VERİ UZAYI

Türkiye Bilişim Derneği
Veri Uzayı Raporu

Yayımcı Adı

TÜRKİYE BİLİŞİM DERNEĞİ
Ceyhun Atuf Kansu Cad., 1246 Sk. No: 4/17 Balgat – ANKARA
Tel: +90 (312) 473 8215 (pbx) Faks: +90 (312) 473 8216
tbd-merkez@tbd.org.tr

Yayın Tarihi

27 Kasım 2023, Ankara

Raporu Hazırlayanlar

TBD Ankara Şubesi KAMUBİB Çalışma Grubu

TBD Yayın Numarası: 2023 / 11-1

ISBN :
© Bu yayının herhangi bir kısmı veya tamamı Türkiye Bilişim Derneği'nden önceden yazılı ve onaylı izin alınmadan herhangi bir formda veya elektronik, mekanik, fotokopi kayıt veya diğer bir yöntemle tekrar çoğaltılabilir. Kaynak gösterilerek kullanılabilir.

Türkiye Bilişim Derneği

VERİ UZAYI RAPORU

Bilişim teknikbilimini ulusal bir kalkınma aracı olarak kullanacağız...

Aydın KÖKSAL, 1968
TBD Kurucusu ve Onursal Başkanı

İçindekiler

Tablo Listesi

Şekil Listesi

Kısaltmalar

2FA : İki Faktörlü Kimlik Doğrulama (Two-Factor Authenticator)

AB : Avrupa Birliği

AES : Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)

AFT : Amazon Fulfilment

AI : Yapay Zekâ (Artificial Intelligence)

ANN : Yapay Sinir Ağları (Artificial Neural Network)

ANSI : Amerikan Ulusal Standartlar Enstitüsü (American National Standards Institute)

API : Uygulama Programlama Arabirimi (Application Programming Interface)

APT : Advanced Persistent Threat

AR : Artırılmış gerçeklik (Augmented Reality)

B2C : Business to Consumer

BDDK : Bankacılık Düzenleme ve Denetleme Kurumu

BKM : Bankalararası Kart Merkezi

BT : Bilgi Teknolojileri

CDISC : Klinik Veri Standartları Değişim Konsorsiyumu (Clinical Data Interchange Standards Consortium)

CDR : Tüketici Veri Kanunu (Consumer Data Right)

CERT : Bilgisayar Acil Müdahale Ekipleri (Computer Emergency Response Team)

CSIRT : Bilgisayar Güvenliği Olay Müdahale Ekipleri (Computer Security Incident Response Team)

CSV : Virgülle Ayrılmış Değeler (Comma Separated Values)

CT : Bilgisayarlı Tomografi (Computed Tomography)

DBA : Database Administration

DeFi : Merkezi Olmayan Finans (Decentralized Finance)

DGA : Data Governance Act

DICOM : Tıpta Dijital Görüntüleme ve İletişim (Digital Imaging and Communication in Medicine)

DISP : Veri Aracılık Hizmet Sağlayıcıları (Data Intermediation Service Provider)

DNA : Deoksiriboz Nükleik Asit (Deoxyribonucleic Acid)

DOEap : Digitization of Energy Action Plan

DPO : Veri Güvenliği Yöneticisi (Data Policy Officer)

DSSC : Veri Uzayları Destek Merkezi (Data Spaces Support Centre)

EBA : Avrupa Bankacılık Otoritesi (European Banking Authority)

ECC : Eliptik eğri şifreleme, (Elliptic Curve Cryptography)

EDI : Elektronik Veri Paylaşımı (Electronic Data Interchange)

ELINT : Elektronik istihbarat (Electronic Intelligence)

ERP : Kurumsal Kaynak Planlama (Enterprise Resource Planning)

ESK : Elektronik Sağlık Kayıtları (Electronic Health Records-EHRs)

FAIR : Findable, Accessible, Interoperable and Reusable

FDA : Amerika Birleşik Devletleri Gıda ve İlaç Dairesi (The Food and Drug Administration)

FTP : Dosya Transfer Protokolü (File Transfer Protocol)

GDPR : General Data Protection Regulation

GPS : Global Positioning System

HDD : Sabit Disk Sürücüleri (Hard Disk Driver)

HKMA : Hong Kong Para Otoritesi (Hong Kong Monetary Authority)

HL7 : Yedinci Sağlık Seviyesi (Health Level Seven)

HPC : Yüksek Performanslı Bilgi İşlem (High-Performance Computing)

HTML : Hyper Text Markup Language

IMINT : Görüntü İstihbaratı (Image Intelligence)

INPS : Ulusal Sosyal Güvenlik Kurumu (National Institute for Social Security)

IoT : Nesnelerin İnterneti (Internet of Things)

JSON : Javascript Object Notation

KKB: : Kredi Kayıt Bürosu

KPI : Temel Performans Göstergesi (Key Performance ındicator)

KVKK : Kişisel Verileri Koruma Kanunu

M2M : Makineden Makineye (Machine to Machine)

ML : Makine Öğrenmesi (Machine Learning)

MDM : Mobil Cihaz Yönetimi (Mobile Device Management)

MRG : Manyetik Rezonans Görüntüleme

NEMA : Ulusal Elektrik Üreticileri Derneği (National Electrical Manufacturers Association)

NCI : Ulusal Kanser Enstitüsü (National Cancer Institute)

NHII : Ulusal Sağlık Bilgi Altyapısı (National Health Information Infrastructure)

NoSQL : Non-Structured Query Language

OBIE : Açık Bankacılık Uygulama Kurumu (Open Banking Limited)

ÖHVPS : Ödeme Hizmetleri Veri Paylaşım Servisleri

PACS : Tıbbi Görüntü Arşivleme ve İletişim Sistemleri (Picture Archiving and Communication System)

PDF : Portable Document Fomat

PET : Pozitron Emisyonu Tomografi (Positron Emission Tomography)

PSD : Ödeme Hizmet Yönergesi (Payment Services Directive)

ROI : Yatırım Getirisi (Return On Investment)

RCRIM : Düzenlenmiş Klinik Araştırma Bilgi Yönetimi (Regulated Clinical Research Information Management)

SAN : Depolama Alanı Ağları (Storage Area Network)

SDO : Akredite Standartlar Geliştirme Kuruluşu (Standards Development Organizations)

SGML : Standart Genelleştirilmiş Biçimlendirme Dili (Standard Generalized Markup Language)

SIGINT : Sinyal İstihbaratı (Signals Intelligence)

SPECT : Tek Foton Işınımı Yapan Bilgisayarlı Tomografi (Single-Photon Emission Computed Tomography)

SQL : Yapılandırılmış Sorgu Dili (Structured Query Language)

SSD : Katı Hal Sürücüleri (Solid State Driver)

SSO : Tek Oturum Açma (Single Sign-On)

SWD : Personel Çalışma Belgesi, Staff Working Document

TBB : Türkiye Bankalar Birliği

TBD : Türkiye Bilişim Derneği

TCMB : Türkiye Cumhuriyet Merkez Bankası

TED : Tenders Electronic Daily

TÜİK : Türkiye İstatistik Kurumu

VPN : Sanal Özel Ağ (Virtual Private Network)

VR : Sanal Gerçeklik (Virtual Reality)

XML : Genişletilebilir İşaretleme Dili, (Extensible Markup Language)

Çalışma Grubu

Bu rapor, Türkiye Bilişim Derneği çatısı altında kurulan Veri Uzayı Çalışma Grubu tarafından hazırlanmıştır.

Başkan

Dirsehan TUNÇEL	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

Başkan Yardımcısı

Özgür YILMAZ	N2Mobil

Grup Üyeleri

Aslıhan Kart	Kart Avukatlık Bürosu
Betül Yılmaz	Sağlık Bakanlığı
Mehmet Çağlar Ünsal	Maden Tetkik ve Arama Genel Müdürlüğü
Hande Eryılmaz	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
İbrahim Alşan	Enerji Bakanlığı
Melih Aşıcı	Mikroarea Digital & Creative
Nergiz Çağıltay	Çankaya Üniversitesi
Sezen Aşıcı	Kürekçi Hukuk ve Danışmanlık
Tamer Ute	Savronik
Taner Kaya	Ziraat Bankası
Veysel Sevim	Ulaştırma ve Altyapı Bakanlığı

1 Önsöz

Bu raporun amacı, Avrupa Birliği uygulamaları ile uyumlu ve dünya ile her alanda entegre bir Türkiye için karar vericilere ışık tutmaktır. Güncel teknolojik gelişmeler, verinin yönetimini ve paylaşımını uluslararası ticaretin merkezine almış durumdadır. Türkiye'nin küresel pazardaki rekabetçiliğini sürdürmesi ve büyütebilmesi için veri uzayı alanında standartlarını tanımlaması ve kurallarını işler hale getirmesi kaçınılmaz bir gerekliliktir. Bu doğrultuda, Türkiye Bilişim Derneği (TBD) bünyesinde oluşturulan **Veri Uzayı Çalışma Grubu**, hazırlamış olduğu bu rapor ile yol gösterici bir rehber sunmayı hedeflemiştir.

Bu raporda, günümüzün güncel ve kritik öneme sahip meselesi olan Veri Uzayı konusu ele alınmıştır. Çalışma grubu, farklı alanlarda faaliyet gösteren gönüllülerin katılımı prensibiyle bir araya gelmiş ve çalışmalarını titizlikle yürütmüştür. Raporun hazırlığı, her bir üyenin katkılarıyla tamamlanmış ve bu süreç, işbu belgenin sunumuyla taçlandırılmıştır.

Uluslararası ticarette etkin bir oyuncu olan Türkiye için, küresel ekonominin dinamiklerini şekillendiren bu alanda, temel kuralları oluşturmak, öncelikli bir gereksinimdir. Rekabetçiliğimizin sürdürülebilmesi ve artırılması adına bu alandaki teknolojik ve regülatif hazırlıkların tamamlanması önemli adımdır.

Veri Uzayı'nda etkin olabilmek için, bilişim altyapısının en son teknolojilere uygun olarak güncellenmesi gerekmektedir. Büyük veri, yapay zeka, bulut teknolojileri ve siber güvenlik gibi alanlarda yapılan yatırımlar, Türkiye'yi bu alanda rekabetçi kılacaktır. Bununla birlikte veri uzayının etkin bir şekilde yönetilmesi için gerekli olan yasal ve düzenleyici çerçeve, mevcut uluslararası standartlarla uyumlu olmalıdır. Avrupa Birliği uygulamalarına uyum sağlamak, bu anlamda temel bir adımdır. Ayrıca, veri mahremiyeti ve güvenliği konularında uluslararası normlara uygun düzenlemeler yapılmalıdır.

Bu çalışmanın ülkemize büyük faydalar sağlayacağını düşüncesiyle, katkıları için Veri Uzayı Çalışma Grubu'nun değerli üyelerine teşekkürlerimizi sunarız.

Dirsehan TUNÇEL & Özgür YILMAZ

2 Giriş

Dijitalleşme, 21. yüzyılın başından itibaren hayatımızın hemen her alanında derinlemesine etkisini göstermeye başladı. Analog dünyadan dijital bir gerçekliğe geçiş, sadece teknolojik araçları ve platformları değil, aynı zamanda yaşam tarzımızı, iş yapış şekillerimizi ve toplumsal etkileşimlerimizi kökten dönüştürdü. Ancak bu dönüşümün arkasındaki en önemli itici güç, şüphesiz ki 'veri' oldu.

Veri, dijitalleşmenin doğal bir sonucu olarak ortaya çıktı. Her tıklama, her paylaşım, her çevrimiçi etkileşim; sadece bireysel tercihlerimizi ve davranışlarımızı değil, aynı zamanda sosyal, ekonomik ve politik trendleri de yansıtan devasa bir veri havuzunun parçası haline geldi. Bu hızla büyüyen veri setleri, iş dünyasından kamu hizmetlerine, sağlıktan eğitime kadar pek çok sektörde dijital dönüşümün anahtarı olarak görülmeye başlandı.

Dijital dönüşüm, temelde bir teknoloji dönüşümü olmasına rağmen, asıl gücünü bu veriden alıyor. Çünkü veri, şirketlerin tüketici davranışlarını daha iyi anlamasını, kamu hizmetlerinin vatandaş ihtiyaçlarına daha hızlı yanıt vermesini, sağlık sektörünün daha kişiselleştirilmiş tedavi yöntemleri geliştirmesini ve eğitimde daha etkili öğrenme yaklaşımları oluşturmasını mümkün kılıyor.

Önümüzdeki yıllarda, dijitalleşmenin ve verinin getirdiği bu dönüşümün ivmesi daha da artacak. Nesnelerin interneti, yapay zeka, makine öğrenimi ve derin öğrenme gibi teknolojiler, veriyi daha anlamlı ve işlevsel hale getirerek, hayatımızın daha da dijitalleşmesine yol açmaya başladı bile. Bu, sadece teknolojik bir ilerleme değil, aynı zamanda sosyal ve kültürel bir evrimin de habercisi. Dijitalleşme ve veri, modern çağın iki temel sütunu olarak karşımıza çıkıyor. Bir yandan bizi bilinmeyen bir geleceğe doğru sürüklüyorlar, diğer yandan da bu geleceği şekillendirme gücünü elimize veriyorlar. Bu yeni dönemin ne getireceğini tam olarak bilmesek de, verinin merkezinde olduğu bir dijital dönüşümün, bireyler ve toplumlar için sınırsız olanaklar barındırdığı kesin. Bu potansiyeli en iyi şekilde değerlendirme sorumluluğu ise hepimize düşüyor.

2.1 Yapay Zeka Gelecekse, Veri Yeni Petrol mü?

Günümüzde sıkça duymaya başladığımız bu ifade, günümüz endüstrilerini güçlendiren petrolün rolü ile geleceği biçimlendirecek Yapay Zeka uygulamaları ve endüstriyel dönüşümün ateşleyicisi olan verinin rolü arasında mecazi bir karşılaştırma yapmaktadır. Petrol, kullanıldığında tükenirken, veri doğru kullanıldığında değerini artırabilir ve sonsuz potansiyele sahiptir. Bu, ulusal ekonomiler için benzersiz fırsatlar sunar.

Önümüzdeki yıllarda Yapay Zeka, endüstriyel dönüşümün merkezinde yer alacak ve gündelik yaşamın hemen hemen her yönünde köklü değişikliklere neden olacaktır. Sağlık sektöründen eğitime, ulaşımdan enerjiye kadar birçok alanda, Yapay Zeka'nın teşhislerin daha doğru konulmasından, öğrencilere birey özelinde eğitim sunmaya, trafik akışını optimize etmekten enerji tüketimini azaltmaya kadar birçok alanda devrim yaratması bekleniyor. Ancak Yapay Zeka'nın bu potansiyelinin tam olarak kullanılabilmesi için, kurumların etik standartları, veri güvenliğini ve çalışanların yeni teknolojilere adaptasyonunu dikkate alarak stratejik yatırımlar yapmaları gerekmektedir.

Ham petrolün değerli ürünleri çıkarmak için rafinasyona ihtiyaç duyması gibi, ham verinin anlamlı içgörüler elde etmek için işlenmesi gerekmektedir. Petrol, ekonomileri, jeopolitik

stratejileri ve hatta savaşları yönlendirmiştir. Benzer şekilde, veri, bugünün dijital çağında büyük bir değere sahiptir. Şirketler, hükümetler ve kurumlar, kararlar almak, içgörü elde etmek ve kişiselleştirilmiş deneyimler oluşturmak için veri toplar, analiz eder ve kullanır. Petrolün dünya genelinde pek çok bölgede bulunuyor ve kullanılıyor olması gibi, veri de önceden görülmemiş oranlarda global olarak üretilmekte ve tüketilmektedir. Petrol üzerindeki kontrol, geçen yüzyılda önemli bir güç ve etkiye yol açmıştır. Benzer şekilde, veri üzerindeki kontrol ve hakimiyet, şirketler için önemli rekabet avantajlarına ve uluslar için stratejik avantajlara yol açabilir.

Kişisel verinin, veri odaklı ürün üreten veya hizmet veren alanlarda yoğun surette kullanıldığı günümüzde, bir yandan General Data Protection Regulation (“GDPR” - Avrupa Genel Veri Koruma Tüzüğü) gibi etki alanı dünya çapında olan düzenlemeler ve uyum sürecindeki ulusal düzenlemeler ile kişisel veri koruma sistemi oluşturulurken; ortaya çıkan gelişmeler, büyük veri mefhumunun yalnızca kişisel veri mevzuatına sıkışıp kalamayacağını, kişi temel hak ve özgürlüklerinin ötesinde rıza sorunları, teknolojik gelişme hızı, dijitalleşme ile birlikte bireylerin her geçen gün daha çok verisinin işlendiği hususları ve bu hususların piyasada yarattığı hakim durum oluşturucu veya mevcut durumu güçlendirici etkileri nedeniyle büyük veri başka bir alana sürüklenmektedir. Bunun da yalnızca güvenlik ve veri koruma alanında değil, rekabet piyasası alanında da sorunlar doğurduğu[1] ifade edilmelidir.

Bununla birlikte, Avrupa Komisyonu Başkanı Ursula von der Leyen, Avrupa'nın "yüksek gizlilik, güvenlik, emniyet ve etik standartları koruyarak veri akışını ve kullanımını dengelemesi gerektiğini" belirtmiştir. Avrupa Veri Stratejisi, veri için tek pazar oluşturmayı ve Avrupa'yı veri ekonomisinde küresel bir lider yapmayı hedeflemektedir. Bu bağlamda, Avrupa Birliği açısından bölgesel bir strateji olarak ortaya çıkan Veri Yasası (Data Act), farklı sektörler arasında yatay veri paylaşımını teşvik etmek ve veri erişimi ve kullanımı için sektörler arası bir yönetişim çerçevesi oluşturmak için önemli bir adım niteliğindedir.

