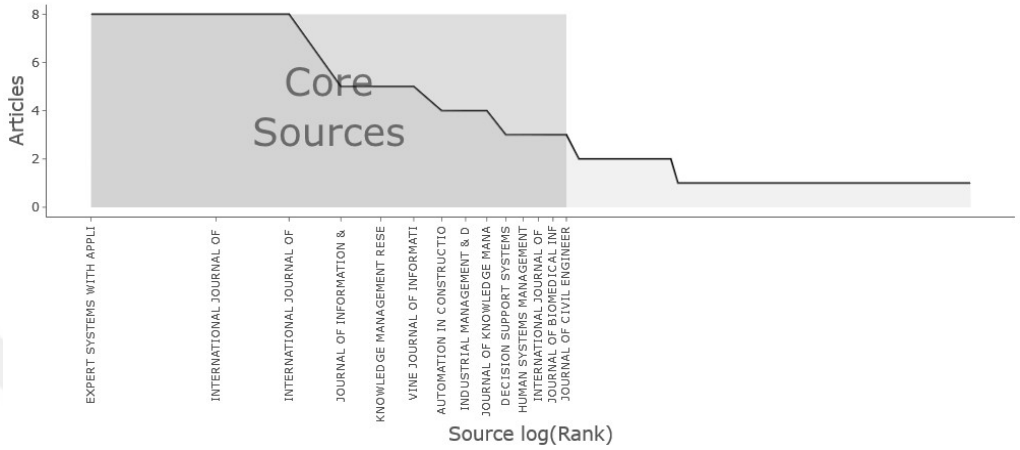
4.9. Bradford Yasası Uyumu

Bradford yasası bilim işleyişini matematiksel yollarla tanımlamaya çalışan çeşitli istatistiksel ifadelerden biridir. Bradford'un saçılma yasası adı ile bilinen bu yasada belirli bir konudaki literatürün dergilere nasıl dağıldığı açıklanır. (Garfield, 1980: 476). Bradford bu yasasında yayınları üç gruba ayırmaktadır.

- Az sayıda olmasına rağmen en verimli dergiler (çekirdek grup),
- Dergilerin daha fazla olduğu fakat verimin azaldığı ikincil grup,

- Çok daha fazla sayıda derginin olduğu fakat verimin daha da azaldığı grup,

Şekil 6. Bradford Yasası



Araştırma kapsamında incelenen 195 yayından 14'ü çekirdek grupta yer almaktadır. Bu dergilerdeki yayın sayısı 66 olarak görülmektedir. İkincil grupta yer alan 54 dergide yayın sayısı 65'tir. Üçüncü grupta 64 dergi bulunmaktadır ve toplam yayın sayısı 64'tür. Bu veriler ışığında yayınların dergilere Bradford yasasına uygun şekilde dağıldığı söylenebilir.

4.10. Ortak-Atıf Analizi

Atıflar (direkt atıf ve bibliyografik eşleme) birçok araştırmacı tarafından dokümanlar arasındaki ilişkilerin tespit edilmesinde kullanılmıştır (Düzyol, 2011: 10). Atıf yapmanın temel sebepleri arasında daha önce yayın yapanlara saygı göstermek ve bu yayınlardaki bilgilerden etik birşekilde faydalanmak sayılabilir. Ayrıca bu çalışmaların incelendiği ortaya konulmaktadır (Garfield, 1965: 191). Atıf, kullanılan bilginin belgelendirilmesi olarak kabul edildiğinden bilimsel bilgiye erişmek isteyenler için öncelikli olarak önem içermektedir (Zan, 2012, 17-18). Atıf, belirli ortak noktaları kapsayan çalışmalar arasındaki açık ve resmi bağların kurulmasını sağlayan bileşen olma özelliğini taşımaktadır. Bununla birlikte spesifik bir konu kapsamında yapılan çalışmalara ait atıfların analiz edilmesi durumunda

ilgili disiplinde kullanılan bir fikir ya da kavramın ortaya çıktığı, genişlediği veya benzeştiği yapının ortaya konması olasıdır (Zan 2019: 503).

Bibliyometrik çalışmalarda gerçekleştirilen atıf analizleri de, bilimsel yayınların niteliklerinin ve belirli bir disipline etkilerinin değerlendirilmesine imkan tanımaktadır. Bibliyometrik çalışmalarda bilimsel işbirliği ve ortak atıf ilişkilerinin incelenmesinde sosyal ağ analizinden yararlanılmaktadır. Sosyal ağ analizi, işbirliği ve ortak atıf ağlarının görselleştirilmesi ile bir araştırma topluluğu içerisinde önemli aktörlerin belirlenmesinde ve araştırma alanının gelişmesinde etkili olan bilgi ağlarının tespit edilmesinde kullanılmaktadır (Karagöz ve Yüncü, 2013: 211-212). Bu tür bibliyometrik ağ analizlerinde analiz birimi olarak bilimsel çalışmalar kullanılır. Amaç, fikirlerin ortaya çıkışlarını ve gelişmelerini izlemektir. Ortak atıf analizinin temeli şudur: Bir doküman çiftinin ortak atıf alma sayısı ne kadar büyükse, bu iki dokümanın içerikleri o kadar birbirine benzerdir, bu iki doküman birbiriyle o derece ilişkilidir (Bellardo, 1980, 231).

Bu konu Biblioshiny paketinde entelektüel yapı başlığı altında bir alt başlıktır. Bu başlık altında ortak atıf ağları ele alınmıştır. Ortak atıf analizi iki farklı yayının ya da çalışmanın birlikte alıntılanma sıklığını göstermektedir. Araştırma alanının entelektüel yapısı bu şekilde ortaya konmaktadır. Seçilen parametreye göre yayın, dergi ya da yazarın ne kadar merkezde ya da çevrede olduğunu, aradaki bağlantıları göstermektedir. Çalışılan alanın zaman içindeki köklerini ve temel eserleri ortaya koymaktadır. Ancak yeni yapılan çalışmalar yeterli atıf sayısına ulaşamayacağı için haritalamada yer alamayabilmektedir (Koç vd., 2022, 100). Çalışmamızda ortak atıf ağları yazarlar ve dergiler alt konularında incelenmiştir. Yazar ve dergi yönünden konu alanını yönlendirenler listelenmiştir. Bu analiz özellikle konu ile ilgilenmeye yeni başlayan araştırmacılara yön göstermesi için önemli ve etkilidir. Ancak özellikle analizde sadece ilk isimlerin yer alması diğer çalışmacıların gözden kaçmasına neden olabilmektedir. Yayının daha önceki bir tarihte yayınlanmış olması doğal olarak daha fazla atıf almasını sağlayacak böylece yayının etkisinin fazla olduğu yönünde bir ön yargı oluşturmaktadır. Aynı şekilde az atıf almış çalışmalar hakkında da yetersiz bir yayın düşüncesi yaratabilmektedir (Koç vd., 2022, 100).