Avrupa Veri Yasası (European Data Act) ve Avrupa Veri Yönetişim Yasası (European Data Governance Act), veriye olan güveni sağlamak için önemli düzenlemeler içeren yasalardır. Avrupa Veri Yasası, kişisel verilerin işlenmesi, saklanması ve aktarılması gibi konularda şeffaflığı ve güveni artırmayı amaçlarken, Avrupa Veri Yönetişim Yasası, veri yönetim süreçlerini ve veri kullanımını düzenlemeye odaklanarak veriye olan güveni güçlendirmeyi hedefler. Her iki yasa da Avrupa'da veri işleme süreçlerini daha şeffaf ve güvenilir hale getirmeyi ve veriye olan güveni artırmayı, buna bağlı olarak da veri paylaşımını arttırmayı amaçlamaktadır.

Avrupa Veri Yönetişim Yasası, örneğin verilerin kamu kurumlarınca (birbirleri ile paylaşılırken) yeniden kullanımı (re-use) halinde korunması ile ilgili olarak şu şartlarda bir koruma sağlanması gerektiğini öngörmektedir: Kişisel veriler söz konusu ise anonimleştirilmelidir. Ticari sırlar veya fikri mülkiyet haklarıyla korunan içerik dahil olmak üzere ticari açıdan gizli bilgiler söz konusu olduğunda bunlar değiştirme/ bir araya getirme/ başka herhangi bir ifşa kontrolü yöntemiyle ele alınmalıdır. Kamu kuruluşu tarafından sağlanan veya kontrol edilen güvenli bir işleme ortamında verilere uzaktan erişmek ve yeniden kullanmak yetkisi tanınabilir. Üçüncü kişilerin hak ve menfaatlerini tehlikeye atmadan, uzaktan erişime izin verilmemek

[1] Ketizmen Muammer - Kart Aslıhan. Kişisel veri ve rekabet hukuku kapsamında “Big data”. Kişisel Verileri Koruma Dergisi. 2019; 1(1): 64-76.

kaydıyla, yüksek güvenlik standartlarına uygun olarak güvenli işleme ortamının bulunduğu fiziki tesislerdeki verilere erişmek ve yeniden kullanmak gerekmektedir.

Türkiye'de AB Veri Yönetişim Yasası muadili sayılabilecek bir düzenleme bulunmamaktadır. Ancak, Türkiye'de 6698 Kişisel Verileri Koruma Kanunu, 18 Ocak 2016'da tasarı olarak meclise girmiş ve 24 Mart 2016 tarihinde kabul edilmiştir. 7 Nisan 2016 tarihinde ise 6698 sayılı kanun olarak 29677 sayılı Resmî Gazete' de yayımlanmış ve sonrasında yürürlüğe girmiştir.

2.2 Ulusal Veri Stratejisinin Oluşturulması Neden Önemlidir?

Veri, modern ekonomilerin itici gücü olmaya başlamıştır. Verinin ekonomik potansiyeli, bir ülkenin rekabetçilik seviyesini doğrudan etkileyebilir. Veriye dayalı karar verme, işletmeler için ürün ve hizmetlerin iyileştirilmesi, pazar trendlerinin öngörülmesi ve müşteri ihtiyaçlarına daha etkili yanıt verilmesi gibi avantajlar sunar. Ulusal veri stratejisi, bu potansiyeli ülke veya bölge çapında en üst düzeye çıkarmak için gerekli olan çerçeveyi oluşturmayı amaçlar.

Ekonomik faydaların ötesinde, ulusal bir veri stratejisinin toplumsal ve politik boyutları da vardır. Bireylerin veri hakları ve gizliliği, demokratik toplumların temel taşlarından biridir. Bu hakların korunması, vatandaşların dijital hizmetlere güven duymasını ve bu hizmetleri kullanmasını sağlar. Ulusal bir veri stratejisi, bu hakların korunmasını ve bireylerin kontrolünü güvence altına alarak, dijital ekosistemde güvenli bir ortam yaratılmasına katkıda bulunabilir.

Ulusal bir veri stratejisi aynı zamanda, veri bilimi ve yapay zeka gibi alanlarda yetenek geliştirmek için eğitim ve araştırma programlarını destekleyerek bir ülkenin teknolojik kapasitesini artırabilir. Bu, ulusal inovasyon ekosistemini güçlendirirken, genç neslin geleceğin mesleklerine hazırlanmasına da yardımcı olur.

Dünya genelinde, veri sınırlarını aşan küresel bir varlık haline gelmiştir. Bu nedenle, veri stratejileri ulusal sınırların ötesine geçmelidir. Ulusal bir strateji, ülkelerin uluslararası normlarla ve en iyi uygulamalarla uyum içinde olmasını sağlar, bu da uluslararası işbirliğini teşvik eder ve veri tabanlı çözümlerin benimsenmesini kolaylaştırır.

Sonuç olarak, ulusal bir veri stratejisi, ekonomik büyüme, toplumsal kalkınma ve politik istikrar için kritik bir öneme sahiptir. Bu strateji, verinin ekonomik potansiyelini en üst düzeye çıkarmak, bireylerin haklarını korumak, teknolojik kapasiteyi artırmak ve uluslararası işbirliğini teşvik etmek için gereklidir. Bu, bir ülkenin sürdürülebilir ve kapsayıcı bir dijital dönüşümü başarıyla gerçekleştirmesine yardımcı olacaktır.

2.3 Ulusal Veri Stratejisi Amaçları

Ulusal veri stratejisinin temel amacı, bir ülkenin veri kaynaklarını, yeteneklerini ve teknolojik altyapısını etkin bir şekilde kullanarak sosyal, ekonomik ve teknolojik kalkınma için sürdürülebilir bir temel oluşturmaktır. Bu amaç doğrultusunda, ulusal veri stratejileri genellikle aşağıdaki hedeflere yöneliktir:

Entegrasyon ve Erişilebilirlik: Farklı kaynaklardan gelen verinin birleştirilmesi ve erişilebilir hale getirilmesiyle, bilgiye dayalı karar alma süreçlerini desteklemek.

Veri Kalitesini Artırma: Doğru, güncel ve tutarlı veri sağlama üzerine odaklanarak, veri kullanıcıları için güvenilir bir kaynak oluşturma.

Veri Güvenliği ve Gizliliği: Kişisel veri koruma, siber güvenlik ve gizlilik standartları oluşturarak bireylerin ve kurumların haklarını koruma.

Inovasyonu Teşvik Etme: Veriye dayalı araştırma ve geliştirmeyi destekleyerek yeni iş modelleri, hizmetler ve ürünlerin ortaya çıkmasını teşvik etme.

Kapasite ve Yetenek Geliştirme: Veri bilimi, analitiği ve ilgili alanlarda eğitim programları ve fırsatları oluşturarak ulusal yetenek havuzunu genişletme.

Açık Veri İlkelerini Benimseme: Kamu verisinin açık ve şeffaf bir şekilde paylaşılmasını teşvik ederek, ekonomik fırsatları ve sivil katılımı artırma.

Uyumlu Düzenlemeler: Uluslararası standartlar ve en iyi uygulamalarla uyumlu yasal ve düzenleyici bir çerçeve oluşturma.

Veri Tabanlı Politika Oluşturma: Kamu politikalarını ve stratejilerini veriye dayalı bilgilerle şekillendirerek, daha etkili ve etkin yönetişim sağlama.

Uluslararası İşbirliği: Ulusal sınırların ötesinde veri paylaşımı ve işbirliğini teşvik ederek, global veri ekonomisine entegrasyonu hızlandırma.

Toplumsal Farkındalık: Kamuoyunu, verinin önemine, kullanımına ve potansiyel risklerine dair bilgilendirme ve eğitme.

Ulusal veri stratejisinin bu hedefleri, ülkenin sosyal, ekonomik ve teknolojik kalkınma hedefleriyle paralel olarak belirlenir ve düzenli olarak gözden geçirilmelidir.

2.4 Ulusal Veri Ekosisteminin Veri Stratejisi Açısından Önemi

Veri ekosistemi, veri üretimi, toplama, depolama, işleme, analiz, paylaşım ve kullanım süreçlerinin bütününü kapsayan bir yapıyı ifade eder. Bu ekosistem, farklı aktörleri (kamu kurumları, özel sektör, sivil toplum, bireyler vb.), teknolojileri, politikaları ve düzenlemeleri bir araya getirir. Ulusal veri stratejisi, bir ülkenin veri potansiyelini tam anlamıyla değerlendirebilmesi için sağlam bir veri ekosistemine ihtiyaç duyar.

2.4.1 Ulusal Veri Ekosisteminin Temel Bileşenleri Nelerdir?

Ulusal veya bölgesel bir veri ekosisteminin etkili ve sürdürülebilir olabilmesi için belirli temel bileşenlere ihtiyaç vardır. Bu bileşenler aşağıdaki gibi özetlenebilir:

Veri Altyapısı: Veri depolama, işleme ve iletim kapasitesine sahip güçlü ve güvenilir bir altyapı gereklidir. Bu, veri merkezlerinden bulut hizmetlerine, geniş bant erişiminden hızlı veri iletim ağlarına kadar geniş bir yelpazeyi kapsar.

Standartlar ve Protokoller: Veri entegrasyonunu ve işbirliğini kolaylaştırmak için ulusal veya bölgesel düzeyde standartlaştırılmış veri formatları, protokoller ve arayüzlerin oluşturulması esastır.

Veri Paylaşımı ve Erişim Politikaları: Veriye erişim ve paylaşımı teşvik eden, aynı zamanda gizlilik ve güvenlik endişelerini dikkate alan politikalara ihtiyaç vardır.

Veri Güvenliği ve Gizlilik: Veri ihlallerini önlemek ve kullanıcıların gizliliğini korumak için güçlü güvenlik protokolleri ve şifreleme yöntemleri gereklidir.

Kalite ve Doğrulama: Verinin doğruluğunu ve güvenilirliğini sağlamak için kalite kontrol ve doğrulama süreçleri önemlidir.

Yetenek Geliştirme: Ekosistemin tüm bileşenleriyle etkili bir şekilde çalışabilmek için gerekli beceri ve bilgiye sahip bireylerin ve kurumların yetiştirilmesi gereklidir.

Yasal ve Düzenleyici Çerçeve: Veri koruma, fikri mülkiyet, erişim hakları ve diğer konuları düzenleyen yasal bir çerçevenin oluşturulması gereklidir.

Kullanıcı Arayüzleri ve Araçlar: Son kullanıcılara, veriyi kolayca anlamalarını ve kullanmalarını sağlayan araçlar ve platformlar sağlanmalıdır.

Ortaklık ve İşbirlikleri: Kamu ve özel sektör arasında, ayrıca farklı sektörler ve disiplinler arasında işbirliği ve ortaklık yapılanmaları teşvik edilmelidir.

Topluluk ve Ağ Oluşturma: Veri ekosisteminin sürdürülebilirliğini ve etkinliğini artırmak için, bu alanda çalışan profesyoneller, araştırmacılar, geliştiriciler ve diğer ilgili taraflar arasında ağlar ve topluluklar oluşturulmalıdır.

Kamuoyu Bilgilendirme ve Katılım: Genel halkın, veri ekosisteminin amaçlarına, faydalarına ve potansiyel risklerine dair bilgilendirilmesi ve katılımının teşvik edilmesi önemlidir.

Inovasyon ve Araştırma: Sürekli gelişim ve adaptasyon için, veri ile ilgili yenilikçi çözümler ve araştırmaları teşvik eden programlar ve inisiyatifler olmalıdır.

Bu bileşenler, bir ulusal veya bölgesel veri ekosisteminin temel taşlarını oluşturur. Ancak, her ülkenin veya bölgenin kendi özel ihtiyaçlarına ve koşullarına uygun şekilde bu bileşenleri uyarlaması ve özelleştirmesi gerekmektedir.

2.4.2 Ulusal Ortak Veri Uzayı

Ortak Veri Uzayı (Common Data Space) bir veri altyapısı veya çerçevesidir ki bu, farklı kaynaklardan gelen veriyi standardize, organize ve erişilebilir hale getirmeyi amaçlar. Bu altyapı, belirli standartlara, protokollere ve araçlara dayanır ve verinin paylaşımını, erişimini ve tekrar kullanımını kolaylaştırır. Ortak veri alanları genellikle belirli bir endüstri, sektör veya hizmetle ilgili olabilir ve bu alanların oluşturulması, genellikle verinin etkin bir şekilde yönetilmesi ve kullanılması için bir ön koşuldur.

Ulusal veri stratejisinin hayata geçirilmesi aşamasında, Ortak Veri Alanlarının birkaç önemli rolü vardır:

Rekabetçilik ve İnovasyon: Ortak Veri Uzayı, kurumların ve kuruluşların farklı veri kaynaklarından yararlanmasını ve bu veriyi kullanarak yeni hizmetler, ürünler ve çözümler geliştirmesini sağlar.

Veri Egemenliği: Ulusal düzeyde veri stratejileri, bir ülkenin veri egemenliğini korumak ve teşvik etmek için tasarlanmıştır. Ortak Veri Uzayı, ulusal ve bölgesel düzeyde verinin nasıl yönetildiğini ve paylaşıldığını standartlaştırarak bu egemenliği destekler.

Güvenlik ve Gizlilik: Standartlaştırılmış veri altyapıları, veri güvenliği ve bireysel gizlilik konularında daha tutarlı protokoller ve yönergeler oluşturabilir.

Entegrasyon: Farklı sektörler, endüstriler ve hükümet birimleri arasında veri entegrasyonunu kolaylaştırarak, daha bütünleşik ve etkili hizmetlerin sunulmasını teşvik eder.

Karar Verme: Ortak Veri Uzayı, hükümetin, özel sektörün ve diğer paydaşların daha bilgilendirilmiş kararlar almasına yardımcı olan daha kaliteli, doğru ve zamanında verilere erişim sağlar.

Ortak veri alanları, belirli bir sektör veya konu odaklıdır ve o alandaki veri paylaşımını ve erişimini düzenleyen platformlar olarak tanımlanabilir. Örneğin, sağlık verileri üzerine odaklanan bir ortak veri alanı, hastaneler, laboratuvarlar ve araştırma kuruluşları arasında bilgi akışını kolaylaştırabilir.

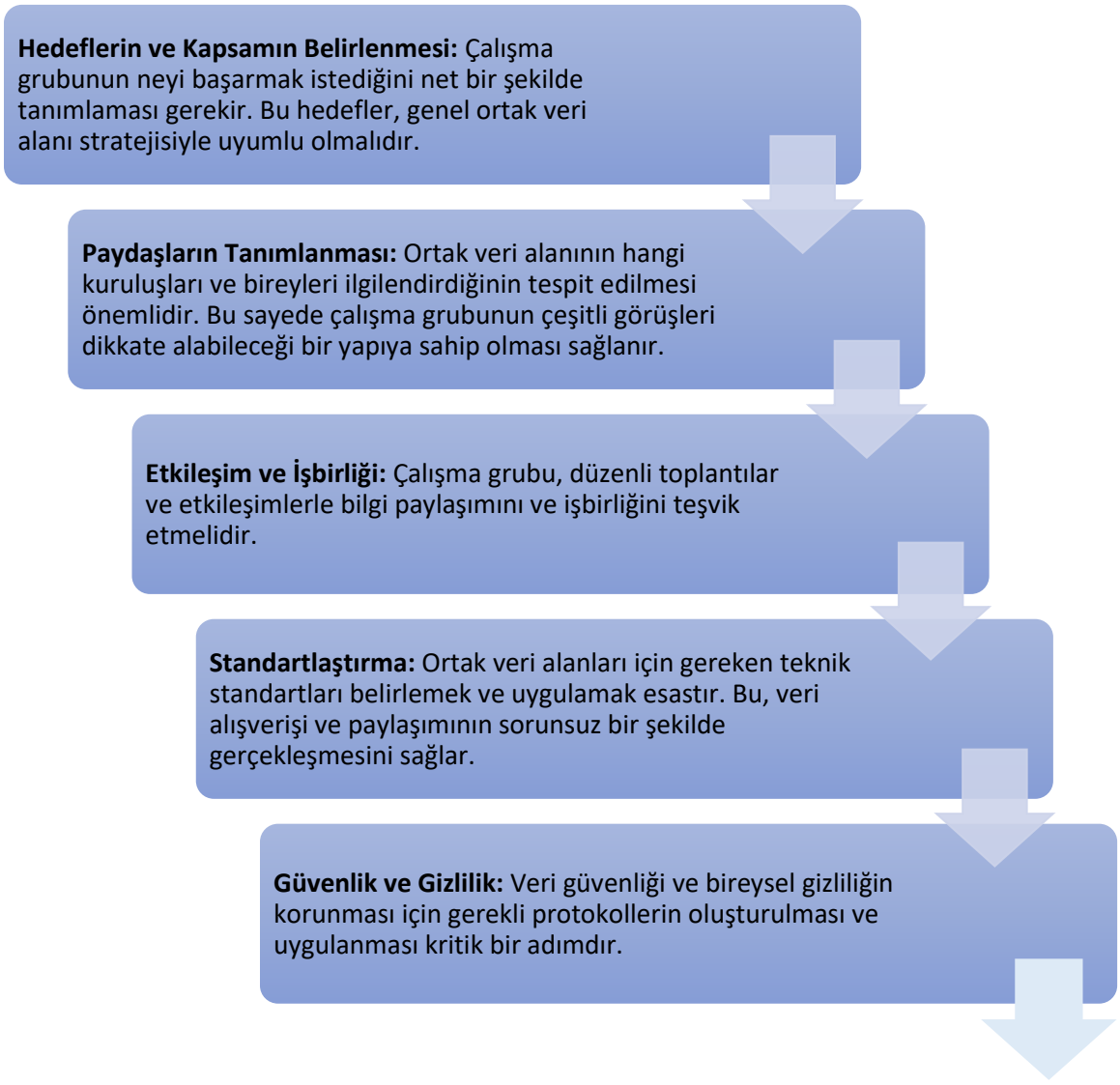
Peki bu ortak veri alanlarının işlevi nedir? İlk olarak, veri alışverişi süreçleri standartlaştırılır. Böylece, farklı kaynaklardan veya farklı formatlarda gelen veriler bile bir araya getirilip etkili bir şekilde işlenebilir. Bu, verinin potansiyelinin tam olarak kullanılmasını sağlar ve analiz süreçlerini daha verimli kılar.

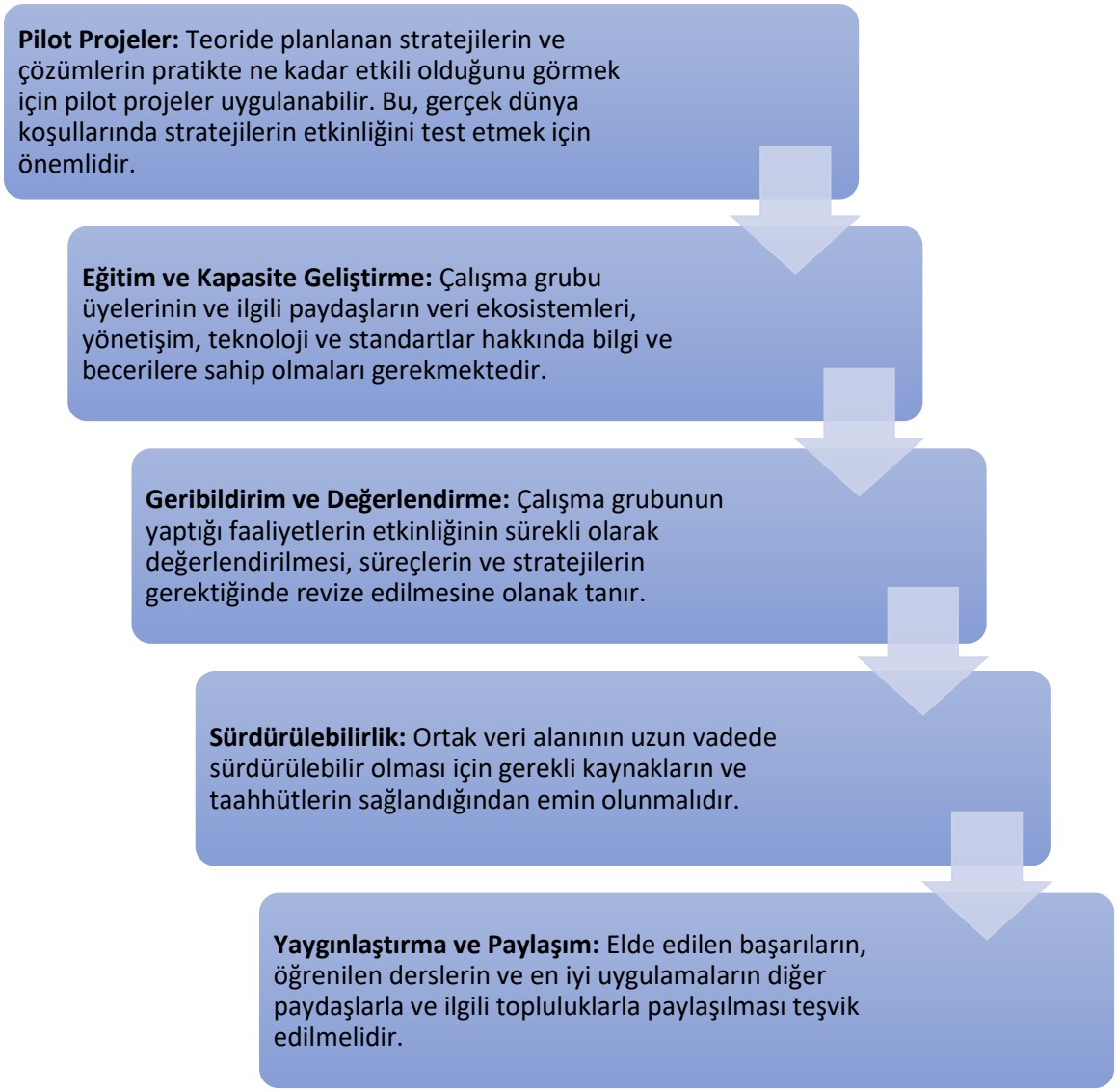
Güvenlik de bu alanların temel işlevlerinden biridir. Ortak veri alanları, veri paylaşımını uygun güvenlik protokolleri altında gerçekleştirmeyi garanti eder. Özellikle kişisel veya hassas veriler söz konusu olduğunda, bu güvenliği sağlamak kritik öneme sahiptir. Aynı zamanda, veriye erişimi daha demokratik kılarak, büyük veya küçük tüm organizasyonların eşit şartlarda faydalanmasını teşvik eder.

Bu alanların bir diğer önemli işlevi de inovasyonun teşvik edilmesidir. Ortak veri alanları, farklı kuruluşların ve uzmanların bir araya gelerek yeni fikirler üretmelerine, araştırmalar yapmalarına ve hatta yeni ürünler veya hizmetler geliştirmelerine olanak tanır. Bu, ekonomik büyüme ve sektörel ilerlemenin önemli bir parçasıdır.

2.4.2.1 Ortak Veri Uzayı Çalışma Grupları Nasıl Bir Yöntem İzlemelidir?

Ortak veri alanı çalışma grupları, veri ekosistemlerinin etkin bir şekilde oluşturulması, yönetilmesi ve geliştirilmesi için önemli aktörlerdir. Bu gruplar, birçok farklı paydaşı (örn. kamu kuruluşları, özel sektör temsilcileri, sivil toplum, akademi) bir araya getirerek kolektif bir yaklaşım benimsemelidir. İşte bu grupların başarılı olmaları için izlemeleri gereken temel adımlar:





Şekil 1: Veri Uzayı Çalışma Grupları Adımları

Ortak veri alanı çalışma grupları, bu adımları izleyerek ortak veri alanının etkili bir şekilde oluşturulmasını, yönetilmesini ve sürdürülmesini sağlar. Grubun, sürekli değişen teknolojik ve sosyal dinamiklere adapte olabilmesi için bu adımların düzenli olarak gözden geçirilmesi esastır.

Örnek: Avrupa Veri Ekosistemi Temel Bileşenleri

Avrupa veri ekosisteminin temel bileşenleri, bölgenin dijital dönüşümüne ve Avrupa'nın veri ekonomisindeki konumuna yön veren unsurlardan oluşmaktadır. Bu bileşenler, Avrupa'nın veri yönetimi, erişimi, kullanımı ve korumasına ilişkin yaklaşımını şekillendirir. Avrupa veri ekosisteminin temel bileşenleri şunlardır:

Tablo 1: Avrupa Veri Ekosistemi Bileşenleri

Bileşen Kategorisi	Örnek Uygulama
Yasal Çerçeve	• **Genel Veri Koruma Tüzüğü (GDPR):** Kişisel verinin korunmasına dair Avrupa Birliği'nin ana yasal çerçevesidir. Bireylerin veri haklarına odaklanır ve veri işleme faaliyetlerinde şeffaflığı ve hesap verebilirliği teşvik eder. • **Açık Veri ve Kamu Sektörü Bilgisi Yeniden Kullanımı Direktifi:** Kamu sektörü verisinin yeniden kullanılabilirliğini teşvik eder, böylece inovasyonu destekler ve ekonomik büyümeye katkıda bulunur. • **Veri Yönetişim Yasası (Data Governance Act):** Kamu kurumları tarafından işlenen, belirli kategorilerdeki verilerin AB içerisinde yönetişimini düzenler.
Teknolojik Altyapı	• **Yüksek Performanslı Bilgi İşlem (HPC) Merkezleri:** Büyük veri analizi ve yapay zeka uygulamaları için gereken bilgisayar gücünü sağlar. • **Veri Altyapıları:** Verinin depolanması, işlenmesi ve iletilmesi için gerekli olan fiziksel ve sanal sistemler. • **Veri Alanları (Data Spaces):** Sektörel veri alanları, farklı sektörlerde veri paylaşımını kolaylaştırır. Örneğin, endüstriyel veri alanı, sağlık veri alanı veya finansal veri alanı gibi.
Eğitim ve Araştırma	• **Eğitim Programları:** Veri bilimi, yapay zeka ve ilgili disiplinlerde uzmanlaşmış profesyoneller yetiştirmek için. • **Araştırma Merkezleri ve Üniversiteler:** Yeni teknolojilerin ve yöntemlerin geliştirilmesine öncülük eder.
İşbirlikleri ve Ağlar	• **Veri İşbirlikleri:** Farklı kuruluşlar arasında veri paylaşımını teşvik eder. • **Sektörel Ağlar:** Belirli endüstrilere veya uygulama alanlarına odaklanan gruplar. • **Standartlar ve Protokoller:** Veri alışverişi, uyumluluk ve güvenliği için gerekli olan teknik standartlar.
Girişimcilik ve İnovasyon	• **Start-up Ekosistemi:** Yeni veri tabanlı çözümler ve teknolojilerin geliştirilmesini teşvik eder. • **İnovasyon Merkezleri:** Yeni fikirlerin ve çözümlerin hızla hayata geçirilmesi için gereken destek ve kaynakları sağlar.
Güven ve Etik	• **Veri Etik Kuralları:** Veri kullanımının etik yönleriyle ilgilenir. • **Güvenilir Veri Ortamları:** Verinin güvenli bir şekilde saklandığı ve işlendiği ortamlar.

Bu bileşenlerin bir araya gelmesi, Avrupa'nın dijital ekonomisinde verinin etkili, güvenli ve etik bir şekilde kullanılmasını sağlar. Böylece Avrupa, global veri ekonomisinde rekabetçi bir konuma gelmeyi hedeflerken aynı zamanda bireylerin haklarını ve gizliliğini koruma altına alır.

Örnek: Avrupa Ortak Veri Alanları

Avrupa Veri Stratejisi'nin temel amacı birleşik ve açık bir Avrupa veri ekosistemi oluşturmaktır. Bu strateji, Avrupa'nın veri ekonomisinin potansiyelini tam anlamıyla gerçekleştirmesi için bir yol haritası sunar. "Ortak veri alanı" (Common Data Spaces) kavramı, bu stratejide merkezi bir yere sahiptir.

Avrupa Veri Stratejisi bağlamında "ortak veri alanı" şunları ifade eder:

Sektörel Bazlı Veri Altyapıları: Ortak veri alanları, belirli sektörlere veya uygulama alanlarına (örn. sağlık, enerji, tarım, finans) odaklanan, paylaşılan ve standartlaştırılmış veri altyapılarıdır.

Veri Paylaşımını Kolaylaştırma: Ortak veri alanları, veri paylaşımını teşvik eder ve bu sayede şirketler, araştırmacılar ve kamu kurumları arasında veri değişimini kolaylaştırır.

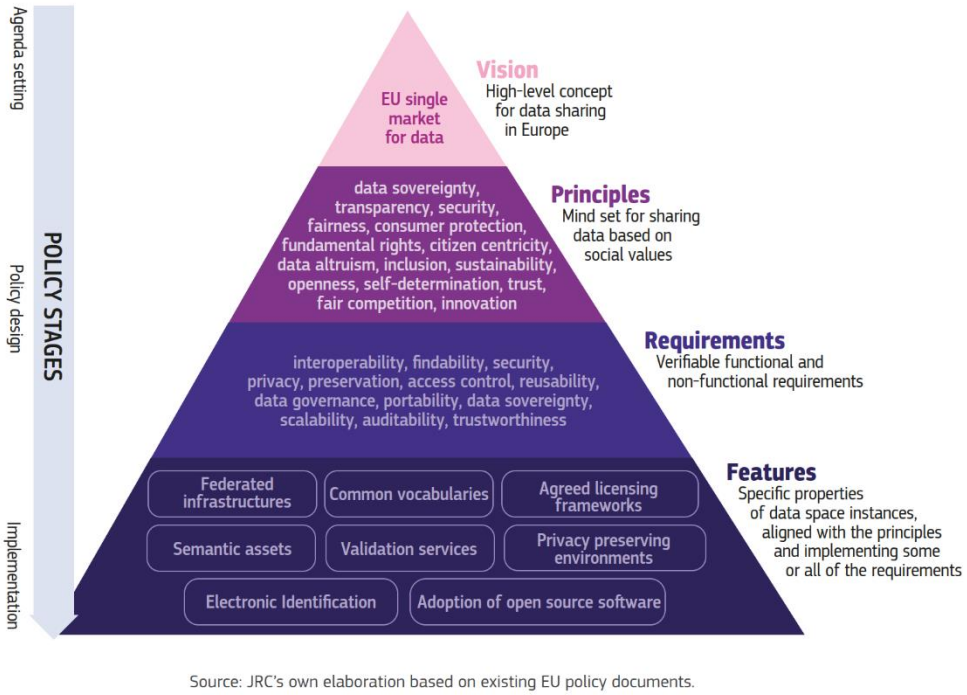
Standartlaştırma: Avrupa genelinde benimsenen standartlar ve protokollerle, veri paylaşımı daha verimli ve güvenli hale gelir.

Veri Egemenliği: Avrupa, veri egemenliğini ve Avrupalı kullanıcıların ve şirketlerin veri üzerindeki kontrolünü artırmayı hedefler. Ortak veri alanları bu amacı destekler.

Güvenlik ve Gizlilik: Ortak veri alanları, GDPR gibi mevcut veri koruma düzenlemeleriyle uyumlu olmalıdır. Bu, veri paylaşımının hem güvenli hem de özel olduğunu garantiler.

Açık Veri ve Kamu Verisi: Kamu sektöründen elde edilen verinin, yenilik ve değer yaratma potansiyelini maksimize etmek için daha geniş bir erişimle paylaşılması teşvik edilir.

Ortak veri alanları, Avrupa veri ekosistemin temel bileşenlerinden biri olarak görülür. AB ortak veri alanı oluşturma aşamaları Şekil 2: Avrupa Birliği Ortak Veri Alanları Oluşturma Aşamaları'nda verilmiştir. Kanunların ortak veri alanına yönelik uyarlanması için prensipler belirlenmiş, ihtiyaçlar ortaya konmuş, nihayetinde buna bağlı çıktılar elde edilmiştir.



Şekil 2: Avrupa Birliği Ortak Veri Alanları Oluşturma Aşamaları

Avrupa'nın veri stratejisi bağlamında ortak veri alanları oluşturma hedefi, veriyi daha etkili bir şekilde paylaşmak, değer yaratmak ve Avrupa ekonomisini güçlendirmek için belirlenen sektörlere odaklanmıştır. Bu ortak veri alanları şunlardan oluşur:

Sanayi (Endüstriyel): Üretim, işleme ve diğer endüstriyel faaliyetlere ilişkin veriler bu kategoride yer alır.

Yeşil Anlaşma: İklim değişikliği, çevresel koruma ve sürdürülebilir enerjiye dair veriler bu alanda toplanmıştır.

Mobilite: Taşımacılık ve hareketlilikle ilgili verilere odaklanır.

Sağlık: Hasta kayıtlarından araştırma verilerine kadar sağlıkla ilgili geniş bir yelpazede veriyi kapsar.

Finans: Bankacılık, sigortacılık ve finansal hizmetlerle ilgili veri setlerini içerir.

Enerji: Enerji üretimi, tüketimi ve dağıtımıyla ilgili veriler bu alanda yer bulmuştur.

Tarım: Tarım ve gıda üretimi ile ilgili verileri kapsar.

Kamu Yönetimi: Kamu hizmetleri, yönetim ve diğer kamu faaliyetlerine dair verilere odaklanır.

Beşeri ve Sosyal Bilimler: Toplumsal araştırmalara, anketlere ve diğer sosyal bilimlerle ilgili verilere yer verilir.

Bu ortak veri alanlarının oluşturulma amacı, veri paylaşımını teşvik etmek, inovasyonu desteklemek, yeni iş modellerini teşvik etmek ve Avrupa'nın global veri ekonomisinde daha

rekabetçi bir konuma gelmesini sağlamaktır.

Şekil 3'te Avrupa Ortak Veri Alanları ile ilişkili çalışmaların zaman planı görülmektedir:[2]

Mavi renk yasama ve siyasi girişimleri temsil etmektedir. **Yeşil renk** Komisyon'un finansman girişimlerini temsil etmektedir. **Kahverengi renk** diğer eylemleri tanımlamaktadır.

Şekil 3: Avrupa Ortak Veri Alanları Zaman Planı

[2] Kaynak: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces

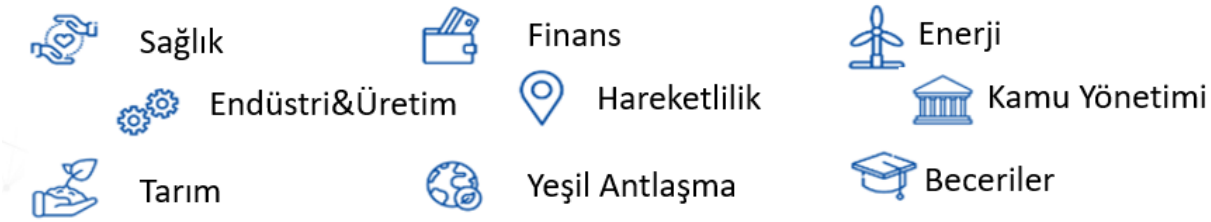
3 Veri Uzayına Genel Bakış

3.1 Veri Uzayının Tanımı ve Kapsamı

“Veri alanı" terimi, bir veya birçok dikey ekosistem içinde veri depolama ve paylaşımına ilişkin aynı yüksek düzeyde standartları ve yönergeleri takip eden, güvenilir ortaklar arasındaki veri ilişkisini ifade eder. Veri alanı kavramının önemli bir yönü, verilerin merkezi olarak depolanmaması, bunun yerine kaynağında tutulmasıdır. Bu şekilde, veriler yalnızca gerektiğinde anlamsal uyumluluk aracılığıyla transfer edilir.[3]

Veri alanı, veri sağlayıcıları, kullanıcılar ve aracılar gibi tüm katılımcıların toplamından oluşur. Veri alanları iç içe geçebilir ve birbiriyle örtüşebilir. Örneğin, bir veri sağlayıcısı aynı anda birkaç veri alanına katılabilir. Veri alanlarının amacına hizmet edebilmesi ve katılımcılar arasındaki ilişkileri desteklemesi için veri egemenliği ve güveni önemlidir.