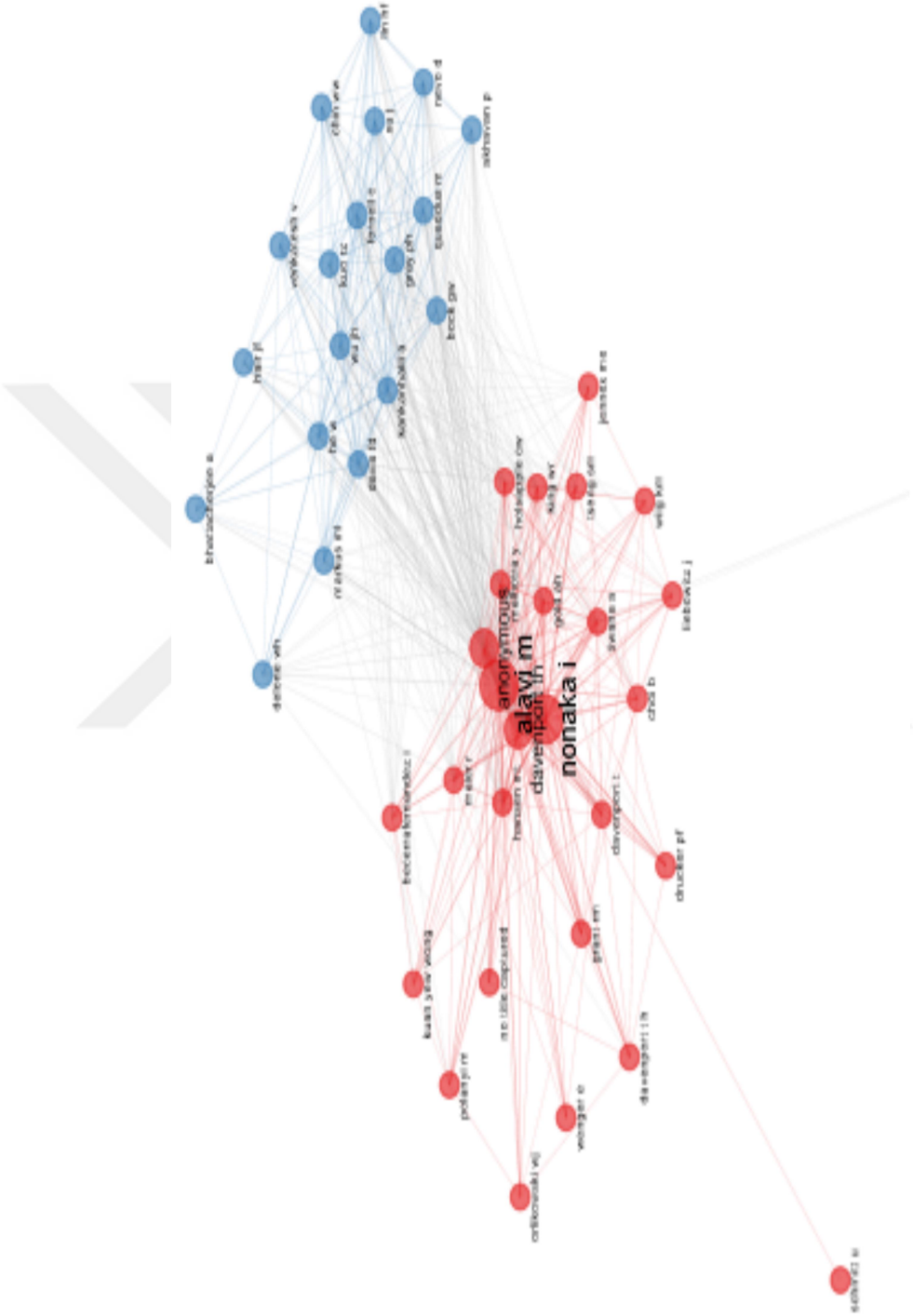
Şekil 6'da yazarların ortak atıf ağları görülmektedir. İki küme ortaya çıkmıştır. Aynı kümede bulunan yazarların benzer konuda yayınlar yaparak birlikte çalıştıkları söylenebilir. Şekilde görüldüğü gibi en çok yayında yer alan yazar Alavi M. olmuştur. Bu yazarı Nonaka I.ve Davenport TH. takip etmektedir. Bu yazarlar kırmızı kümenin merkezinde yer almaktadırlar. Mavi kümede daha eşit bir dağılım olsa da bu kümenin en etkin yazarı Kankanhlli olmuştur.

Dijital yenilikler ve stratejik BT uygulamaları konusunda uzman olan Maryam Alavi, çok sayıda yayınlanmış makaleye imza atmıştır ve birçok prestijli iş ve teknoloji dergisinin yayın kurullarında görev yapmaktadır. Halen Georgia Tech Üniversitesinde çalışmaktadır (www.scheller.gatech.edu).

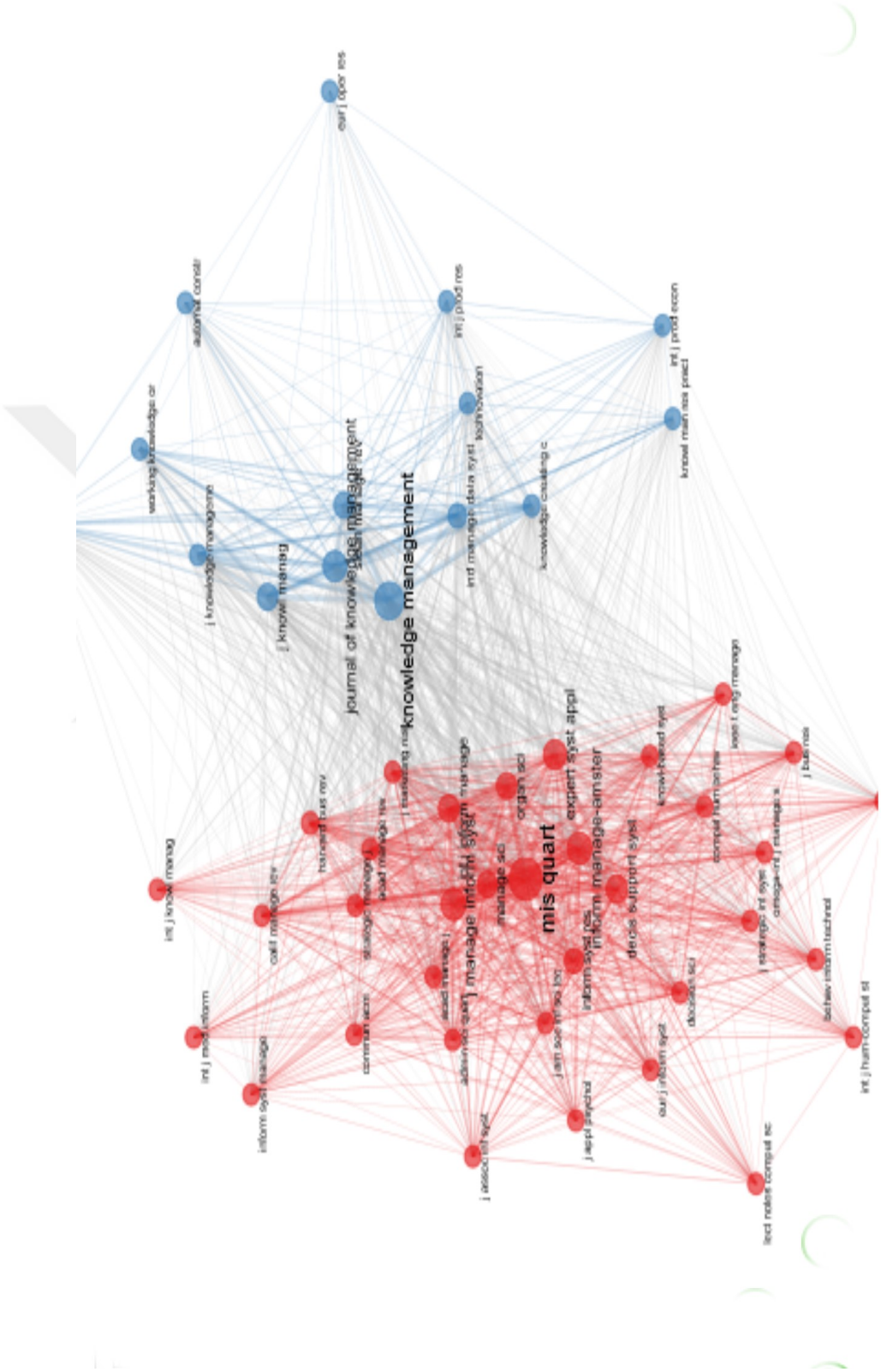
Japon bilim insanı Ikujiro Nonaka bilgi yönetimi konusunda uzmanlaşmıştır. Hitotsubashi Üniversitesi'nde çalışmaktadır. 2008 yılında Wall Street Journal iş dünyasında en etkili kişiler listesinde yer almıştır. Ayrıca The Economist dergisi de Yönetim Fikirleri ve Guruları Rehberine kendisini dahil etmiştir (https://en.wikipedia.org/wiki/Ikujiro_Nonaka).