Avrupa Komisyonu (European Commision), Avrupa ekonomisi ve toplumunun yararına veri kullanımına ilişkin stratejik ekonomik sektörler ve kamu yararı alanlarında Avrupa'nın ortak veri alanlarını geliştirmeyi desteklemektedir. Şubat 2020'de duyurulan Avrupa Veri Stratejisi (European Data Strategy), sağlık, tarım, üretim, enerji, mobilite, finans, kamu yönetimi, beceriler, Avrupa Açık Bilim Bulutu ve Yeşil Anlaşma (Green Deal) hedeflerini karşılamak için stratejik alanda veri alanlarının oluşturulacağını içermektedir. Bu süreçte, medya ve kültürel miras gibi diğer önemli alanlarda da veri alanları ortaya çıkmıştır. Nihai hedef, bu veri alanlarının birleştirilerek tek bir Avrupa veri alanının oluşturulmasıdır.



Avrupa'nın Ortak Veri Alanları, aşağıdaki özellikleriyle veri havuzlamayı ve paylaşmayı kolaylaştırmak üzere ilgili veri altyapılarını ve yönetim çerçevelerini bir araya getirir.

- Veri paylaşım araçları ve hizmetlerini kullanarak veri havuzlama, işleme ve paylaşma süreçlerini gerçekleştirirken, enerji verimli ve güvenli bulut kapasitelerini ve ilgili hizmetleri birleştirir.
- Veriye erişim ve işleme konusunda hakları şeffaf ve adil bir şekilde belirleyen, ilgili Avrupa Birliği (AB) mevzuatıyla uyumlu veri yönetim yapılarını içerir.
- Verinin mevcudiyetini, kalitesini ve uyumluluğunu, hem alan özelinde hem de sektörler arasında, geliştirir.[4]

Ortak Avrupa veri alanları (Common European Data Spaces), veri ekosistemini geliştirerek, farklı sektörler ve kuruluşlar arasında veri paylaşımını arttırmayı hedefler ve Avrupa'nın veri tabanlı inovasyon ve ekonomik büyüme potansiyelini maksimize etmeyi amaçlar.

[3] What are Data Spaces?, https://gaia-x.eu/what-is-gaia-x/deliverables/data-spaces/
[4] Data Spaces, https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces

Tüm bunların sonucunda, veri alanlarının dijital dönüşümü hızlandırmaya ve farklı alanlar arasında ekonomik iyileşme planlarını desteklemeye önemli katkıda bulunması beklenmektedir. Gelecekteki hedef, farklı veri alanlarını birbirine bağlayan ve AB değerleri ve düzenlemelerine uygun şekilde verilerin yaygın bir şekilde paylaşıldığı ve kullanıldığı bir Avrupa veri alanına sahip olmaktır.[5]

3.2 Veri Uzayının Özellikleri ve Bileşenleri

Ortak Avrupa Veri Alanları, Avrupa Veri Stratejisi'nin temel hedefleri arasında yer alır. Bu vizyon, Avrupa Birliği genelinde stratejik sektörlerde uyumlu ve birleştirilmiş veri alanlarının oluşturulmasını öngörür. Amacı, veri paylaşımına ilişkin yasal ve teknik engelleri aşmak ve güvenlik konularına ortak kurallarla çözüm getirmektir. Ortak bir Avrupa Veri Uzayı, ilgili veri altyapılarını ve yönetim çerçevelerini bir araya getirerek veri havuzlamayı ve paylaşmayı kolaylaştırır. Bu sayede, veriye dayalı işbirliği ve yeniliklerin teşvik edilmesi, Avrupa ekonomisinin rekabet gücünü artırmaya yönelik önemli bir adım olacaktır.

Avrupa veri stratejisine göre, veri alanları aşağıda belirtilen kriterleri taşıyacaktır.

1. Ortak Avrupa Veri Alanları, veri havuzlaması, işleme ve paylaşımı için birden fazla kuruluşun aynı veri paylaşım araçlarını ve hizmetlerini kullanmasını amaçlamaktadır. Bu sayede, veri altyapıları ve hizmetleri standartlaştırılarak veri paylaşım süreçleri daha verimli ve etkin bir şekilde gerçekleştirilebilecektir.

2. AB mevzuatıyla uyumlu veri yönetim yapıları, veriye erişim ve işleme haklarını şeffaf ve adil bir şekilde belirlenmesi Veriye erişimin, veri yönetim yapılarının ve işleme haklarının AB mevzuatıyla uyumlu, şeffaf ve adil bir şekilde belirlenmesi hedeflenmektedir.

3. Verinin mevcudiyetini, kalitesini ve uyumluluğunu hem kendi alanı özelinde hem de sektörler arasında geliştirmek.

Avrupa'da ortak veri alanlarında, veri sahipleri mevcut birlik veya üye devlet mevzuatının gerektirdiği veri paylaşım yükümlülüklerine ek olarak, verilerini gönüllü bir şekilde sunma özgürlüğüne sahip olacak ve verilerini tazminat karşılığında veya ücretsiz olarak yeniden kullanılmasına yönelik kendi kararlarına bağlı olarak sunabileceklerdir.

Ortak Avrupa Veri Uzayı, veri havuzlamayı, erişimi, paylaşımı, işlemeyi ve kullanımı güvenli ve gizlilik koruyucu bir altyapı üzerinden gerçekleştirmeyi amaçlayan bir girişimdir. Aynı zamanda, adil, şeffaf, orantılı ve ayrımcılık yapmayan bir erişim yapısı, güvenilir veri yönetimi mekanizmaları ve Avrupa'nın kişisel veri koruması, tüketici koruma ve rekabet hukuku gibi değerlerine tam uyum içinde veriye yaklaşımı teşvik eder. Veri sahipleri, kontrol ettikleri kişisel veya kişisel olmayan verilere erişimi düzenleyebilir, sunulan veri ücretli veya ücretsiz olarak yeniden kullanılabilir ve farklı kuruluşlar ile bireylerin katılımını destekler. Bu yaklaşım, Avrupa Birliği'nin veri ekonomisini güçlendirme ve veri odaklı yenilikleri teşvik etme hedeflerine yönelik önemli bir adımdır.

[5] What are Data Spaces?, https://joinup.ec.europa.eu/collection/semic-support-centre/data-spaces

4 Veri Uzayı Yönetimi

Veri (data) sözlük anlamı olarak; bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done anlamına gelmektedir.[6] Veri, bilişim teknolojisi açısından "sayısal ortamlarda bulunan, işlenen veya taşınan sinyaller, "anlamlı hale dönüştürülmemiş bitler" veya "birbiriyle bağlantısı henüz kurulmamış bilinenler" olarak tanımlanabilir.[7]

Veri uzayı, veri entegrasyon sisteminde karşılaşılan bazı sorunların üstesinden gelmeyi amaçlayan bir soyutlamadır. Amaç, mevcut eşleştirme ve harita oluşturma tekniklerine güvenerek bir veri entegrasyon sistemi kurmak için gereken çabayı azaltmak ve sistemi "kullandıkça öde" (pay-as-you-go) tarzında iyileştirmektir.[8.]

Günümüzde kurumlar, verileri çeşitli ama birleşik bir veri katmanında yönetmenin verimli bir yolunu sunan bir veri yönetim çözümüne ihtiyaç duymaktadır. Veri yönetimi sistemleri, veri yönetimi platformları üzerine kuruludur ve veritabanları (database), veri gölleri (data lake), veri ambarları (data warehouse), büyük veri yönetim sistemleri, veri analizi ve daha fazlasını içerir. Tüm bu bileşenler, bir kurumun uygulama yazılımları için ihtiyaç duyduğu veri yönetim becerilerini sunmak üzere "veri aracı" olarak birlikte çalışır. Bu uygulama yazılımlarından gelen analitik ve algoritmalarda da bunlardan yararlanılır. Mevcut araçlar veritabanı yöneticilerinin (Database Administrator-DBA) geleneksel yönetim görevlerinin çoğunu otomatikleştirmelerine yardımcı olsa da çoğu veritabanı konuşlandırmasının boyutu ve karmaşıklığı nedeniyle manuel müdahale hâlâ sık sık gerekmektedir. Manuel müdahale gerektiğinde hata olasılığı artacağı için manuel veri yönetimi ihtiyacını azaltmak gerekmektedir. Bu yeni veri yönetim teknolojisi, kendi kendini yöneten veritabanının temel hedeflerinden biridir.[9]

Veri uzayı yönetimi; verilerin güvenli, verimli ve uygun maliyetli bir şekilde toplanması, saklanması ve kullanılması uygulamasıdır. İnsanların, kurumların ve bağlantılı araçların, verilerin politika ve düzenleme sınırları kapsamında kullanımını optimize etmelerine yardımcı olmayı amaçlamaktadır. Böylece, kurum ve kuruluşlar en yüksek düzeyde fayda sağlayacak kararlar alabilir ve bunları hayata geçirebilirler. Kuruluşlar değer yaratmak için giderek daha fazla maddi olmayan varlıklara yöneldiklerinden, güçlü bir veri yönetimi stratejisi her zamankinden daha önemli hale gelmiştir.[10]

Veri uzayı konusunda hazırlanan en önemli belgelerden birisi Avrupa Veri Stratejisi (European Data Strategy[11])'dir. Avrupa Komisyonu'nun yeni dijital stratejisini belirleyen bu belge, teknoloji geliştirmeyi ilk sıraya koymasının yanında, teknolojinin Avrupa değerleri çerçevesinde ve gerçek ekonomiye uygun olarak nasıl tasarlanacağı, nasıl üretileceği ve nasıl uygulanacağı konusuna odaklanmaktadır.[12]

Avrupa Veri Stratejisi, Avrupa'nın küresel rekabet edebilirliğini ve veri egemenliğini sağlayacak tek bir veri pazarı oluşturmayı amaçlamaktadır. Avrupa ortak veri uzayı (Common European

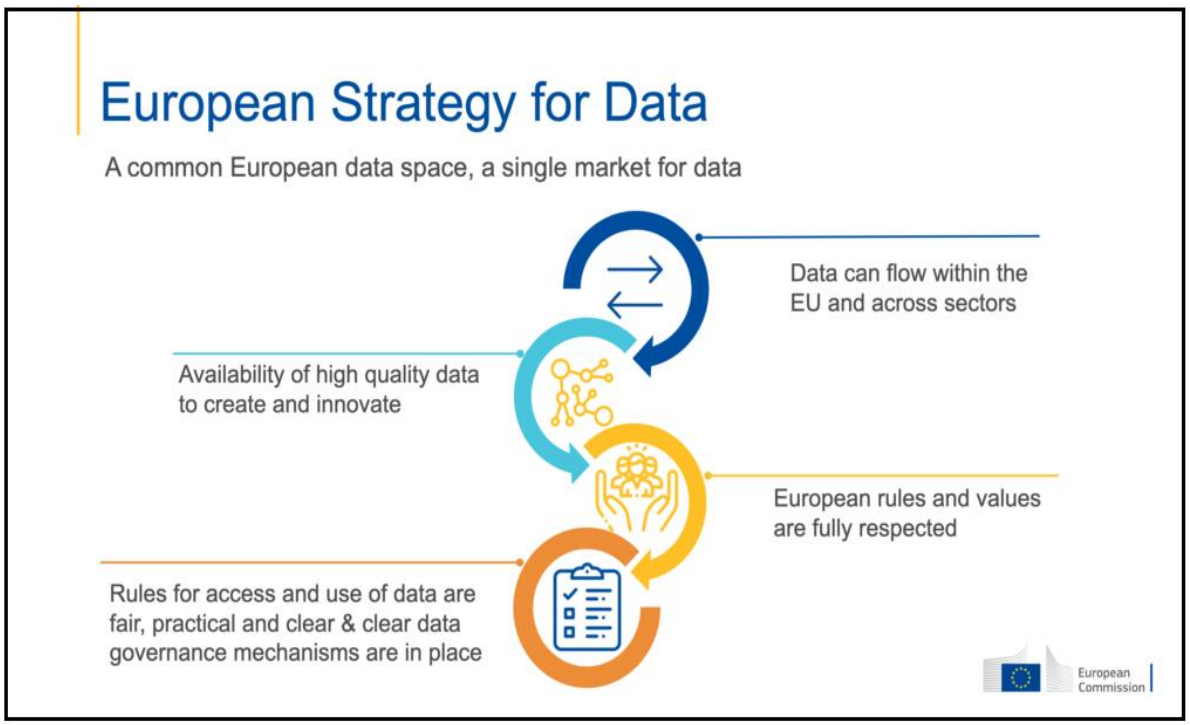
[6] https://sozluk.gov.tr/ (Erişim:07.06.2023)
[7] Sağıroğlu ve diğerleri, 2017:15
[8] https://en.wikipedia.org/w/index.php?title=Dataspaces&oldid=1150311659 (Erişim:07.06.2023)
[9] https://www.oracle.com/tr/database/what-is-data-management (Erişim:07.06.2023)
[10] https://www.oracle.com/tr/database/what-is-data-management/ (Erişim:07.07.2023)
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 (Erişim:07.07.2023)
[12] http://dataspaces.info/common-european-data-spaces/#page-content (Erişim:07.07.2023)

data space), aynı zamanda verileri üreten şirketleri ve bireyleri kontrol altında tutarken, ekonomi ve toplum için daha fazla verinin kullanılabilir olmasını sağlamayı da amaçlamaktadır. Strateji, veriyi ekonomik büyüme, rekabet edebilirlik, yenilikçilik, iş yaratma ve genel olarak toplumsal ilerleme için temel bir kaynak olarak kabul etmektedir.[13] Stratejide veri uzayı yönetimine ilişkin belirlenen hedefler dört ana başlıkta toplanmaktadır. Bunlar;

- **Tek Pazar :** Ortak bir Avrupa veri uzayı için tek bir veri pazarı oluşturulacak
- **Veri Akışı :** AB içinde ve sektörler arasında veri akışı sağlanacak
- **Veri Kalitesi :** Yaratıcılık ve yenilikçilik için yüksek kaliteli verilere odaklanılacak
- **Veri Yönetişimi:** Verilere erişim ve veri kullanımına ilişkin adil, pratik, açık ve net kurallar içeren veri yönetişim mekanizmaları kurulacak ve Avrupa veri uzayı, AB'deki işletmelere Tek Pazar ölçeğini geliştirme imkânı verecektir.

Strateji ayrıca bu hedeflere ulaşabilmek için şu mekanizmaların harekete geçirilmesi gerektiğini de vurgulamaktadır:[14]

- Veriler AB içinde ve sektörler arasında akabilir,
- Avrupa kural ve değerlerine, özellikle kişisel verilerin korunmasına, tüketicinin korunması mevzuatına ve rekabet yasasına tam olarak uyulur,
- Verilere erişim ve veri kullanımına ilişkin kurallar adil, pratik ve açıktır ve açık ve güvenilir veri yönetişim mekanizmaları mevcuttur; uluslararası veri akışlarına Avrupa değerlerine dayanan açık ama iddialı bir yaklaşım vardır.



Şekil 4: Avrupa Veri Stratejisi[15]

Stratejiye göre kamu harcamalarının şeffaflığını ve hesap verebilirliğini ve harcama kalitesini iyileştirmek, hem AB hem de ulusal düzeyde yolsuzlukla mücadele etmek, yasa uygulama

[13] http://dataspaces.info/common-european-data-spaces/#page-content (Erişim:08.07.2023)
[14] European Commission, 2020:5
[15] http://dataspaces.info/common-european-data-spaces/#page-content (Erişim:07.06.2023).

ihtiyaçlarını karşılamak ve AB yasasının etkili bir şekilde uygulanmasını desteklemek ve aşağıda sıralanan yenilikçi teknolojileri mümkün kılmak amacıyla kamu idareleri için ortak Avrupa veri uzayı uygulaması desteklenmesi gerektiğini belirtirken bu desteklerin, kamu yararına yapılan hizmetleri de kapsayacağını ifade etmektedir. Bu manada kamunun ele alması gereken üç tür genel teknoloji vardır. Bu teknolojiler;

- **GovTech (Government Technology):** Devlet faaliyetlerinin verimliliğini artırmak ve yönetimini iyileştirmek için yaratılan teknolojik çözümler bütünü olarak tanımlanır. E-devlet, akıllı şehir vs.
- **RegTech (Regulatory Technology):** Düzenleyici ve uyumluluk süreçlerini geliştirmek için bilgi teknolojisinin kullanılmasıdır. RegTech, en çok finansal hizmetler, oyun, sağlık, ilaç, enerji ve havacılık gibi yoğun şekilde düzenlenmiş endüstrilere ve faaliyetlere uygulanır. RegTech, CivicTech (Sivil Teknolojiler) gibi kavramları da içinde barındıran çatı bir kavramdır.
- **LegalTech (Legal Technology):** Hukuk teknolojisi, hukuk hizmetleri sağlamak ve hukuk endüstrisini desteklemek için teknoloji ve yazılımın kullanımını ifade eder.

Sıralanan bu teknolojiler aynı zamanda veri uzayı yönetiminin teknolojik bileşenlerini oluşturmakta ve kurum ve kuruluşlara teknolojik olarak gerçekleştirecekleri eylemler konusunda yol göstermektedir.

Farklı alanlarda büyük veri üreticisi ve aynı zamanda kullanıcısı olan kamu kurumlarının veri uzayı alanında gerçekleştirecekleri eylemler, orantılılık ilkesine, veri koruma kurallarına ve AB yasalarına göre gerçekleştirilmelidir. Bu durumda verilerin kullanımı hem hukuka hem de kamu yararına uygun olacaktır. Örneğin kamu verileri, kamu harcamalarının şeffaflığını ve hesap verebilirliğini geliştirmek, yolsuzlukla mücadele etmek ve harcama kalitesini iyileştirmek için önemlidir. AB ve üye devlet mevzuatına, içtihatlarına ve e-adalet hizmetlerine ilişkin bilgilere sorunsuz erişim ve kolay kullanım, hem AB hukukuna hem de yenilikçi "hukuk teknolojisi" uygulamalarına olanak tanır.[16] Bu olanaklar aynı zamanda yargıçlar, kamu görevlileri, şirket danışmanları ve avukatlar gibi uygulayıcılar açısından da kolaylık oluşturur.[17]

Avrupa Komisyonu'nun bu stratejisi hem AB ile uyum açısından hem de veri aktarımının önündeki engelleri ortadan kaldırarak ülkemizin veri ekonomisini kalkındırma açısından uygun ve gerekli olacaktır. Bu bağlamda ülkemizde, verileri toplama ve elde etme, depolama, düzenleme, yapılandırma, diğer sistemlerle entegre etme, birlikte çalışabilirliğini ve güvenliğini (gizlilik, bütünlük ve erişebilirlik) sağlama gibi tüm süreçleri kapsayan bir veri uzayı yönetim sisteminin kurulması gerekmektedir.