Thomas H. Davenport analitik iş süreci yenilikleri, bilgi yönetimi ve yapay zeka konularında uzmanlaşmış Amerikalı bir akademisyen ve yazardır (https://en.wikipedia.org/wiki/Thomas_H._Davenport). Atreyi Kankanhalli ise bilgi sistemleri, çevrimiçi topluluklar, yapay zeka ve dijital dönüşüm konularında yayınlar yapan Singapur Ulusal Üniversitesinde görevli bir bilim insanıdır (https://www.comp.nus.edu.sg/disa/bio/atreyi/).

Şekil 7. Yazarlar Ortak Atıf Ağları



Şekil 8. Dergi Ortak Ağları



Şekilde görüleceği üzere MIS Quarterly en çok işbirliği yapan dergi durumundadır. Bu dergiyi sırası ile Inform Management ve Expert Systems ith Applications dergileri takip etmektedir. Bu dergiler kırmızı kmenin merkezinde yer almaktadırlar. Diğer küme olan mavi kümede Knowledge Management ve Journal of Knowledge Management dergileri merkezi konumadırlar.

4.11. Kelime Analizleri

Bu bölümde yayınlarda yer alan kelimelerle ilgili analizler yapılacaktır. En sık kullanılan kelimeler, anahtar kelimeler, başlıklar, özetler ve konu kategorileri olarak dört alt başlıkta incelenmiştir.

4.11.1. Anahtar Kelimelerde En Sık Kullanılan Kelimeler

Araştırma kapsamında incelenen 195 yayında anahtar kelimelerde en sık kullanılan kelimeler Tablo 15'de görülmektedir. En sık kullanılan ilk 10 kelime tabloya dahil edilmiştir.

Tablo 15. Anahtar Kelimelerde En Sık Kullanılan Kelimeler

Words	**Kelimeler**	**Yayın Sayısı**
Knowledge management	Bilgi yönetimi	88
Knowledge management system	Bilgi yönetim sistemi	47
Knowledge management systems	Bilgi yönetim sistemleri	18
Knowledge sharing	Bilgi paylaşımı	11
Knowledge	Bilgi	8
Ontology	Ontoloji	7
İnformation technology	Bilgi teknolojisi	5
Organizational culture	Organizasyon kültürü	5
Artificial intelligence	Yapay zeka	4
Case study	Vaka analizi	4

Tabloda görüleceği üzere anahtar kelime olarak en sık bilgi yönetimi kullanılmıştır (88 yayın). Bunu bilgi yönetim sistemi (47 yayın) ve bilgi yönetim sistemleri (18 yayın) takip etmiştir.

Şekil 9. Anahtar Kelimelerde En Sık Kullanılan Kelimeler Kelime Bulutu

4.11.2. Başlıklarda En Sık Kullanılan Kelimeler

Araştırma kapsamında incelenen 195 yayında başlıklarda en sık kullanılan kelimeler Tablo 16'da görülmektedir. En sık kullanılan ilk 10 kelime tabloya dahil edilmiştir.

Tablo 16. Başlıklarda En Sık Kullanılan Kelimeler

Words	**Kelimeler**	**Sayı (n)**
Knowledge	Bilgi	214
Management	Yönetim	197
System	Sistem	191
İmplementation	Uygulama	18
Performance	Verim	17
Design	Tasarım	15
Study	Ders çalışma	14
Development	Gelişim	13
Learning	Öğrenme	11
Model	Modeli	11

Tabloda görüleceği üzere başlıklarda en sık kullanılan kelime bilgi (n=214) olmuştur. Bunu yönetmek (n=197) ve sistem (n=191) kelimeleri izlemektedir. Başlık içinde aynı kelime birden çok kullanılabildiği için sayılar toplam yayın sayısından fazla çıkabilmektedir.

Şekil 10. Başlıklarda En Sık Kullanılan Kelimeler Kelime Bulutu

4.11.3. Özetlerde En Sık Kullanılan Kelimeler

Araştırma kapsamında incelenen 195 yayında özetlerde en sık kullanılan kelimeler Tablo 17'de görülmektedir. En sık kullanılan ilk 10 kelime tabloya dahil edilmiştir.

Tablo 17. Özetlerde En Sık Kullanılan Kelimeler

Words	Kelimeler	Sayı (n)
Knowledge	Bilgi	838
Management	Yönetim	467
System	Sistem	393
Kms	BYS	346
Km	BY	192
Study	Ders çalışma	191

İnformation	Bilgi	151
Research	Araştırma	148
Paper	Kağıt	134
Model	Model	131

Tabloda görüleceği üzere özetlerde en sık kullanılan kelime bilgi (n=838) olmuştur. Bunu yönetmek (n=467) ve sistem (n=393) kelimeleri izlemektedir. Başlık içinde aynı kelime birden çok kullanılabildiği için sayılar toplam yayın sayısından fazla çıkabilmektedir.

Şekil 11. Özetlerde En Sık Kullanılan Kelimeler Kelime Bulutu

4.11.4. Konu Kategorilerinde En Sık Kullanılan Kelimeler

Araştırma kapsamında incelenen 195 yayında konu kategorilerinde en sık kullanılan kelimeler Tablo 18'de görülmektedir. En sık kullanılan ilk 10 kelime tabloya dahil edilmiştir.

Tablo 18. Konu Kategorilerinde En Sık Kullanılan Kelimeler

Words	**Kelimeler**	**Sayı (n)**
Management	Yönetim	50
İnformation science & library science	Bilgi bilimi ve kütüphane bilimi	34
Computer science information systems	Bilgisayar bilimi bilgi sistemleri	27
Computer science artificial intelligence	Bilgisayar bilimi yapay zeka	22
Operations research & management science	Yöneylem araştırması ve yönetim bilimi	18
Computer science interdisciplinary applications	Bilgisayar bilimi disiplinler arası uygulamalar	17
Engineering electrical & electronic	Mühendislik elektrik ve elektronik	12
Engineering civil	Mühendislik inşaat	11
Engineering industrial	Mühendislik endüstriyel	11
engineering multidisciplinary	Mühendislik multidisipliner	10

Tabloda görüleceği üzere konu kategorilerinde en sık kullanılan kelime yönetmek (n=50) olmuştur. Bunu bilgi bilimi ve kütüphane bilimi (n=34) ve bilgisayar bilimi bilgi sistemleri (n=27) kelimeleri izlemektedir. Konu kategorisi birden çok seçilebileceği için sayılar toplam yayın sayısından fazla çıkabilmektedir.

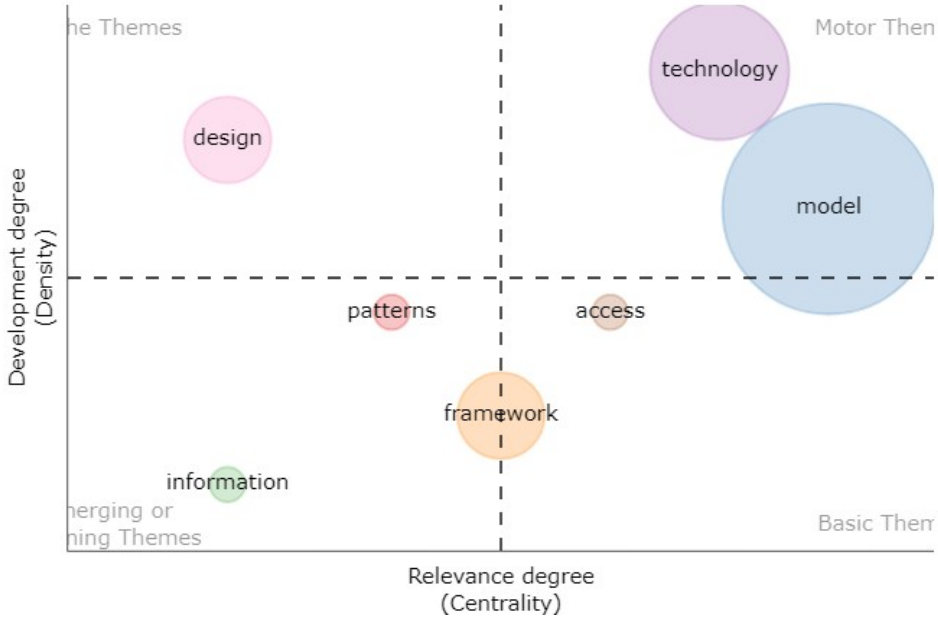
Şekil 12. Konu Kategorilerinde En Sık Kullanılan Kelimeler Kelime Bulutu

4.12. Tematik Evrim Analizi

Tematik evrim analizi incelenen yayınların içinde yer alan kavramların ilişkilerinin zamana bağlı olarak değişimini göstermektedir. Bu analiz kullanılarak alandaki gelişim gösterilebilmektedir (Seyhan, 2021, 622). Analizde yüksek seviyede ilgili anahtar kelimeler, en sık kullanıma sahip anahtar kelimeler tarafından tema kümelerini oluşturmaktadır (Kurutkan ve Terzi, 2022, 420).

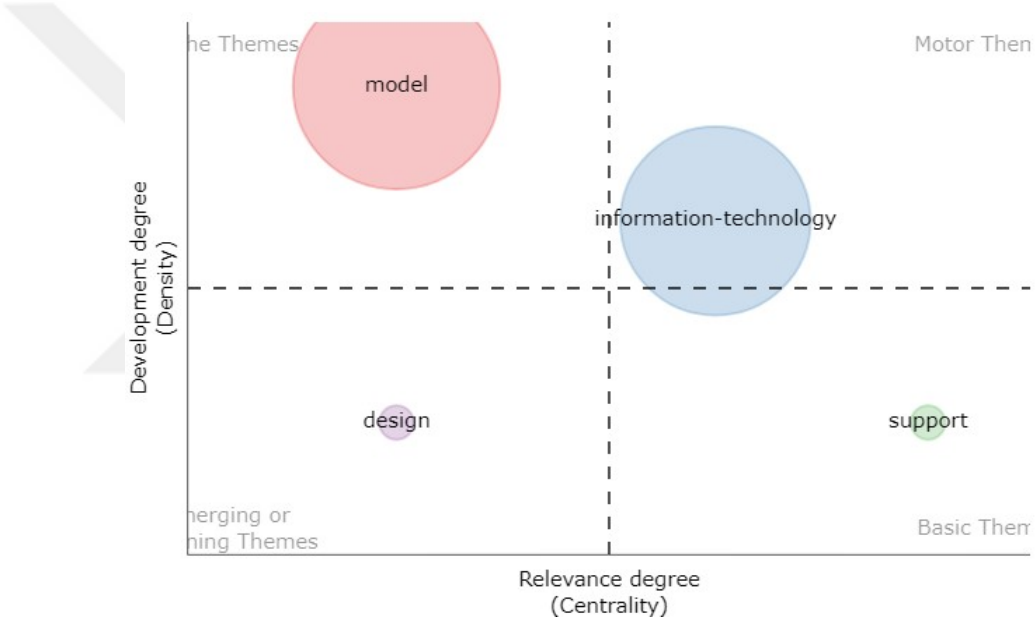
Tematik evrim haritalamasında dört alan görülmektedir. Sağ üst alan motor temalar olarak adlandırılmaktadır ve en gelişmiş, en merkezi ve en yoğun yayınların yer aldığı alandır. Sol üst alan niş temalar veya gelişmiş ve izole edilmiş temalar alanıdır. Bu alanda merkeziliği düşük ancak yoğunluğu yüksek temalar yer almaktadır. Sol alt alan kaybolan ya da gelişen temalar alanı olarak isimlendirilirken bu alanda düşük merkeziliğe ve yoğunluğa sahip temaları içermektedir. Sağ alt alanda merkeziliği yüksek ancak yoğunluğu düşük çeşitli disiplinler için paylaşılan temaların bulunduğu temel ve dönüşümsel temalar yer almaktadır (Karayel ve Kurutkan, 2022: 222). Analiz sonucunda 4 farklı tematik dönem ortaya konulmuştur.

Şekil 13. Birinci Zaman Dilimi (1993-2008) Tema Diyagramı



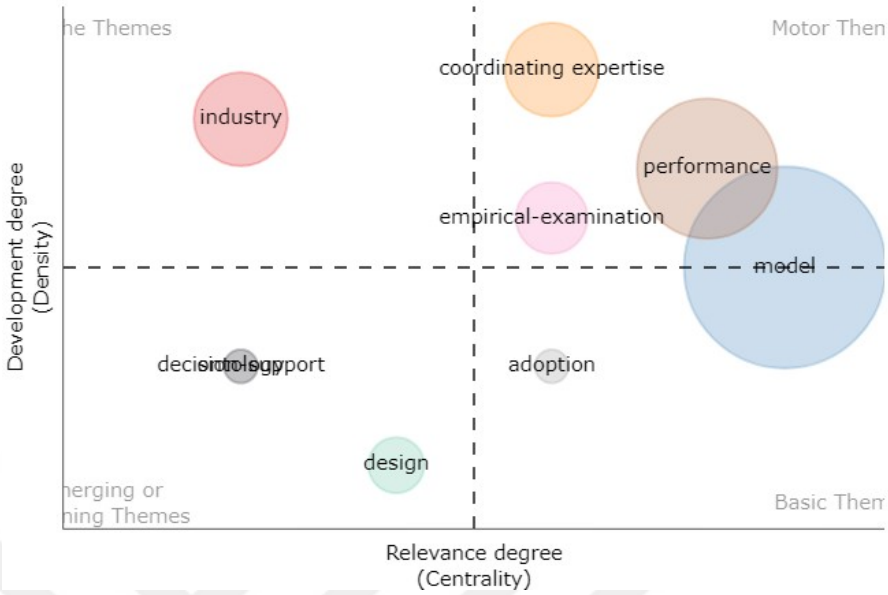
Birinci Dönem (1993-2008): Bu dönemde yedi küme ortaya çıkmıştır. Motor tema bölgesinde yer alan model teması en güçlü temadır. Aynı bölgede var olan technology (teknoloji) teması ikinci en güçlü temadır. “Design” (dizayn) teması niş temalar bölgesinde yer almaktadır. “Patterns” (desenler) ve “information” (bilgi) temaları gelişen temalar kısmında iken, “access” (erişim) teması) temel temalar bölümündedir. "Framework” (çerçeve) teması ise dikey ve yatay eksen üzerindedir. Sonuç olarak bu dönemde üzerinde en fazla çalışılan tema model teması olarak görülmektedir.