Bu bölümde veri uzayı yönetimi sürecinin temel adımları olan veri toplama ve elde etme, veri depolama ve düzenleme, veri entegrasyonu, veri yönetişimi ve veri birlikte çalışabilirliği sağlanması konularına değinilecek, sonunda ise veri uzayı yönetimi konusunda karşılaşılan sorunlar ile çözüm önerileri sunulacaktır.

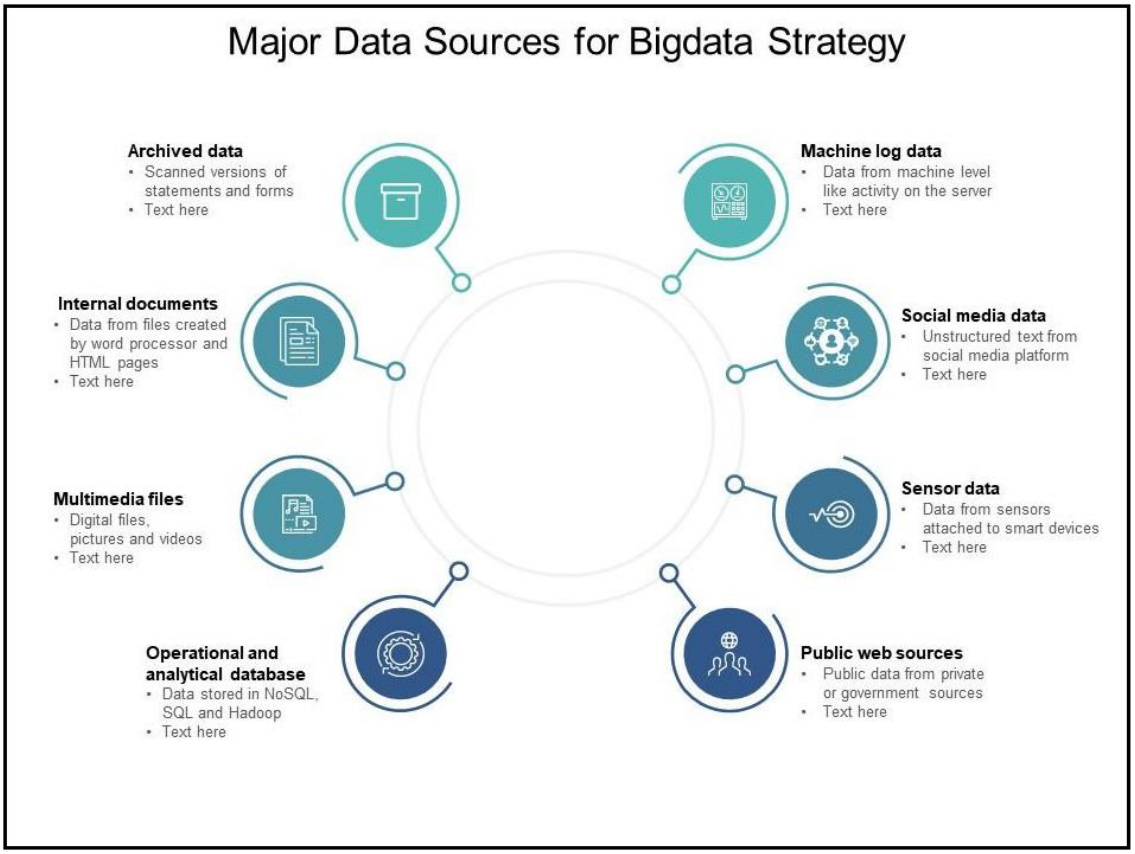
[16] European Commission, 2020:31.
[17] European Commission, 2020:32.

4.1 Veri Toplama ve Elde Etme

Günümüzde veri kaynaklarının sayısının artması, büyük veri toplayabilmek için birçok farklı alternatif ortaya çıkartmıştır. Veri kaynaklarına bilgi sistemleri açısından bakıldığında oldukça fazla olduğu görülür. Bu kaynaklardan en önemlileri (Şekil 5) şunlardır:

- Arşivlenmiş veriler (Archived data): İfadelerin ve formların taranmış versiyonu
- İnternet belgeleri (Internal documents): Kelime işlemci ve HTML sayfaları tarafından oluşturulan dosyalardan elde edilen veriler.
- Multimedya dosyaları (Multimedia files): Dijital dosyalar, resimler ve videolar,
- Operasyonel ve analitik veri tabanı (Operational and analytical database): NoSQL, SQL ve Hadoop'ta[18] saklanan veriler bu türden verilerdir. Veri tabanlarında tutulan pazarlama amaçlı kişisel veriler ile davranış analizine yönelik veriler gibi veriler de örnek olarak verilebilir.
- Makine log verileri (Machine log data): Sunucudaki makine düzeyinde etkinlik benzeri veriler önemli veri kaynaklarıdır. Veriler makineden makineye (M2M) olarak da bilinen yöntemle de paylaşılmaktadır. Araçların ve cep telefonlarının GPS verileri, yiyecek-içecek otomatları gibi internete bağlanabilen cihazlar topladıkları verileri bir merkeze iletirler.
- Sosyal medya verileri (Social media data): Sosyal medya platformundan yapılandırılmamış metinler veri içerir. Bir e-posta gönderme, Facebook'ta yazılan bir yorum, telefon anketine verilen yanıtlar, elektronik tabloya konulan bilgiler, hatta bir WhatsApp mesajı gibi gün içinde yapılan sayısız eylem muazzam bir veri kaynağı oluşturur.
- Sensör verileri (sensor data): Akıllı cihazlarda ve akıllı şehirlerde bulunan sensörlerden ve trafik sistemindeki kameralar bu tür veri kaynaklarına örnektir. Biyometrik veri toplayan parmak izi okuyucuları, retina tarayıcılar, DNA okuyucular, yüz tanıma sensörleri ve ses tanıma sistemleri ile özel, kurumsal, askeri, emniyet ve istihbarat servisleri gibi kurumların kullandığı biyometrik kimlik doğrulama teknolojileri de bu grupta değerlendirilmektedir.
- Herkese açık web kaynakları (Public web sources): Özel veya devlet kaynaklarından gelen herkese açık veriler.

[18] Hadoop, sıradan sunuculardan büyük verileri işlemek amacıyla kullanılan açık kaynak kodlu bir kütüphanedir. Her türlü veri için devasa depolama, çok yüksek işlem gücü ve neredeyse sınırsız sayıda eşzamanlı görevleri yönetme yeteneği sağlar. Dağınık bir bilgi işlem ortamında büyük verilerin verimli bir şekilde yönetilmesini ve işlenmesini mümkün kılar.



Şekil 5: Büyük Veri Stratejisi İçin Başlıca Veri Kaynakları[19]

Günümüzde bilgisayar, akıllı telefonlar, tabletler ve akıllı saatler gibi teknolojik ve bilgisayar donanımlı cihazlar, içeriklerinde bulunan programlar vasıtasıyla kişisel verilerin otomatik olarak toplanmasına olanak sunmaktadır.

Kişisel verilerin otomatik olmayan yöntemlerle toplanması ve işlenmesi de söz konusu olabilir. Bunun anlamı manuel olarak, el ile bilgilerin girişlerinin yapılmasıdır. Resmi kurumlarda, memurların kişilerin bilgilerini sorarak, elektronik sisteme manuel olarak girmelerini de bu yönteme örnek olarak gösterebiliriz. Bu şekilde alınan veriler de elektronik ortamda yer almaları bakımından düşünüldüğünde önemli veri kayıt sisteminden bahsedildiği anlaşılacaktır.

4.2 Veri Depolama ve Düzenleme

4.2.1 Veri Depolama Teknolojileri

Veri depolama teknolojileri, bilgisayar sistemlerinde verilerin saklanması ve muhafaza edilmesi için kullanılan cihazlar ve yöntemlerdir. Bilgisayar kullanımında verilerin depolanması, işlenmesi ve erişilmesi son derece önemlidir. Depolama teknolojileri, verilerin fiziksel olarak saklandığı cihazlar ve yöntemler olarak tanımlanabilir.

Günümüzde kullanılan depolama teknolojileri arasında aşağıdaki sistemler yer almaktadır. Bu teknolojiler, kullanım amaçlarına bağlı olarak çeşitli avantaj ve dezavantajlara sahiptirler. Örneğin, HDD'ler büyük miktarda depolama alanı sunarken, SSD'ler daha hızlı veri aktarımı

[19] https://www.slideteam.net/major-data-sources-for-bigdata-strategy.html (Erişim: 03.07.2023)

ve işlemesi sağlar. Ağ depolama ve SAN'lar, birden fazla cihazın veri depolamasını merkezi bir sistemde toplayarak yönetmeye olanak tanırken, yedekleme ve kurtarma işlemleri veri kaybını önlemek için son derece önemlidir.[20]

1. **Sabit Disk Sürücüleri (HDD):** HDD (Hard Disk Drive) sabit disk sürücüleri, verilerin manyetik bir kaplama üzerine kaydedildiği bir mekanik depolama aygıtıdır. HDD'lerin dezavantajları arasında mekanik hareketli parçaları olduğundan, daha yüksek enerji tüketimleri ve daha az dayanıklılık söz konusu olabilir. Bu nedenle, taşınabilir cihazlar için SSD'ler gibi daha dayanıklı depolama seçenekleri tercih edilebilir.
2. **Katı Hal Sürücüleri (SSD):** SSD (Solid State Drive), verilerin flash bellek yongalarında depolandığı bir depolama aygıtıdır. SSD'ler, manyetik bir kaplama ve hareketli okuyucu/ yazar kafası yerine, bir bellek kontrol cihazı ve flash bellek yongaları kullanarak çalışır. Modern SSD'ler daha dayanıklı bellek hücreleri kullanır ve bu hücreler daha uzun ömürlüdür. Ancak, yüksek maliyetleri ve sınırlı depolama kapasiteleri, bazı kullanıcılar için dezavantajlar olarak görülebilir.
3. **Ağ Depolama:** Ağ depolama, ağ bağlantılı depolama aygıtlarının kullanımıyla gerçekleştirilen veri depolama işlemidir. Ağ depolama, sunucuların ve çalışanların verilere herhangi bir yerden ve herhangi bir cihazdan erişmelerini sağlayarak işletmeler ve kuruluşlar için birçok avantaj sunar.
4. **Depolama Alanı Ağları (SAN):** SAN (Storage Area Network), bir ağ üzerinde birden fazla sunucu ve depolama aygıtının birbirine bağlanarak merkezi bir depolama alanı oluşturduğu bir depolama mimarisidir. SAN, ihtiyaç duyulan depolama alanını kolayca genişletilebilen ve yüksek performans sağlayabilen bir seçenektir. SAN'ların çalışma prensibi, sunucuların bir ağ üzerinden depolama aygıtlarına erişimini sağlamaktır.
5. **Depolama Sanallaştırma:** Depolama sanallaştırma, fiziksel depolama kaynaklarının sanal depolama alanlarına dönüştürülerek, kullanıcılara daha esnek, daha ölçeklenebilir ve daha verimli bir depolama çözümü sunar. Depolama sanallaştırmanın avantajları arasında esnek depolama, ölçeklenebilirlik, verimli depolama, daha iyi yedekleme ve kurtarma, daha iyi performans avantajları arasında sıralanabilir. Dezavantajları ise yüksek maliyet, performans kaybı, daha fazla yönetim gereksinimi, güvenlik riskleri ve uyumluluk sorunları olarak görülmektedir.

Sonuç olarak, depolama teknolojileri, bilgisayar sistemlerinde verilerin saklanması ve yönetilmesinde önemli bir rol oynar.

Gelecekteki veri depolama teknolojileri, veri büyüklüğü ve işlem gücündeki sürekli artışa yanıt olarak geliştirilmeye devam edilmektedir. Gelecekte kullanılacağı öngörülen bazı depolama teknolojiler şunlardır:

- **Optik Depolama:** Optik depolama, verileri lazer ışınları kullanarak disk üzerinde depolamayı içerir. Bu teknoloji, hızlı okuma/yazma hızları ve yüksek yoğunluklu depolama kapasitesi sağlar.
- **Holografik Depolama:** Holografik depolama, lazer ışınlarını kullanarak üç boyutlu hologramlar oluşturur. Bu teknoloji, disk başına çok yüksek depolama kapasitesi sunar ve veri aktarım hızlarını artırır.
- **DNA Depolama:** DNA, son yıllarda veri depolama için bir seçenek olarak ortaya çıkmıştır.DNA molekülleri, çok yoğun bir şekilde veri depolama için kullanılabilir. DNA depolama, sınırsız depolama kapasitesi ve çok uzun ömürleri ile öne çıkmaktadır.
- **Kuantum Depolama:** Kuantum depolama, verileri atomların ve elektronların kuantum mekaniği özelliklerini kullanarak depolar. Bu teknoloji, veri depolama kapasitesini artırır ve güvenlik açısından daha güçlü bir seçenek sunar.

[20] https://tr.linkedin.com/pulse/veri-depolama-teknolojileri-entegres (Erişim: 05.07.2023)

- **Bulut Depolama:** Bulut depolama, her yerden erişim sağlamak için verileri internet üzerinden saklar. Bulut depolama, daha fazla depolama alanı ve kolay erişim sunar.

Bu teknolojilerin bir kısmı zaten kullanılmakta ve bir kısmı henüz geliştirilmekte olup, gelecekte daha yaygın hale gelecekleri düşünülmektedir. Bununla birlikte, her teknolojinin avantajları ve dezavantajları vardır ve bu teknolojilerin en uygun şekilde kullanılması için dikkatli bir değerlendirme gereklidir.

4.2.2 Veri Düzenleme ve Yapılandırma

Teknolojiye uyum sağlamaya çalışan kuruluşlar, verileri daha iyi yönetmek, farkındalık elde etmek, işlem süresini en aza indirmek ve geçmiş verilerin kullanımını artırırken maliyetlerden tasarruf ederek getirilerini artırmak için veri yönetimi sistemleri ve çözümlerini kullanmaktadırlar. Veri yönetim sistemlerinin başarılı olması verilerin depolama biçimine bağlıdır. Veriler, veri tabanında tutulma şekline göre yapılandırılmış, yarı yapılandırılmış ve yapılandırılmamış veriler olmak üzere üçe ayrılır[21]. Yapılandırılmamış ve yarı yapılandırılmış veriler yapay zeka (AI) sistemleri kullanılarak analiz edilerek çeşitli kullanılabilir veriler elde edilebilmektedir.

Yapılandırılmış Veriler (Structered Data): Hem yazılımların hem de insanların verimli erişim sağlaması için standartlaştırılmış bir formata sahip verilere yapılandırılmış veriler denir. Bu veriler, veri özniteliklerini açıkça tanımlayan satırlar ve sütunlar ile genellikle tablo şeklindedir. Bilgisayarlar, nicel yapıları nedeniyle öngörüler için yapılandırılmış verileri etkili bir şekilde işleyebilir. Örneğin, sütunlar (ad, adres ve telefon numarası) içeren yapılandırılmış bir müşteri verileri tablosu, toplam müşteri sayısı ve maksimum müşteri sayısına sahip bölge gibi öngörüler sağlayabilir. Bunun aksine, sosyal medya gönderilerinin bir listesi gibi yapılandırılmamış verilerin analiz edilmesi daha zordur[22].

Yapılandırılmış veriler iki gruba ayrılır. Birincisi, **"Yatay Bölümlenmiş Dağıtık Homojen Veriler"**dir. Bu veriler; farklı veri tabanlarında farklı veri sahipleri için aynı yarı tanımlayıcı değerlerini tutan veri tabanları bu gruptaki verileri içerir. Örneğin; e-Devlet Projeleri bu gruptadır. Her bir idare farklı bir veri tabanında vatandaşların farklı özniteliklerini tutar. Örneğin Tapu Kadastro Genel Müdürlüğü, bireyin sahip olduğu gayrimenkulleri tutarken yerel yönetimler bu gayrimenkullere ilişkin bireyin emlak vergisini, Gelir İdaresi Başkanlığı, aynı gayrimenkullerde bireyin kiracısından elde ettiği gelire ilişkin bilgileri kendi veri tabanlarında saklar. Emniyet Genel Müdürlüğü Trafik Dairesi, bireyin sahip olduğu silah ruhsatına ait kayıtları tutarken aynı genel müdürlüğün İstihbarat Şubesi ise başka bir veri tabanında bu silahın karıştığı suçlara ilişkin istihbarat bilgilerini muhafaza eder.

İkinci tür yapılandırılmış veri ise **"Dikey Bölümlenmiş Dağıtık Homojen Veriler"** olarak adlandırılmaktadır. Bu veriler, farklı veri tabanlarında aynı veri sahipleri için farklı öznitelik değerlerini tutan veri tabanları bu gruptaki verileri içerir. Aynı birey için özniteliklerin bir kısmı bir veri tabanında, (bağlantıyı sağlayan alan hariç) ortak olmamak kaydı ile diğer öznitelikler bir başka veri tabanında yer alır. Üretim (araba, lastik, motor, araba camı üreticileri) gibi alanlarda özellikle bir ürünün farklı kısımlarını üreten farklı üreticilerde en sıkça görülen örnekleri yer alır.