Şekil 14. İkinci Zaman Dilimi (2009-2013) Tema Diyagramı



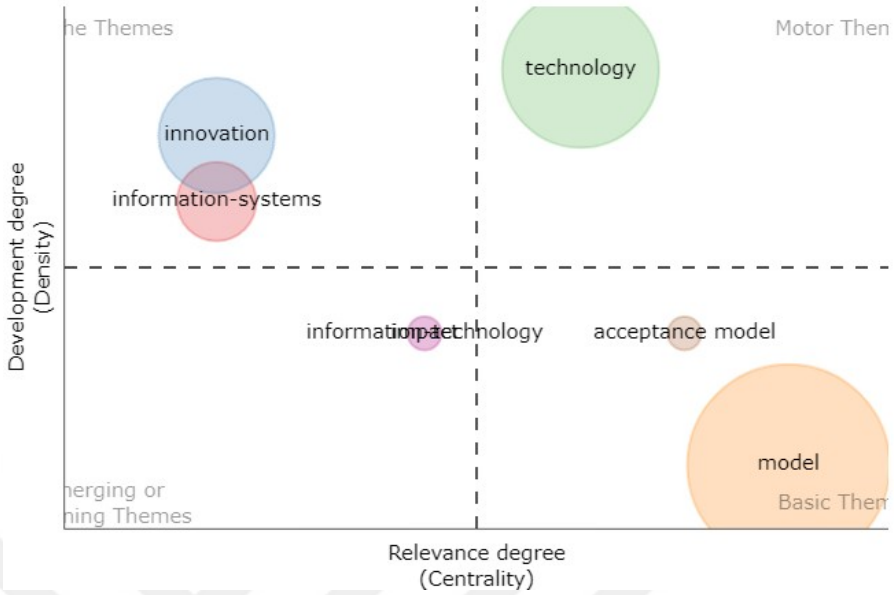
İkinci Dönem (2009-2013): Bu dönemde 4 küme görülmektedir. Güçlü ve izole iki öğeden biri olan “information-technology” (bilgi-teknoloji) motor tema alanında, “model” ise niş tema alanında yer almaktadır. Temel tema alanındaki “support” (destek) ve kaybolan ya da gelişen temalar alanındaki “design” (dizayn) daha zayıf temalar olarak görülmektedir.

Şekil 15. Üçüncü Zaman Dilimi (2014-2018) Tema Diyagramı



Üçüncü Dönem (2014-2018): Bu dönemde 8 tema görülmektedir. En güçlü tema olan "model" motor tema alanı ile temel tema alanı ortasında yer almakta ve ikinci güçlü tema olan "performance" (performans) ile motor tema alanında kesişim göstermektedir. "Coordinating expertise" (koordinasyon uzmanlığı) teması yine güçlü temalardan biri olup motor tema alanında yüksek yoğunlukta ve oldukça merkezi konumdadır. Motor tema alanındaki son tema "empirical-examination" (ampirik çalışmalar) temasıdır. "Industry" (endüstri" teması niş tema alanında güçlü ve izole bir tema olarak ortaya çıkmaktadır. "Design" (dizayn) teması bir önceki dönemdeki yerini korumakta ve "decision-support" (karar desteği) teması ile birlikte kaybolan ya da gelişen temalar bölgesinde yer almaktadır. Dizayn kaybolmaya başlayan bir tema olarak yorumlanabilirken karar desteği gelişen bir tema durumundadır.

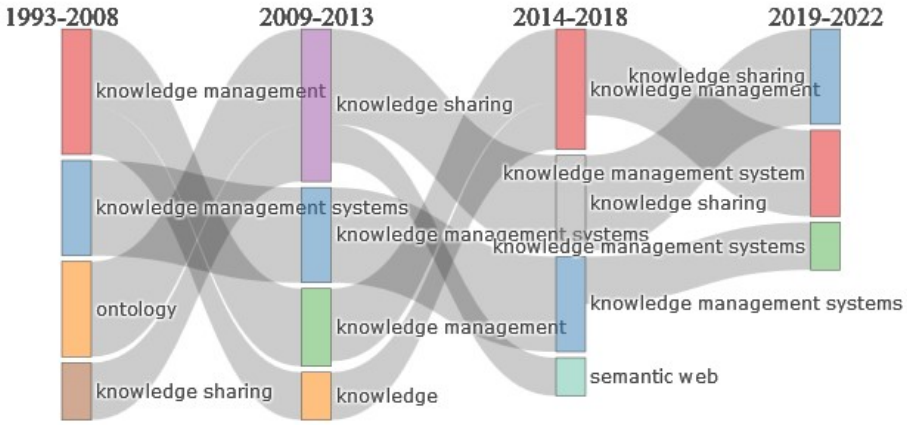
Şekil 16. Dördüncü Zaman Dilimi (2019-2022) Tema Diyagramı



Dördüncü Dönem (2019-2022): Bu dönemde 6 tema yer almaktadır. “Model” helan en güçlü ve izole tema olmakla birlikte motor tema bölgesinden temel tema bölgesine geçmiş görünmektedir. Motor tema bölgesindeki tek tema “technology” (teknoloji) teması güçlü ve izole bir tema olarak ortaya çıkmaktadır. Niş tema alanındaki “innovation” (yenilik) teması “information-systems” (bilgi-sistemler) teması ile kesişme halindedir. “Information-technology” (bilgi-teknoloji) teması kaybolan ya da gelişen temalar bölgesinde oldukça merkeze yakın bir konumdadır. “Acceptance model” (kabul modeli” teması da temel temalar alanında yer almaktadır.

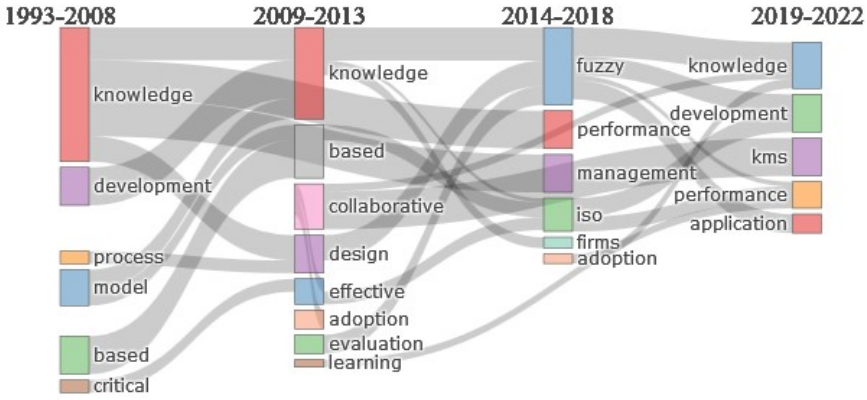
Tematik evrimin tüm zaman dilimlerini içeren haritası ise Şekil 16’da görülmektedir.

Şekil 17. Tematik Evrim Haritası (Anahtar Kelimelere Göre)



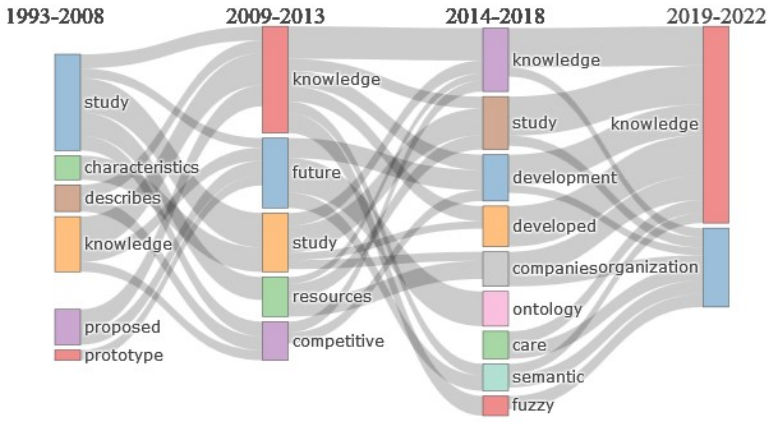
Tüm zaman dilimlerinde anahtar kelimelere göre inceleme yapıldığında bilgi yönetimi ve bilgi yönetimi kavramları her zaman en güçlü temalar arasında olmaya devam etmiştir. Ontoloji ve bilgi kelimeleri başlarda çok kullanılırken ilerleyen zamanlarda kullanımları azalmıştır.

Şekil 18. Tematik Evrim Haritası (Başlıklara Göre)



Tüm zaman dilimlerinde başlıklara göre kelimeler incelendiğinde bilgi kelimesi her dönemde en güçlü tema olmuştur. Model teması başlarda güçlü iken ilerleyen dönemlerde zayıflamıştır. Gelişim teması da başlarda güçlü olmuş, üçüncü dönemde bir miktar zayıflamış ama son dönemde gene öne çıkan bir temadır.

Şekil 19. Tematik Evrim Haritası (Özetlere Göre)



Tüm zaman dilimlerinde özetlere göre kelimeler incelendiğinde gene bilgi temasının her dönemde en güçlü tema olduğu görülmektedir. Çalışma teması ilk üç dönem güçlü iken son dönemde zayıflamıştır. Son dönemde bilgi temasının yanında organizasyon teması da güçlü tema haline gelmiştir.

BÖLÜM 5

5. SONUÇLAR VE ÖNERİLER

ISO 27001 ve Bilgi Yönetim Sistemi kavramları dünya çapında, uzun yıllardır akademik makalelerin ve bilim dünyasının konusu olmaktadır. Bilginin en önemli sermaye haline geldiği günümüzde korunması da bir o kadar önem arz etmektedir. Bilgiyi doğru yönetmek ve doğru korumak gerekmektedir. Bunu standardize etmek hata yapmanın önüne geçmenin en iyi yollarından biri olmaktadır. Tüm bu sebepler çalışma konusunun ne denli önemli olduğunu göstermektedir.

Bu tez çalışmasında, ISO 27001 ve Bilgi Yönetim Sistemi kavramlarının literatürdeki yeri geçmişten günümüze mercek altına alınmakta, alanın bibliyometrik analizi yapılarak literatüre katkıda bulunulmakta ve gelecekte oluşturulabilecek akademik çalışmalar için bir temel kaynak niteliği taşıması amaçlanmaktadır. Bu amaç doğrultusunda; Bu çalışmada, ISO 27001 ve Bilgi Yönetim Sistemi alanının geçmişten günümüze, bibliyometrik analiz, doküman analizi ve içerik analizi yöntemleriyle analiz edilmiştir.

ISO 27001 ve Bilgi Yönetim Sistemi alanlarında uluslararası yayınların analizi için R Studio ve Bibliometrix R paketi kullanılmıştır. Bu araçlar kullanılarak, Web Of Science dizininde toplam 195 dokümana erişilmiş ve analiz edilmiştir.

Bulgular incelendiğinde 25 dergide konu ile ilgili 2 ve daha fazla yapıldığı görülmüştür. Expert Systems with Applicatıons, International Journal of Computer Science and Network Security ve International Journal of Knowledge Management en çok yayın yapılan dergiler olarak karşımıza çıkmaktadır. Expert Systems with Applications dergisi toplam atıf sayısında da en önde yer alarak konu ile ilgili en etkili yayın olduğunu göstermektedir.

Elde edilen veriler neticesinde ISO 27001 ve Bilgi Yönetim Sistemi alanlarında WoS veri tabanlı yayınlar yıllara oranla analiz edildiğinde, 1995'den beri alanda hazırlanmış olan yayınlarda 2005 yılından sonra bir yükseliş trendi olduğu saptanmış ve en çok yayının 2016 yılında olduğu gözlemlenmiştir. Dolayısıyla alanın popülerliğinin ve araştırmacıların ISO 27001 ve Bilgi Yönetim Sistemi duydukları ilginin artış gösterdiği saptanmıştır. Yıl başına atıf sayıları da giderek artmaktadır. Bu konunun daha fazla gündem oluşturduğu şeklinde yorumlanabilir.

Çalışmadaki 195 yayın toplamda 563 yazar tarafından hazırlanmıştır. 36 makale tek yazarlı olarak yayına hazır hale gelmiştir. 159 makalede yazarlar işbirliği yapmışlardır. En çok yayın yapan yazarlar kim diye bakıldığında herhangi bir yazarın çok öne çıkmadığı görülmektedir. En fazla yayını olan 2 kişinin 5'er yayını mevcuttur.

ISO 27001 ve Bilgi Yönetim Sistemi WoS veri tabanında yapılan analiz sonucunda ülke düzeyinde ISO 27001 ve Bilgi Yönetim Sistemi araştırmalarının en çok Çin'de olduğu tespit edilmiştir. Bu durum, Çin'in ISO 27001 ve Bilgi Yönetim Sistemi alanlarında WoS veri tabanınca incelenen yayınlarda dünyada en önemli ülke konumunda oluşunun bir göstergesi olduğu şeklinde yorumlanabilir. Çin en çok atıf alan ülke sıralamasında da açık ara önde yer almaktadır.

En çok atıf yapılan yayının Lin TC ve Huang CC isimli yazarların Information & Management adlı dergide 2008 yılında yayınladıkları "Understanding knowledge management system usage antecedents: An integration of social cognitive theory and task technology fit" adlı yayın olduğu görülmektedir. Yazarlar en çok yayın yapan yazarlar listesinde 16 ve 20. sıralarda olmalarına karşın çok okunan ve en çok atıf alan makaleye imza atmışlardır.

Çalışma kapsamında incelenen makalelerde en çok katkı sağlayan kurumlar arasında Hong Kong Polytechnic Üniversitesi ve Malezya Putra Üniversitesi ilk sırada yer almaktadır. İlk 5 kurum arasında Uzak Doğu üniversitelerinin çoğunlukta olduğu dikkat çekmektedir.

Ortak atıf analizine bakıldığında konunun iş birliği yapılarak çalışmaya uygun olduğu görülmektedir. Yazarlar bazında da yayınlar bazında da çeşitli işbirliği ağları ve kümelerinin oluştuğu görülmektedir.

Kelime analizleri incelendiğinde yayınlarda anahtar kelimelerde en çok bilgi yönetimi kavramının kullanıldığı saptanmıştır. Bilgi kelimesi de başlıklarda en çok kullanılan kelime olmuştur. Aynı kelime özetlerde de en sık yer alan kelimedir. Konu kategorilerinde ise yönetim kelimesinin en çok kullanılan kelime olduğu görülmektedir.

Yayınların tematik evrimine bakıldığında model teması dört zaman diliminde de en güçlü tema olarak görülmektedir. Zaman içinde motor tema durumunda temel tema kısmına evrimleşmiştir. Aynı şekilde teknoloji teması da tüm zaman dilimlerinde kendine yer bulmuştur. Geçen sürede başlarda etkili olan bazı kavramlar daha sonra etkisini yetirmiştir. Dizayn teması buna örnek olarak verilebilmektedir.