[21] Afyonluoğlu, 2019:93
[22] https://aws.amazon.com/tr/what-is/structured-data/ (Erişim: 16.07.2023)

Yapılandırılmış veri, biçimlendirilmiş ve iyi tanımlanmış veri modeline dönüştürülmüş bilgidir. Önceden tanımlanmış biçimlerde bulunur ve tipik olarak ilişkisel bir veritabanında (RDBMS) depolanır. Bu, satırlar ve sütunlar içeren bir tablo biçimine uygun olduğu anlamına gelir.Bu tür veriler hem insanlar hem de makineler tarafından oluşturulur. Yapılandırılmış verileri finansal verilerde, barkodlarda, makine günlüklerinde, müşteri yıldız derecelendirmelerinde vb. bulacaksınız. Örneğin; Excel dosyaları ve SQL veritabanları yapılandırılmış veriler içerir.[23]

Yarı Yapılandırılmış Veriler (Semistructered Data): Yarı yapılandırılmış veriler, normalde bir şema ile ilişkilendirilebilen ve kendini tanımlayan olarak adlandırılan verilerin içinde yer alır. Yarı yapılandırılmış veriler son zamanlarda çeşitli nedenlerle önemli bir çalışma konusu olarak ortaya çıkmıştır[24].

Yarı yapılandırılmış veriler, ilişkisel veritabanları veya diğer veri tabloları biçimleriyle ilişkili veri modellerinin tablo yapısına uymayan, ancak yine de anlamsal öğeleri ayırmak ve kayıt hiyerarşilerini zorlamak için etiketler veya diğer işaretleyiciler içeren bir yapılandırılmış veri biçimidir. Bu nedenle kendini tanımlayan yapı olarak da bilinir. Yarı yapılandırılmış verilerde, aynı sınıfa ait varlıklar bir arada gruplanmış olsalar bile farklı özelliklere sahip olabilir ve niteliklerin sırası önemli değildir. Yarı yapılandırılmış veriler, tam metin belgelerinin ve veritabanlarının artık tek veri biçimi olmadığı ve farklı uygulamaların bilgi alışverişi için bir ortama ihtiyaç duyduğu İnternet'in ortaya çıkışından bu yana giderek daha fazla ortaya çıkmıştır Nesne yönelimli veritabanlarında, genellikle yarı yapılandırılmış veriler bulunur[25].

Yarı yapılandırılmış verilere bazı örnekler BibTex, XML, JSON (JavaScript Object Notatio) dosyaları veya Standart Genelleştirilmiş Biçimlendirme Dili (SGML) belgesi örnek olarak verilebilir. Yarı yapılandırılmış dosyalar, kayıtlardan oluşan rasyonel veriler içerebilir, ancak bu veriler tanınabilir bir yapıda düzenlenemeyebilir. Veri tabanında bazı alanlar eksik olabilir veya kolayca tanımlanamayan bilgileri içerebilir. Yarı yapılandırılmış verilerde, veriler içinde yer alan bilgiler normalde bir veritabanı şeması ile ilişkilendirilir.

Akıllı telefon kullanılarak çekilen her fotoğraf, yapılandırılmamış görüntü içeriği içerir. Ancak, konum, zaman damgası, cihaz kimliği ile de etiketlenirler. Bu nedenle akıllı telefondaki fotoğraflar yarı yapılandırılmış veri olarak değerlendirilir. Yarı yapılandırılmış verilere örnek olarak XML verileri, JSON belgeleri, EDI ve CSV dosyaları verilebilir.[26]

Yapılandırılmamış Veriler (Unstructered Data): Yapılandırılmamış veriler, günümüzün büyük veri dünyasında en yaygın veri türüdür. Bu tür bir veri deposunda, iş kararlarının alınmasına yardımcı olmak için kullanılabilecek çok sayıda yararlı bilgi vardır. Yapay zekâ (AI) ve makine öğrenimi, yararlı sonuçlar elde etmek için büyük miktarda veriyi filtreleyen yeni yazılım çözümleri kullanılmaktadır[27].

[23] https://www.numpyninja.com/post/does-your-data-have-a-structure (Erişim: 16.07.2023)
[24] Buneman, 1997:2
[25] https://en.wikipedia.org/wiki/Semi-structured_data (Erişim:17.07.2023)
[26] https://www.numpyninja.com/post/does-your-data-have-a-structure (Erişim: 16.07.2023)
[27] https://www.questionpro.com/blog/tr/yapilandirilmamis-veri-nedir-ve-ne-ise-yarar/ (Erişim:17.07.2023)

Tablo 2: Yapılandırılmış, Yapılandırılmamış ve Yarı Yapılandırılmış Veriler

Özellikler	Yapılandırılmış Veri	Yapılandırılmamış Veri	Yarı Yapılandırılmış Veri
Organizasyon	İyi organize edilmiş	Hiç organize değil	Kısmen organize
Esneklik ve Ölçeklenebilirlik	Şemaya bağımlı - Bu nedenle daha az esnek ve ölçeklenmesi zor	Şema Yok - Daha esnek ve daha hesaplanabilir	Yapılandırılmamış verilerden daha esnek ve ölçeklendirmesi daha basit
Versiyon Yönetimi	Dizinler, satırlar ve tablolar üzerinde versiyon oluşturma	Versiyon oluşturma bütün bir veri olarak yapılır	Dizinler üzerinden versiyonlama mümkündür
Teknoloji	İlişkisel veri tabanına dayalıdır	Karakter ve ikili verilere dayalıdır	XML/RDF tabanlıdır
Transaction (İşlem) Yönetimi	Olgunlaştırılmış işlem ve çeşitli eşzamanlılık teknikleri mevcuttur	İşlem yönetimi ve eşzamanlılık yoktur	İşlem, DBMS'den uyarlanmıştır, ancak yine de veri eşzamanlılığı mevcut değildir
Örnekler	Finansal veriler, Barkodlar, Derecelendirmeleri başlatın	Medya kayıtları, Videolar, Ses Dosyaları	Hashtag'lere göre düzenlenen Tweetler, konulara göre düzenlenen klasör

Yapılandırılmamış veriler, yasal belgeler, ses, konuşmalar, videolar, fotoğraflar, bir web sitesindeki metin gibi çeşitli formatları ve kaynakları içerir. En yaygın türleri olarak E-postalar, Sosyal Medya, anket yanıtları, yayınlar, iletişim verileri, multimedya dosyaları, belgeler, web sayfaları sayılabilir. Yapılandırılmamış veriler herhangi bir veri modele, formata ve veri tabanlarında olduğu gibi satır ve sütunlara sahip değillerdir. Tanınabilir yapıları olmadığı için bilgisayar programlarının kullanımını zorlaştırmaktadırlar.

Daha fazla insanın dijital hizmetleri ve uygulamaları kullanması nedeniyle hızla genişleyen yapılandırılmamış veriler doğru ve etkin değerlendirilmeleri halinde kurumlar ve işletmeler için oldukça faydalı sonuçlar verebilirler, rakamların ve istatistiklerin aktaramayacağı çeşitli farkındalıklar sunma potansiyeline sahiptirler.

İşletmeler tarafından oluşturulan ve toplanan çoğu yapılandırılmamış verilerin hacmi hızla artmaktadır. Yapılandırılmamış veriler, net bir çerçeveden yoksun olduğu için bilgisayar

programları tarafından kullanılabilmeleri oldukça zordur. Bir veri modeline uymaz ve tanınacak bir yapıya sahip değildirler. Bu tür verilerin çoğu metinden oluşur, ancak tarihler, sayılar ve gerçekler gibi diğer bilgi türlerini de içerebilir.

Yapılandırılmamış veriler, analiz için ayıklanana kadar doğal biçiminde saklanır. Önceden tanımlanmış bir biçimden yoksundur ve doğası gereği ilişkisel bir veritabanında saklanamaz. Yapı eksikliği, bunların araştırılmasını, yönetilmesini ve analiz edilmesini zorlaştırmaktadır. Bununla birlikte, yapılandırılmamış verileri depolama ve işleme yeteneği son yıllarda büyük ölçüde artmıştır. Genellikle veri göllerinde (data lake) depolanan yapılandırılmamış verilerin miktarı, yapılandırılmış verilerinkinden çok daha fazladır. Yapılandırılmamış verileri sosyal medya etkinliğinde, gözetleme görüntülerinde, ses dosyalarında, uydu görüntülerinde vb. Word, Medya günlükleri, Metin, PDF gibi dosyalar yapılandırılmamış veri içerirler.[28]

Yapılandırılmış, Yapılandırılmamış ve Yarı Yapılandırılmış veriler arasındaki bazı farklar Tablo 2'de görülmektedir.

4.2.3 Veri Düzenleme

Veri düzenleme, ham veriyi yeniden düzenleyerek, temizleyerek ve zenginleştirerek daha işlenmiş bir şekle dönüştürme sürecidir. Veri düzenleme, verilerin çeşitli formatlarda ve analizlerde işlenmesini ve anlamlı içgörüler üretmek için başka bir veri setiyle birleştirilmesini gerektirir. Belirli stratejiler, kullanılan verilere ve ulaşmaya çalışılan hedefe göre değişir. Aşağıda veri düzenleme örnekleri verilmiştir[29]:

- Analiz için veri kaynaklarının birleştirilmesi.
- Veri boşluklarının doldurulması veya kaldırılması.
- Gereksiz veya ilgisiz proje verilerini silme.
- Veri aykırı değerlerinin belirlenmesi ve analize izin vermek için bunların açıklanması veya silinmesi.

Veri düzenleme manuel veya otomatik olarak yapılabilir. Veri kümeleri çok büyük olduğunda, bunları otomatik olarak temizlemek çok önemlidir. Kapsamlı bir veri ekibine sahip işletmelerde verilerin düzenlenmesinden genellikle bir veri bilimci veya diğer özel ekip üyeleri sorumludur. Daha küçük şirketler, kullanmadan önce verilerini temizlemek için genellikle veri uzmanı olmayan kişilere güvenmektedir. Verilerin düzenlenmesinin bazı faydaları şunlardır:

1. **Basit analiz:** İş analistleri ve paydaşlar, ham veriler ehlileştirilip dönüştürüldükten sonra en karmaşık verileri bile hızlı, verimli ve etkili bir şekilde inceleyebilir.
2. **Veri işleme:** Prosedür ham, yapılandırılmamış verileri satırlara ve sütunlara dönüştürür. Bu teknik, daha derin bir anlayış elde etmek için verileri zenginleştirir.
3. **Geliştirilmiş hedefleme:** Çeşitli kaynaklardan gelen verileri birleştirmek, hedef kitlenizi daha iyi anlamanıza yardımcı olarak reklam kampanyalarının ve içerik stratejisinin hedeflemesini iyileştirir.
4. **Zaman kullanımı:** Bu teknik, analistlerin düzensiz verileri yönetmek için daha az zaman harcamasına ve anlaşılması kolay verilere dayalı doğru kararlar almak için içgörü elde etmeye daha fazla zaman ayırmasına olanak tanır.

[28] https://www.numpyninja.com/post/does-your-data-have-a-structure (Erişim: 16.07.2023)
[29] https://www.questionpro.com/blog/tr/veri-duzenleme-nedir-ve-izlenecek-adimlar/(Erişim:16.07.2023)

5. **Veri görselleştirme:** Veriler, düzenlendikten sonra sıralamak, analiz etmek ve özetlemek için herhangi bir görsel analitik platformuna aktarılabilir.

4.2.4 Veri Düzenleme Adımları

Veri düzenleme gerçekleştirmek için gerekli adımlar Her veri projesi, nihai veri setinin güvenilir ve kullanılabilir olmasını garanti altına almak için farklı bir stratejiye ihtiyaç duyar. Bunlar sıklıkla gerekli veri düzenleme aşamaları veya faaliyetleri olarak adlandırılır. Veri düzenlemeyi gerçekleştirmek için aşağıda sıralanan adımlar takip edilmelidir.

Şekil 6: Veri Düzenleme Adımları

1. Adım - Keşif: Keşif süreci, veri düzenleme sürecinin ilk adımıdır. Bu, verilerin daha iyi anlaşılmasına yönelik bir adımdır. Verilerinizin kullanımını ve analizini kolaylaştırmak için, verilere bakmalı ve verilerin nasıl düzenlenmesini istediğinizi düşünmelisiniz. Veriler, keşif süreci sırasında eğilimler veya modeller gösterebilir. Bu çok önemli bir adımdır çünkü sonraki tüm eylemleri etkileyecektir. Ayrıca, eksik veya tamamlanmamış değerler gibi bariz sorunları da tanımlar.

2. Adım - Yapılandırma: Çoğu zaman, eksik veya yanlış biçimlendirilmiş ham veriler amaçlanan hedef için uygun değildir. İşlenmemiş verilerin alınması ve daha kolay kullanılabilecek şekilde dönüştürülmesi işlemi veri yapılandırma olarak bilinir. Bu, yeni verilerden ilgili bilgileri çıkarma yöntemidir. Veriler, sütunlar, sınıflar, başlıklar vb. eklenerek bir elektronik tabloda yapılandırılabilir. Bu, analistin analizinde kolayca kullanabilmesi için kullanılabilirliği artıracaktır.

3. Adım - Temizlik: Verilerin temizlenmesi, analizinizi çarpıtabilecek veya kullanışlılığını azaltabilecek kökleşmiş kusurların ortadan kaldırılmasını içerir. Veri temizleme veya düzeltme, analiz için nihai verilerin etkilenmemesini sağlamayı amaçlar. Ham veriler genellikle kullanılmadan önce temizlenmesi gereken hatalar içerir. Veri temizleme, aykırı değerlerin düzeltilmesini, kötü verilerin silinmesini vb. içerir. Verileri temizlerken aşağıdaki sonuçları elde edilir:

- Veri analizi sonuçlarını saptırabilecek aykırı değerler ortadan kaldırılır.
- Kaliteyi ve tutarlılığı artırmak için veri türü değiştirilir ve veriler basitleştirir.
- Yinelenen değerler bulunur, yapısal sorunlar ortadan kaldırılır ve kullanımı kolaylaştırmak için veriler doğrulanır.

4. Adım - Zenginleştirme: Verilere bağlam eklemek, zenginleştirme ile kastedilen şeydir. Bu işlem, önceden temizlenmiş ve biçimlendirilmiş verileri yeni türlere dönüştürür. Bu noktada, hâlihazırda sahip olduğunuz bilgilerden en iyi şekilde yararlanmak için stratejik bir planlama yapılması gerekir. Aşağı örnekleme, yukarı örnekleme ve ardından veriyi artırma, veriyi en rafine haliyle elde etmenin en iyi yoludur. Zenginleştirmenin gerekli olduğunu düşünüyorsanız, elde ettiğiniz ek veriler için yöntemleri tekrarlanması gerekecektir. Verilerin zenginleştirilmesi

adımı isteğe bağlıdır. Hâlihazırda sahip olunan veriler ihtiyaçları karşılamıyorsa, bu adımı uygulanabilir.

5. Adım - Doğrulama: Verilerin doğru, tutarlı, güvenli ve gerçek olmasını sağlamak için tekrarlanan programlama adımları gereklidir. Verilerinizin doğru ve tutarlı olmasını sağlama süreci veri doğrulama olarak bilinir. Bu adım, düzeltilmesi gereken sorunları ortaya çıkarabilir veya verilerin analiz için hazır olduğu sonucuna varabilir.

6. Adım - Yayınlama: Yayınlama, veri düzenlemenin son adımıdır ve tüm sürecin neyle ilgili olduğunu gösterir. Bu, yeni düzenlenmiş verileri sizin ve diğer paydaşların kolayca bulabileceği ve kullanabileceği bir yere koymakla ilgilidir. Bilgiler yeni bir veri tabanına eklenebilir. Önceki adımlar izlendiğinde sürece, içgörüler, iş raporları ve daha fazlası için yüksek kaliteli verilere sahip olunur.

Veri düzenleme, kullanıcı deneyimlerini iyileştirmek için her gün işlenen büyük miktarda veri nedeniyle son yıllarda giderek daha önemli hale gelmiştir. Güçlü bir veri depolama sistemi ve veri düzenleme tekniklerine yapılan yatırımlar olmadan işletme zarar görecektir.

4.3 Veri Entegrasyonu ve Birlikte Çalışabilirlik

Veri entegrasyonu hizmetleri ve çözümleri için en önde gelen kullanım örneklerinden biri, iş ve müşteri verilerinin yönetimidir. Müşterinin müşterisine ve hatta onun da müşterisine kadar giden süreçte ürünü, satışı, ödemeyi veya başka bir değerli bilgiye edinmek için bugün birçok şirket çok ciddi yatırımlar yapmaktadır. Ölçemediğiniz değeri iyileştiremeyeceğiniz gibi, önce o veriyi ölçebilmeniz için veriye sahip olmanız ya da erişebiliyor olmanız gerekmektedir.

Veri entegrasyonu sağlık sektöründe de önemli bir rol oynamaktadır. Farklı hasta kayıtlarından ve kliniklerden elde edilen entegre veriler, farklı sistemlerden gelen verileri yararlı bilgilerle eşleştirilir ve doktorların tıbbi durumları ve hastalıkları teşhis etmelerine yardımcı olur. Etkili veri toplama ve entegrasyon, tıbbi sigortacılar için talep işleme doğruluğunu da geliştirir ve hasta adlarının ve iletişim bilgilerinin tutarlı ve doğru bir şekilde kaydedilmesini sağlar. Farklı sistemler arasındaki bu bilgi alışverişine genellikle birlikte çalışabilirlik denir.

Birlikte çalışılabilirliğin önemi şudur: Hiç bir sistem her işi yapamaz, tek başına tüm işlemleri yapabilecek bir yazılım mevcut değildir. Uygulamaların kendi amaçları dışına çıkmaya başlamaları durumunda yönetilemez ve sürdürülemez hale gelirler. Örneğin kendi uzmanlık alanına göre çalışan iki farklı uygulama iyi bir entegrasyon sayesinde bütünleşik yapısı korunur ve sürdürülebilirliği artar. Örneğin bir ERP sisteminde internet üzerinden satış yapamazsınız fakat bir B2C sistemini ERP'ye tam ve eksiksiz bir biçimde entegre edildiğinde artık ERP'ye uç çözüm olarak geliştirilen B2C sistemi bir anda söz konusu ERP sistemine manevra kabiliyeti ve verimlilik katar. Hem B2C hem de B2B bütünleşik olarak çalışabilen bir ekosistem yaratır ve son kullanıcıya konforlu bir uygulama deneyimi sağlar. Entegrasyon, beklentilerin bu kadar arttığı bir dönemde uygulamaların uyarlanabilirliğini arttıracak, olmazsa olmaz bir olgudur.