Tüm bu veriler gelecekte konu ile ilgili çalışma yapmak isteyen kişilere önemli bilgiler vererek yol gösterici olabilecektir. Takip etmelerinde fayda olacak ülke, kurum dergi ve yazarlar konusunda fikir sahibi olmalarına yardım edecektir. İşbirliği yapılabilecek konu ve yazarları saptamalarında yararlanabileceklerdir.

Konu ile ilgili önerilerimiz aşağıdaki gibi sıralanabilir;

- Konu güncelliğini koruduğu hatta zaman içinde daha fazla ilgi gördüğü için çalışmalar artmalıdır.
- Çalışma olası işbirlikleri yönünden kaynak olarak kullanılabileceği için bu yönde yayınlar da artmalıdır.
- Ülkemizde de yazarlar kurumlar, dergiler konuya daha fazla ilgi göstermelidir.
- Konu hem kamu hem de özel sektör Ar-Ge çalışmalarında kendine daha fazla yer bulabilmelidir.
- Özellikle yazılım alanında en önemli sermayenin insan kaynağı olduğundan hareketle bu yönde eğitim faaliyetleri artarak devam etmelidir.

- Konu ile ilgili yeni çalışmalar yapılırken tematik evrim dikkate alınmalı, son dönemlerde güçlü olan temalar üzerinde odaklanılmalıdır. Tarama çalışmalarında da bu evrim mutlaka göz önünde bulundurulmalıdır. Bu noktada bilgi paylaşımı kavramı güncel ve öne çıkan bir başlık olduğu düşünüldüğünde bu konu üzerine çalışmaların arttırılması önerilmektedir.

BÖLÜM 6

KAYNAKÇA

Akay, İ.G., (2014), *Bilgi Güvenliği Yönetim Sistemleri: Bilgi Güvenliği Uygulama Mülakatları*, Yayınlanmamış Yüksek Lisans Tezi, Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü, Bilecik.

Alavi, M. ve Lediner, D., (1999), Knowledge Management Systems: Issues, Challenges, and Benefits, *Communications of the Association for Information Systems*: Cilt: 1, Sayı: 7, 1-37.

Altınpulluk, Ö. (2016), *ISO 27001: 2013 Bilgi Güvenliği Yönetim Sistemi Kurumsal Risk Yönetimi,* İstanbul: Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi.

Anı, N. A. (2018), *Kişisel Verilerin İşlenmesi ve Açık Rıza,* İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul.

Ateş, V. (2016), Bilişim Teknolojileri Risk Yönetimi ve Yöntemleri Üzerine Bir Değerlendirme, *3. Uluslararası Yönetim Bilişim Sis temleri Konferansı Bildiriler Kitabı*, 6-8 Ekim 2016, İzmir.

Aydın, İ. (2012), *Bilişim Sektörü ve Türkiye'nin Sektördeki Potansiyeli,* İstanbul: International Journal of New Trends in Arts, 1(1).

Bellardo, T., (1980), The use of co-citations to study science. *Library Research*, 2, 231- 237.

Bingöl, U. (2010), *ISO 27001 Bilgi Güvenliği Yönetim Sistemi Otomasyonu.* Sakarya: Sakarya Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.

Calder, A. (2006), *A Business Guide to Information Security*, Kogan Page Limited, Sterling\VA-ABD

Calder, A. (2016), *EU GDPR A Pocket Guide*, IT Governance Publishing, Cambridgeshire.

Chau, KW., (2007), An ontology-based knowledge management system for flow and water quality modeling, *Advances in Engineering Software*, Cilt: 30, Sayı: 3, 172-181.

Çekin, M. (2016), *6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) Ve İrade Serbestisi Açısından Değerlendirilmesi*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 74, Sayı 2.

Çelik, T. (2021), *Bilgi Güvenliği Yönetim Sistemlerinin Belgelendirilmesi: Batı Karadeniz'de Bir Alan Araştırması*, Yayınlanmamış Yüksek Lisans Tezi, Karabük Üniversitesi Lisansüstü Eğitim Enstitüsü, Karabük.

Çetinkaya, M. (2008), *Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi Maksatlı Araç,* İstanbul: Bahçeşehir Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi.

Çokmutlu, M. (2014), *Türk Ceza Hukukunda Kişisel Verilerin Korunması*, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Kocaeli.

Çubukçu, F. (2018), *Bilgi Güvenliği Yönetim Sistemi ISO 27001:2013 Uygulama Klavuzu*, Pusula Yayınları, İstanbul.

De Terwangne, C. (2014), *The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data*, International Review of Law, Computers & Technology, Cilt 28, Sayı 2.

Doğantimur, F. (2009), *ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği,* Ankara: Maliye Bakanlığı Strateji Geliştirme Daire Başkanlığı Mesleki Yeterlilik Tezi.

Drucker, P., (1994), *Kapitalist Ötesi Toplum*, Çev. Belkıs ÇORAKÇI, İnkılap Kitapevi, İstanbul.

Düzyol, G., (2011), *Türkiye Kütüphanecilik ve Bilgibilim Literatürünün Entellektüel Haritasının Çıkarılması: Bir Yazar Ortak Atıf Analizi Çalışması*, Yayınlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Elgesem, D. (1999). *The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data*, Ethics and Information Technology.

Erdoğan, Ş. E. (2020), *Bilgi Güvenliği Yönetim Sisteminin Oluşturulması, IEC / ISO 27001 Standardının Bir Sivil Havacılık Kurumunda Hayata Geçirilmesi,* İstanbul: İstanbul Kültür Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.

Ersoy, E. V. (2012), ISO/IEC 27001 *Bilgi Güvenliği Standartı Tanımlar ve Örnek Uygulamalar*, Odtü Yayıncılık Ankara.

Evrin, V. ve Demirer, M. (2011). *Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO / IEC – 27001 Örneği,* www.emo.org.tr

Fıkırkoca M., (2003), *Bütünsel Risk Yönetimi*, Birinci Basım, Pozitif Matbaacılık, Ankara.

Garfield, E., (1965), Can citation indexing be automated?, *Statistical Association Methods for Mechanized Documentation* (Nbs Misc. Pub. 269) içinde (s.189). Washington, D.C.: National Bureau of Standards.

Garfield, E. (1980). Bradford's Law and Related Statistical Patterns, *Essays of an Information Scientist*. 4:476-483.

Gencer, K. (2015). *ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım,* Afyon: Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi.

Gözüküçük, M. (2014), Veri işleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirilmesi, İstanbul Bilgi Üniversitei, Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul.

Gündoğan, B. (2016), Bilgi Sistemleri Denetiminde ISO/IEC 27001 ve ISO/IEC 27002 Standartlarının Yeri, *Muhasebe ve Denetim Dünyası*, 15-28.

Güner, O. ve Altuğ, A. (2019), *Protection of Personal Data in the European Union-turkey Relations: Effect of Visa Liberalisation Dialogue*, Yönetim ve Ekonomi Araştırmaları Dergisi, Cilt 17, Sayı 4.

Gürsel, E. ve Düğmeci, F. (2018), Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme, *R&S - Research Studies Anatolia Journal*, Cilt: 1, Sayı: 2, 318-329.