Bu aşamada üzerinde durmamız gereken konu veri entegrasyonu için geliştirilen yaklaşımlar olacaktır.

4.3.1 Veri Entegrasyonu Yaklaşımları

Veri entegrasyonu, sistemler arasındaki heterojenliği veri düzeyinde çözerek bilgi sistemlerinin birlikte çalışabilirliğinin sağlanmasına ilişkin sorunları ele alan araştırma alanıdır[30]. Veri entegrasyonu, nihai amacı kullanıcılara konu ve yapı türleri yelpazesinde tutarlı erişim ve veri teslimi sağlamak ve tüm uygulamaların ve iş süreçlerinin bilgi ihtiyaçlarını karşılamak için farklı kaynaklardan gelen verileri tek bir veri kümesinde birleştirme pratiğidir. Veri entegrasyon süreci, genel veri yönetimi sürecinin ana bileşenlerinden sadece bir tanesidir. Uygulamalar büyüdükçe veri paylaşma ihtiyacı artar veya dış sistemlerden gelecek olan veriler ile beslenmeye ihtiyaç duyar.

Veri entegrasyonu mimarları, kaynak sistemlerden hedef sistemlere veri bağlamak ve yönlendirmek için yazılımlar geliştirir. Bu sistemlerin verimliliği sürecin otomatikleşmesi ile doğru orantılıdır. Veri Entegrasyonu sürecinde aşağıdaki yöntemler uygulanır[31].

- **Extract, Transform and Load (Çıkart, Dönüştür ve Yükle):** Farklı kaynaklardan gelen veri kümelerinin kopyaları bir araya toplanır, uyumlu hale getirilir ve bir veri ambarına veya veritabanına yüklenir.
- **Extract, Load and Transform (Ayıkla, Yükle ve Dönüştür):** Veriler, büyük veri sistemine olduğu gibi yüklenir ve belirli analitik kullanımlar için daha sonra dönüştürülür.
- **Change Data Capture (Veri Yakalamayı Değiştir):** Veritabanlarındaki veri değişikliklerini gerçek zamanlı olarak tanımlar ve bunları bir veri ambarına veya diğer havuzlara uygular
- **Data Replication (Veri Çoğaltma):** Bir veritabanındaki veriler, bilgileri operasyonel kullanımlarla senkronize tutmak veya yedeklemek için çoğaltılır.
- **Data Virtualization (Veri Sanallaştırma):** Farklı sistemlerden gelen veriler yeni bir havuza yüklemek yerine birleşik bir görünüm oluşturmak için sanal olarak birleştirilir.
- **Streaming Data Integration (Akış Veri Entegrasyonu):** Farklı veri akışlarının sürekli olarak entegre edildiği ve analitik sistemlere yani veri depolarına gerçek zamanlı bir veri entegrasyonu sağlayan yöntemdir.

Uygulama Entegrasyonu

Veri entegrasyon teknolojileri, ilişkisel veritabanlarının aralarındaki bilgileri verimli bir şekilde taşıma ihtiyacının artmasından dolayı uygulama entegrasyonu kavramları ortaya çıkmıştır. Bu sebeple iki veya daha fazla uygulama arasında canlı, operasyonel verilerin gerçek zamanlı entegrasyonuna uygulama entegrasyonu denir. Uygulama entegrasyonunun nihai amacı, bağımsız olarak tasarlanmış uygulamaların birlikte çalışmasını sağlamaktır. Bu, verilerin ayrı kopyaları arasında veri tutarlılığı, farklı uygulamalar tarafından yürütülen çoklu görevlerin senkronize bir biçimde yürütülmesi ve verilerin işlenmesi demektir. Bağımsız olarak tasarlanmış uygulamalar birbirirleriyle canlı olarak konuşabilmekte ve veri alışverişini kusursuz olarak yapmak hedeflenmektedir.

[30] Koch, 2001:39

[31] https://tr.linkedin.com/company/dokuzsistem?trk=article-ssr-frontend-pulse_publisher-author-card (Erişim: 07.07.2023)

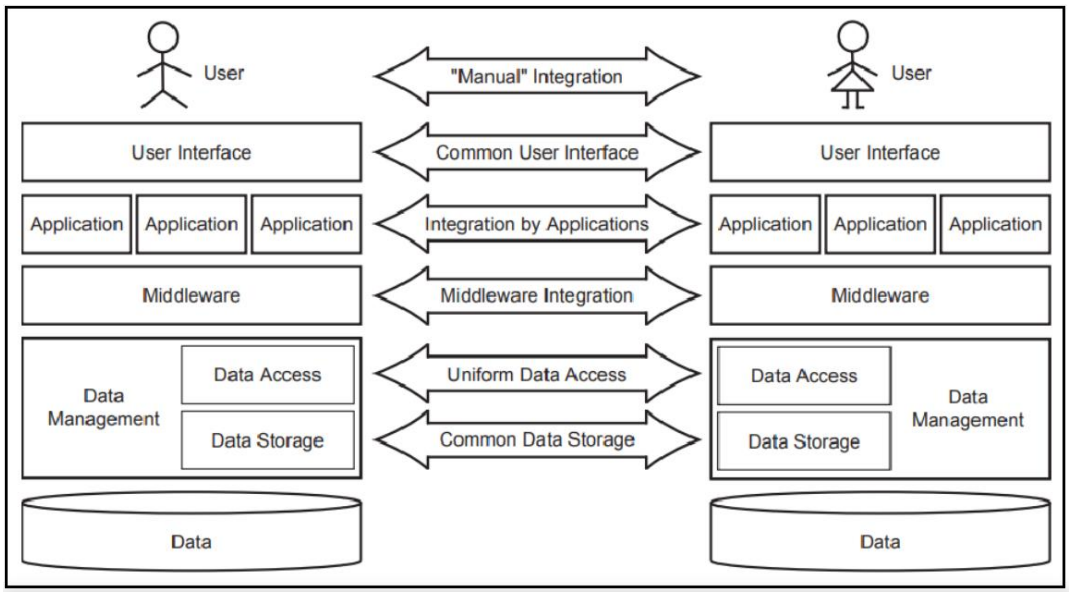
Uygulama entegrasyonunun gerçek zamanlı olarak yapılmasının en mümkün olduğu sistemler genellikle bulut sistemlerdir. Uygulama ile veritabanı arasında bir API (Application Programming Interface - Uygulama Programlama Arabirimi) veya service olmayan sistemlerde canlı tetikleyicilerin olmadığı düşünülürse anlık entegrasyonun yapılabilmesi için veri tabanının önüne bir katman oluşturmak gerekmektedir.

Veri Entegrasyon Araçları

Veri entegrasyon teknikleri, tam otomatik yöntemlerden manuel yöntemlere kadar çok çeşitli yöntemlerle uygulanır ve projelendirilir (Şekil 7).

- **Manual Integration or Common User Interface (Manuel Entegrasyon veya Ortak Kullanıcı Arayüzü):** Verilerin birleşik bir görünümü yoktur. Kullanıcılar, tüm kaynak sistemlere erişerek ilgili tüm bilgilerle çalışır.
- **Application Based Integration (Uygulama Tabanlı Entegrasyon):** Her uygulamaya özel entegrasyon geliştirmek demektir ve her uygulama için ayrı efor harcanacaktır.
- **Middleware Data Integration (Ara Yazılım Veri Entegrasyonu):** Entegrasyon uçları arasında veya veri tabanı katmanı arasına bir ara katman geliştirilir, entegrasyonlar dokümante edilmiş olur ve uç sistemler entegrasyon yaparken daha hızlı proje geliştirilir. Yapılan ara katmanlarda ayrıca loglama mevcuttur ve hata yönetimi bu katmanda yönetilir.
- **Uniform Data Access (Tekdüzen Veri Erişimi):** Veri tabanı verilerinin entegrasyon amacıyla görselleştirilmesi veya ham datanın entegrasyon uçları vasıtasıyla yetkili kullanıcı veya uygulamalar sayesinde okunması /göreselleştirilmesi sağlanır.
- **Common Data Storage or Physical Data Integration (Ortak Veri Depolama veya Fiziksel Veri Entegrasyonu):** Replikasyon mekanizmasına benzese de aynı mantıkta çalışan yöntem değildir. Eski veriler alınacaksa ve canlı veri aktarımı yapılmayacaksa yedek data üzerinde çalışılabilir ve sürekli olarak veri giriş çıkışı olmayan bir data üzerinde geliştirme tamamlanır.

Geliştiriciler, bir veri entegrasyon sistemini elle kodlamak için Structured Query Language (SQL) kullanabilir. Ayrıca, geliştirme sürecini kolaylaştıran, otomatikleştiren çeşitli uygulamalar da mevcuttur.



Şekil 7: Veri Entegrasyon Yaklaşımları

4.3.2 Veri Birlikte Çalışabilirliği

Veri uzayında veri birlikte çalışabilirliği, "Veri Uzayı Yönetimi" ve "Veri Uzayı Yönetişimi" ile ilgili bir konudur. Her iki konuda da ülkemiz ile Avrupa ülkeleri arasında bir uyum her iki taraf için de veri paylaşımı ve dolayısıyla ticari, ekonomik ve diğer ortak çalışmalar açısından önem arz etmektedir. Bu açıdan Avrupa ülkelerinin konu ile yapmış olduğu çalışmalara, devamında ise mevcut hukuki duruma değinmek faydalı olacaktır.

Birlikte çalışabilirlik (Interoperability), bir ürün veya sistemin diğer ürün veya sistemlerle çalışabilme özelliğidir. Terim dar anlamda bilgi sistemleri arasındaki bilgi alışverişine izin vermek anlamına gelirken geniş anlamda sosyal, politik ve organizasyonel faktörler arasındaki bilgi alışverişini kapsar. Birlikte çalışabilirliğin üç türü vardır.

Sözdizimsel birlikte çalışabilirlik (syntactic interoperability): İki veya daha fazla sistem ortak veri formatları ve iletişim protokolleri kullanıyorsa ve birbirleriyle iletişim kurabiliyorsa sözdizimsel birlikte çalışabilirlik sergilerler. XML ve SQL, yaygın veri formatları ve protokollerine örnektir. Alt düzey veri formatları da alfabetik karakterlerin tüm iletişim sistemlerinde aynı ASCII veya Unicode formatında saklanmasını sağlayarak sözdizimsel birlikte çalışabilirliğe katkıda bulunurlar.

Anlamsal birlikte çalışabilirlik (semantic interoperability): İki veya daha fazla bilgisayar sisteminin bilgi alışverişi yeteneğinin ötesinde, her iki sistemin son kullanıcıları tarafından tanımlandığı şekilde faydalı sonuçlar üretmek için değiş tokuş edilen bilgileri anlamlı ve doğru bir şekilde otomatik olarak yorumlama yeteneğidir. Anlamsal birlikte çalışabilirliği sağlamak için, her iki taraf da ortak bir bilgi alışverişi referans modeline başvurmalıdır. Bilgi alışverişi taleplerinin içeriği açık bir şekilde tanımlanmış olmalıdır. gönderilen ile anlaşılan aynıdır.

Etki alanları arası birlikte çalışabilirlik (cross-domain interoperability): Ortak bir çıkar veya bilgi alışverişi için birlikte çalışan çok sayıda sosyal, örgütsel, politik, yasal varlığı içerir[32].

[32] Sartipi ve Dehmoobad, 2008:3

Çeşitli veri kümelerinin anlamlı şekillerde birleştirilmesine veya toplanmasına izin verecek şekilde verilerin biçimlendirilme yollarını ifade eder. FAIR'deki “Ben”i oluşturan FAIR Veri İlkelerinin kilit bir yönüdür[33].

Verilere ve diğer dijital nesnelere erişim ve bunların kullanımı tamamen otomatikleştirildiğinde ve hem insan hem de makine için erişilebilir olduğunda optimum birlikte çalışabilirlik elde edilmiş olur.

Verilerin birlikte çalışabilir olması için olguları aynı şekilde ölçmeleri gerekir; bu, her değişkenin aynı soruyu sorması ve yanıtları aynı şekilde biçimlendirmesi gerektiği anlamına gelir. Bu nedenle, örneğin, bir veri kümesi “doğum tarihiniz nedir” diye sorarsa ve yanıtlar tarih olarak biçimlendirilirse, kişinin yaşını soran ikinci bir veri kümesi, önemli bir veri temizliği olmadan birincisiyle birlikte çalışamayabilir.

Verilerin birlikte çalışabilirliği, meta verilere ve veri belgelerine dayanır, çünkü uygun belgeler olmadan hangi veri kümelerinin ve değişkenlerin karşılaştırılabilir olduğu bilinemez. Verilerin birlikte çalışabilirliği, genellikle verilerin toplanması ve düzenlenmesine yönelik üzerinde anlaşmaya varılan yaklaşımlar olan veri standartlarının kullanılmasıyla gerçekleştirilir. Veri birlikte çalışabilirliği, bir dizi izin verilen yanıtla kesin olarak tanımlanmış sorular olan Ortak Veri Öğelerinin kullanılmasıyla da gerçekleştirilebilir.

4.3.3 Veri Birlikte Çalışabilirlik Standartları

Birlikte çalışabilirlik standartları tüm dijital çıktıların FAIR (Findable, Accessible, Interoperable and Reusable) ilkelerine göre Bulunabilir, Erişilebilir, Birlikte Çalışabilir ve Yeniden Kullanılabilir olmasını sağlamak için farklı sistemler arasında bilgi alışverişi ve paylaşımını mümkün kılmaktadır.[34]

Açık standartlar, önerilen bir ortak protokolün teknik ve ekonomik avantajlarını, dezavantajlarını ve fizibilitesini tartışan satıcılar, akademisyenler ve geliştirmede pay sahibi olan diğerlerinin temsilcilerini içeren, geniş ölçüde istişari ve kapsayıcı bir gruba dayanır. Tüm üyelerin şüpheleri ve çekinceleri giderildikten sonra, ortaya çıkan ortak belge ortak bir standart olarak kabul edilir. Bu belge daha sonra halka yayınlanabilir ve bundan böyle açık bir standart haline gelir.

1. **Kamu birlikte çalışabilirliği:** İlk müdahale ekiplerinin geniş çaplı acil durumlar sırasında iletişim kurabilmeleri gerektiğinden, birlikte çalışabilirlik kolluk kuvvetleri, yangınla mücadele, acil tıbbi hizmetler ve diğer halk sağlığı ve güvenliği kurumları için gerekli ve önemli bir konudur.

2. **E-devlet birlikte çalışabilirliği:** E-devlet perspektifinden konuşursak, birlikte çalışabilirlik, vatandaşlar, işletmeler ve kamu idareleri için sınır ötesi hizmetlerin işbirliği yeteneğini ifade eder.

3. **Masaüstü birlikte çalışabilirliği:** Yazılım birlikte çalışabilirliğinin bir alt kümesidir. İlk günlerde, birlikte çalışabilirliğin odak noktası, web uygulamalarını diğer web uygulamalarıyla entegre etmektir. Zamanla, bu uygulamaların kaydedilebileceği ve daha sonra basit yayınla-abone ol modellerini kullanarak birbirleriyle iletişim

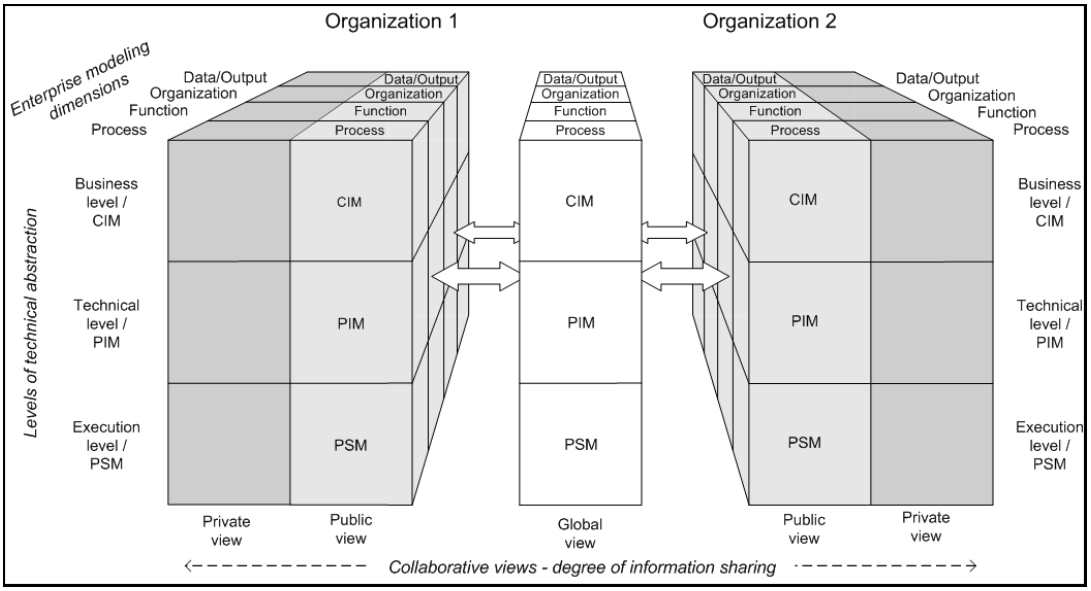
[33] https://www.nnlm.gov/guides/data-glossary/data-interoperability (Erişim:07.07.2023)
[34] Interoperability Standards, 2016:1

kurabilecekleri sanal bir masaüstü ortamı oluşturmak için açık sistem kapsayıcılar geliştirilmiştir.

4. **Arama birlikte çalışabilirliği:** İki veya daha fazla bilgi koleksiyonunun tek bir sorgu ile aranabilmesini ifade eder.

5. **Yazılım birlikte çalışabilirliği:** Birbiriyle ilişkili beş yolla elde edilir. Bunlar; ürün testi, üretim mühendisliği, Endüstri/topluluk ortaklığı, Ortak teknoloji ve IP ve standart uygulamadır.