Henkoğlu, T. (2017), *Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme*, Arşiv Dünyası Dergisi, Sayı 17-18, 46-56.

https:// bilgiguvenligi,saglik,gov,tr, Erişim Tarihi: 20.11.2022.

https://www.comp.nus.edu.sg/disa/bio/atreyi/, Erişim Tarihi: 21.11.2022.

https://en.wikipedia.org/wiki/Ikujiro_Nonaka, Erişim Tarihi: 21.11.2022.

https://en.wikipedia.org/wiki/Thomas_H._Davenport, Erişim Tarihi: 21.11.2022.

https://www.marketingturkiye.com.tr/haberler/we-are-social-2022-verileri/, Erişim Tarihi: 20.11.2022

https://www.scheller.gatech.edu/directory/faculty/alavi/index.html, Erişim Tarihi: 21.11.2022.

Hung, Y., Huang, S., Lin, Q. ve -Tsai, M. (2005), Critical factors in adopting a knowledge management system for the pharmaceutical industry, *Industrial Management & Data Systems*, Cilt: 105, Sayı. 2, 164-183.

ISO, (2022), *ISO/IEC 27001 International Standart*, ISO Copyright Office, Cenevre.

Jouini, M., Rabai, LBA. ve Aissa, AB. (2014), Classification of Security Threats in Information Systems, *Procedia Computer Science* Sayı: 32, 489-496.

Kahraman, S. (2006), *Yönetimde Bilgi Güvenlik Sisteminin Yapısı, İşleyişi ve Aselsan A.Ş.'de Uygulaması,* Eskişehir: Anadolu Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.

Karagöz, D. ve Yüncü, H. R., (2013), Sosyal Ağ Analizi ile Turizm Alanında Yazılmış Doktora Tezlerinin Araştırma Konularının İncelenmesi, *Adıyaman Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 6(15): 205-232.

Karayel, T. ve Kurutkan, M.N., (2022), Covid 19 Sürecinde Yapay Zekâ ve Bileşenleri ile İlgili Yayınların Bibliyometrik Analizi, *Sağlık Akademisyenleri Dergisi*, Cilt: 9, Sayı: 3, 220-233.

Kılınç, D. (2012), *Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*, Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 61, Sayı 3.

King, WR. ve Marks PV. (2008), Motivating knowledge sharing through a knowledge management system, *Omega*, Cilt: 36, Sayı: 1, 131-146.

Koç, A. vd., (2022), *Bir Literatür İncelemesi Aracı Olarak Bibliyometrik Analiz*, Nobel Yayınları, İstanbul.

Korkmaz, İ. (2016), *Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme*, Türkiye Barolar Birliği Dergisi, Cilt 29, Sayı 124.

Korucu, O., (2021), *Veri Güvenliğinin İyileştirilmesi Sürecinde Risk Tabanlı Küresel Standart, Çerçeve ve En İyi Uygulama Yaklaşımları*, Yayınlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü, İstanbul.

Lee, S.M. ve Hong, S. (2002), "An enterprise-wide knowledge management system infrastructure", *Industrial Management & Data Systems*, Cilt: 102 Sayı: 1, 17-25.

Li, M., Jin, L. ve Wang, J., (2014), A new MCDM method combining QFD with TOPSIS for knowledge management system selection from the user's perspective in intuitionistic fuzzy environment, *Applied Soft Computing*, Sayı: 21, 28-37.

Lin, TC. ve Huang, CC., (2008). Understanding knowledge management system usage antecedents: An integration of social cognitive theory and task technology fit, *Information & Management*, Cilt: 45, Sayı: 6, 410-417.

Marttin, V. ve Pehlivan, İ. (2010), *ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme*, Mühendislik Bilimleri ve Tasarım Dergisi, 1(1), 49-56.

Memiş, T. (2017), *Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni*, Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 6.

Natek, S. ve Zwilling, M., (2014), Student data mining solution–knowledge management system related to higher education institutions, *Expert Systems with Applications*, Cilt: 41, Sayı: 14, 6400-6407.

Nonaka, I., (2000), *The Knowledge-Creating Company*, Harvard Business Review Press, Ne Yokr, ABDç

Öğüt, P. (2006), *Küreselleşen Dünyada Bilgi Güvenliğine Yönelik Politikalar: Sayısal İmza Teknolojisi ve Türkiye,* Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.

Pekmez, C. (2019), *Overview of the Definitons of Data Controller and Data Processor within the Scope of The Turkish Code of Personal Data Protection (TCDP)*, Annales de la Faculté de Droit d'Istanbul, Sayı 67.

Revere, D., Turner, A. M., Madhavan, A., Rambo, N., Bugni, P. F., Kimball, A., ve Fuller, S. S. (2007) Understanding the information needs of public health practitioners: a literature review to inform design of an interactive digital knowledge management system, *Journal of biomedical informatics*, Cilt: 40, Sayı: 4, 410-421.

Sağıroğlu, S., Ersoy, E. ve Alkan, M. (2007), *Bilgi Güvenliğinin Kurumsal Bazda Uygulanması,* Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı.

Santoro, G. vd (2018), The Internet of Things: Building a knowledge management system for open innovation and knowledge management capacity, *Technological Forecasting and Social Change*, Sayı: 136, 347-354.

Seyhan, M., (2021), Yönetsel Bağlamda Yeşil İnovasyonun Evriminin Bibliyometrik Analizi, *Journal of Socıal Sciences*, Cilt: 20, Sayı: 2, 611-625.

Shephard, B., (2002), Information security-who cares?, *2002 Fifth International Conference on Power System Management and Control Conf. Publ.* No. 488, 124-129.

Solmaz, E. (2019), *Avrupa İnsan Hakları Mahkemesi Kararları'nın "Kişisel Verilerin Korunması"na Katkısı*, İdare Hukuku ve İlimleri Dergisi, Cilt 18, Sayı 1.

Stewart, R.A. vd., (2010) Web-based knowledge management system: linking smart metering to the future of urban water planning, *Australian Planner*, Cilt: 47, Sayı: 2, 66-74.

Tikkinen-Piri, C., Rohunen, A. and Markkula, J. (2018), *EU General Data Protection Regulation: Changes and implications for personal data collecting companies*, Computer Law & Security Review, Cilt 34, Sayı 1.

Tipton H. and F, Krause M. (2008), *Information Security Management Handbook*, Auerbach Publicaions, Florida, ABD.

Thomson, KL., Solms, R. ve Louw, L., (2006), Cultivating an Organizational Information Security Culture, *Computer Fraud & Security*, October 2006, 7-11.

Vural, Y. ve Sağıroğlu, Ş., (2008), Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme, *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, Cilt 23, No 2, 507-522.

Yetkin, B., (2018), Siyasal İletişimin Dijital Propaganda Makineleri: Botlar, *Ata İlet Derg*i, Sayı: 16, 51-72.

Yılmaz, H. (2015). *TS ISO / IEC 27001 Bilgi Güvenliği Yönetim Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi,* KİDDER Denetişim Dergisi, Sayı: 15, 45-59..

Yücedağ, N. (2017), *Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı Ve Genel Hukuka Uygunluk Sebepleri*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 72, Sayı 2.

Zan, B.U., (2012), *Türkiye'de Bilim Dallarında Karşılaştırmalı Bibliyometrik Analiz Çalışması*, Yayımlanmamış Doktora Tezi. Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Zan, B.U., (2019), Doğrudan Atıf, Ortak Atıf ve Bibliyografik Eşleşme Yaklaşımlarına Dayalı Olarak Araştırma Alanlarının Değerlendirilmesi, *Sosyal Bilimler Araştırmaları Dergisi*, Cilt: 14, Sayı: 2, 501-516.

Zupic, I. ve Cater, T., (2015), Bibliometric methods in management and organization, *Organizational Research Methods*, Cilt: 18, Sayı: 3, 429-472.