Bunların her biri, interkomünikasyon yazılımlarındaki değişkenliği azaltmada ve ulaşılmak istenen nihai hedefe ilişkin ortak bir anlayışı geliştirmede önemli bir role sahiptir. İki bilgi sisteminin organizasyonun birlikte çalışabilirliği Şekil 8'de görüldüğü gibi veri, organizasyon, işlev ve süreç boyutlarına sahiptir. Bu organizasyonları tüm boyutlarıyla birlikte çalışabilir hale getiren bir arayüz (global view) tasarlanmalıdır. [35]



Şekil 8: Birlikte Çalışabilir Bilgi Sistemlerinin Mimarisi

Verilerin ve diğer herhangi bir dijital nesnenin (kod, algoritmalar, iş akışları, modeller, yazılım veya dergi makaleleri gibi) FAIR olmasını sağlamak için tasarlanmış spesifikasyonlar, yönergeler veya kriterlere uygun standartların altyapısını oluşturur. Standartlar, makinelerin dijital nesneleri otomatik olarak bulma ve kullanma becerisini geliştirmeye ve bireylerin yaşam döngüleri boyunca yeniden kullanmalarını desteklemeye özel bir vurgu yapmaktadır. Tüm dijital nesnelerin FAIR olmasını sağlamak için belirlenmiş çeşitli standart türleri vardır. Standartların en iyi şekilde nasıl kategorize edileceğine dair bir uzlaşma yoktur. Bu standartlar genellikle aşağıda sıralanan tamamlayıcı ihtiyaçlara cevap verir.[36]

- Açıklama (Description): Makine tarafından işlenebilir açıklamalar (Alıntı, minimum raporlama gereksinimleri, terminolojiler, dosya formatları veya kavramsal modeller),

[35] https://en.wikipedia.org/wiki/Architecture_of_Interoperable_Information_Systems(Erişim:9.7.2023)
[36] Interoperability Standards, 2016:2

- Tanılama (Identification): Tanılama için keşif ve alıntı,
- Erişilebilirlik (Accessibility): Erişim izni, veri koruma, anonimleştirme ve şifreleme,
- Gösterge (Indicator): Göstergeler veya metrikler ile verim ve kalite
- Sürüm Oluşturma (Versioning): Kod ve algoritmalar,
- İzleme (Tracking): Yorumlar ve sonuçlar,
- Analiz (Analysis): Kullanılan iş akışının ve ilgili yazılımın standartlaştırılmış açıklamalar

4.3.3.1 Açık Standartlar

Birlikte çalışabilirlik, açık standartlar kullanılarak geri kalanı hariç tutularak iki ürün arasında özel bir önlem olarak post-facto olarak geliştirilebilir. Bir firma, sistemini açık standartlara dayalı olmayan bir sisteme uyarlamak zorunda kaldığında, bu birlikte çalışabilirlik değil, uyumluluk anlamına gelir. Açık standart, herkesin erişebileceği ve kullanabileceği bir standarttır[37]. Açık standartların genişletilebilirlik sağlayan bir açık lisans kullanması da ön koşuldur. Doğası gereği herkes açık standardın geliştirimesine katkı sunabilir.[38] Açık standardın karşılaması gereken kriterler şunlardır[39]:

- **Kullanılabilirlik:** Herkesin okuması ve uygulaması için açık standartlar mevcuttur.
- **Son Kullanıcı Seçimini En Üst Düzeye Çıkarma:** Açık Standartlar, standardın uygulamaları için adil ve rekabetçi bir pazar yaratır. Müşteriyi belirli bir satıcıya veya gruba mecbur etmezler.
- **Telif Hakkının Olmaması:** Açık standartlar, telif veya ücret olmaksızın herkesin uygulaması için ücretsizdir. Standartlar kuruluşu tarafından uygunluğun belgelenmesi bir ücret gerektirebilir.
- **Ayrımcılık Olmaması:** Açık standartlar ve bunları yöneten kuruluşlar, bir satıcının uygulamasının teknik standartlara uygunluğu dışında herhangi bir nedenle bir uygulayıcıyı diğerine tercih etmez. Sertifikasyon kuruluşları, düşük ve sıfır maliyetli uygulamaların doğrulanması için bir yol sağlamalıdır, ancak gelişmiş sertifika hizmetleri de sağlayabilir.
- **Uzatma veya Alt Küme:** Açık standartların uygulamaları genişletilebilir veya alt küme şeklinde sunulabilir. Bununla birlikte, sertifika kuruluşları alt küme uygulamalarını onaylamayı reddedebilir ve uzantılara gereksinimler getirebilir.
- **Yıkıcı Uygulamalar:** Açık standartlar, standardın bozulmasına karşı koruma sağlayan lisans koşullarını kullanabilir.

4.3.3.2 Meta Veri Standartları

Meta veri standardı, verilerin sahipleri ve kullanıcıları tarafından doğru ve uygun şekilde kullanılmasını ve yorumlanmasını sağlamak için verilerin anlamı veya semantiği hakkında ortak bir anlayış oluşturmayı amaçlar. Bu ortak anlayışı elde etmek için, meta veriler olarak da bilinen bir dizi özellik veya veri özniteliğinin tanımlanması gerekir.[40]

Meta veriler genellikle üç türde kategorize edilir:

[37] https://en.wikipedia.org/wiki/Open_standard#cite_note-3 (Erişim:08.07.2023)
[38] https://www.w3.org/2005/09/dd-osd.html (Erişim:08.07.2023)
[39] https://opensource.com/resources/what-are-open-standards (Erişim:08.07.2023)
[40] MUNIER, Manuel – LALANNE, Vincent - ARDOY, Pierre-Yves – RICARDE, Magali, Legal Issues about Metadata Data Privacy vs Information Security, 8th International Workshop on Data Privacy Management (DPM'2013), Sep 2013, Egham, United Kingdom. pp. 162-177.

- **Tanımlayıcı meta veriler:** Başlık, yazar ve özet gibi öğeler aracılığıyla tanımlama ve erişim için bir bilgi kaynağını tanımlar.
- **Yapısal meta veriler:** Diğer bileşenlere bağlantılar gibi öğeler (bölümleri oluşturmak için sayfaların nasıl bir araya getirildiğ gibi) aracılığıyla nesnelerin içindeki ve arasındaki ilişkileri belgeler.
- **İdari meta veriler:** Dosya yönetimi, hak yönetimi ve koruma amacıyla sürüm numarası, arşivleme tarihi ve diğer teknik bilgiler gibi öğeler aracılığıyla bilgi kaynaklarının yönetilmesine yardımcı olur.

Meta veriler, bilgi güvenliği için önemli araçlardan kabul edilmektedir (belge paylaşımı ve bulut güvenliği için kullanım kontrolü, dijital adli tıp, ispat araçları gibi). Ancak bu teknolojik imkanların uygun güvenlik politikalarının uygulanması ve bilgi izlenebilirliğinin sağlanması, depolanabilecek meta veriler (kişisel veriler, mahremiyet kapsamındakiler gibi), bunların işlenme hüküm ve koşulları gibi hususlar da ele alınmalıdır.

Verilerin anonimleştirilerek işlenmesi ve yeniden kullanımı, ortaya çıkabilecek iş birliklerinde veri türü, veri kategorisi, işlemenin hukuki nedenleri, işlenme amaçları, saklama yöntemleri, saklama süreleri ve tüm bunların ötesinde karşılıklı sorumluluk taahhütlerinin metaveri açısından da belirtilmesi gerekir. Ancak bu noktada metaveri açısından da “geleneksel” veri rejimi mi kabul edilmeli, yoksa ona bağlı veya ondan bağımsız bir düzenleme yoluna mı gidilmeli tartışması da tartışılmaya değerdir. Böyle bir tartışmada da hem ulusal hem de uluslararası düzeyde düzenleyici ve denetleyici düzenlemelerin yeterli olup olmadığına bakılır.

GDPR ile ilişkisi açısından konu değerlendirildiğinde GDPR’ın metaveriye müsaade edip etmediği konuşulmalıdır. Konunun elektronik haberleşmede trafik veya konum (meta)verileri açısından ele alındığı bir örnekten hareketle[41], GDPR’ın meta verileri doğrudan ve açık olarak düzenlemediği, GDPR’ın genel gerekçesinde ise GDPR’ın 49 no.lu şerhi ile bağlantılandırılarak dolaylı olarak meta verileri kabul ettiği ve bunu da bir tür veri olarak etiketlediği ifade edilmelidir[42]. Nitekim GDPR’ın 49 no.lu şerhi ile, kişisel verilerin ağ ve bilgi güvenliğinin sağlanması amacıyla kesinlikle gerekli ve orantılı olduğu ölçüde işlenmesi gerektiği de eklenmiş ve “veri sorumlusunun meşru menfaati” hukuki nedeni ile bağlantı kurulmuştur. Buna göre, bir ağın veya bilgi sisteminin, belirli bir güven düzeyinde, depolanan veya iletilen kişisel verilerin kullanılabilirliğini, gerçekliğini, bütünlüğünü ve gizliliğini tehlikeye atan kazara olaylara veya suç eylemlerine veya hukuka aykırı diğer eylemlere direnme yeteneği; bu ağlar ve sistemler, kamu yetkilileri, bilgisayar acil müdahale ekipleri (CERT'ler), bilgisayar güvenliği olay müdahale ekipleri (CSIRT'ler), elektronik iletişim ağları ve hizmetleri sağlayıcıları tarafından sunulan veya bu ağlar ve sistemler aracılığıyla erişilebilen ilgili hizmetlerin güvenliği ve güvenlik teknolojileri ve hizmetleri ilgili veri sorumlusunun meşru menfaatini oluşturacaktır. Bu meşru menfaat ve buna dayanan davranışlar da örneğin, elektronik iletişim ağlarına yetkisiz erişimin ve kötü niyetli kod dağıtımının önlenmesini ve

[41] 2002/58/EC (Regulation on Privacy and Electronic Communications/ Mahremiyet ve Elektronik Haberleşme Tüzüğü) yürürlükten kaldırmak üzere sunulan elektronik haberleşmede kişisel verilerin ve özel hayatın korunmasına dair Avrupa Parlamentosu ve Konsey Tüzüğü teklifi hükümleri (Bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN) ve Adalet Divanı’nın Tele2 kararı olarak bilinen kararından hareketle, ayrıntıları için Bkz. CJEU C-203/15 ve C-698/15 Tele2 Sverige AB ve Secretary of State for the Home Department, ECLI:EU:C:2016:970; https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=101544

[42] https://etno.eu/datas/positions-papers/2018/ETNO_Metadata_Memo.pdf

“hizmet reddi (denial of service)” saldırılarını ve bilgisayar ve elektronik iletişim sistemlerine verilen zararı durdurmayı içerebilir. Ağların güvenliğini ve bilgi güvenliğini sağlamak için gerekli olan bu tür işlemeler, tipik olarak bir telekomünikasyon bağlamında meta verilerin işlenmesini de içereceğinden GDPR'ın metaverileri de dolaylı olarak kabul ettiği ve bunu bir tür bilgi olarak etiketlediği sonucuna varılır. Bu anlamda meta verilerin (kişisel veri ile örtüşmesi halinde) GDPR md. 6/ 1 (f) uyarınca veri sorumlusunun meşru menfaati nedenine dayanılarak işlenmesinin mümkün olabileceği söylenebilir. Bunun için de veri sorumlusunun meşru menfaatleri için öngördüğü amaçlar açısından işlemenin gerekli olması ve kişisel verilerinin korunması gereken ilgili kişinin menfaatleri veya temel hak ve özgürlüklerinin veri sorumlusunun meşru menfaatlerin önüne geçmesi aranmaktadır ki bu durum özellikle veri öznesinin çocuk olduğu hallerde daha da önem kazanır.

Türk hukukunda da KVKK md. 5/ 2 (f) ile veri sorumlusunun meşru menfaati ile işleme hukuki nedeni düzenlenmektedir. Ancak Kişisel Verileri Koruma Kurulu’nun da kararlarında sıklıkla vurguladığı üzere, meşru menfaat ile işleme şartı açısından Türk hukukunda aydınlatma yükümlülüğü ayrıca önemlidir. Türk hukukunda metaveri özelinde henüz bir düzenleme yoktur. Bir an için veri sorumlusunun meşru menfaat işleme nedenine dayanarak bir işleme gerçekleştirdiği düşünüldüğünde, kişinin hem menfaatler dengesinin belirlenmesi ve anlaşılması hem de veri sorumlusunun meşru menfaatlerinin neler olduğu hakkında tam bilgilendirilmesi konusu açmaza girmektedir. Buradaki, işleme nedeni elbette KVKK md. 5/ 1. fıkrasındaki açık rıza değildir. Ancak meşru menfaatler konusunda yapılan açıklamada istenen aslında ilgili kişinin, kavramsal olarak rıza olmasa da meşru menfaat nedeniyle işleme zorunluluğuna ikna olmasıdır. Şayet ülkemizde de metaveri üzerinden yapılacak (kişisel) veri işlemeleri konusunda bir değerlendirme yapılacak olur ise, KVKK ve Kişisel Verileri Koruma Kurulu açısından dayanılabilecek hukuki neden yine veri sorumlusunun meşru menfaati olacak ve yine yukarıda sayılan unsurlara riayet beklenecektir, diye değerlendirmekteyiz.

4.3.4 Veri Taşınabilirliği ve Birlikte Çalışabilirliğe İlişkin Hukuki Tablo

GDPR md. 20 uyarınca veri öznesi, bir veri kontrolörüne sağladığı kendisiyle ilgili kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makinece okunur bir formatta alma ve bu verileri başka bir veri kontrolörüne iletme/ taşıma hakkına sahip olacaktır. Veri kontrolörü tarafında da veri öznesini hiçbir engel ile karşılaştırmadan, birlikte çalışabilirliğin, temin edilmesi ve taşımanın sağlanması gerekmektedir. GDPR md. 20’ye göre;

- İşleme faaliyetinin, GDPR’ın “veri öznesinin bir ya da daha fazla sayıda spesifik amaca yönelik olarak kişisel verilerinin işlenmesine onay vermesi” işleme şartını düzenleyen md. 6/ 1 (a) bendi veya “Birlik veya üye devlet hukuku çerçevesinde 1. paragrafta belirtilen yasağın veri öznesi tarafından kaldırılamayacağına ilişkin bir hüküm sağlanması haricinde, veri öznesinin belirtilen bir veya daha fazla sayıda amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık bir şekilde rıza göstermesi”ni düzenleyen md. 9/ 2 (a) bendi uyarınca bir rızaya veya “veri öznesinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri öznesinin talebiyle adımlar atılması için, işleme faaliyetinin gerekli olması”nı öngören md. 6/ 1 (b) bendi uyarınca bir sözleşmeye dayanması;
- İşleme faaliyetinin otomatik yollarla gerçekleştirilmesi gerekmektedir.

Veri taşınabilirliği hakkının kullanımı, başkalarının hak ve özgürlüklerine de müdahale etmemelidir.

Ayrıca Madde 29 Kişisel Veri Çalışma Grubu rapor ve rehberlerinde de konu, kişisel kendi verileri üzerindeki self-determinasyon, self-kontrolü ile ilgili vurgu üzerinden ele alınmaktadır. Buna göre kişinin kendi verileri üzerinde kontrol ve tasarruf hakkı vardır. Verisinin kontrolörler arası taşınması da bu bağlamda onun talebi ile sağlanmalıdır. Kaldı ki aynı kabule göre, kontrolörler arası bu kesişim, Avrupa Birliği'nin dijital tek pazar stratejisine de katkı sağlayacaktır.

Türk hukukunda 6698 sayılı KVKK ve diğer mevzuat düzenlemelerinde veri taşınabilirliğine ilişkin bir düzenleme doğrudan yok ise de bazı spesifik alanlarda veri taşınabilirliği ve birlikte çalışabilirlik düzenlemeleri getirilmeye başlanmıştır. İlk örnek mobil numara taşınabilirliğidir. 2009 yılında yayımlanarak yürürlüğe giren Numara Taşınabilirliği Yönetmeliği ile muhtelif yollar ile abonenin telefon numarasını mobil telekomünikasyon hizmet sağlayıcıları arasında taşınmasını istemesi mümkün hale gelmiş olup uygulanagelmektedir.

Ayrıca Avrupa Bankacılık Otoritesi (EBA, European Banking Authority) düzenleyici standardı olarak 2017'de yayınlanan düzenlemesinde (Payment Services Directive, PSD2)[43] ile bankacılık sistemi üzerinden gerçekleştirilecek olan veri taşınabilirliği ve yalnızca bankalar arası değil bankaların üçüncü taraf kuruluşlar ile de veri alıp verme noktasında teknik yeterlilikler geliştirmeleri gerektiği ve bunların neler olduğuna ilişkin hükümler getirilmiştir. Türk hukukunda da 2013'te yürürlüğe giren 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun ile bu EBA düzenlemesine uyum sağlanmıştır. Zorunlu açık bankacılık yolu ise Cumhurbaşkanlığı 11. Kalkınma Planı[44] ve 2020 Yıllık Programı[45] ile açılmıştır. 2020 yılında yürürlüğe giren "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" hükümleri ile de "müşterilerin ya da müşteriler adına hareket eden tarafların API, web servis, dosya transfer protokolü gibi yöntemlerle bankanın sunduğu finansal servislere uzaktan erişerek bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri elektronik dağıtım kanalı" şeklinde açık bankacılık tanımlanmış; bankaların API ve FTP alt yapılarını temin etmeleri için tanımlar ve gereklilikler ifade edilmiş; ayrıca TCMB'nin 01.12.2022 tarih ve 2022/ 48 sayılı duyurusu[46] ile Ödeme Hizmetleri Veri Paylaşım Servisleri'ni hayata geçirmek adına TCMB ile Bankalararası Kart Merkezi (BKM) tarafından geliştirilen ve taraflara standart Açık Bankacılık işlemleri sunulmasını sağlayan 'Açık Bankacılık Geçidi' (GEÇİT) altyapısı üzerinden hizmet vermeye başladığı duyurusu yapılmıştır. Bu noktada da hem finans kuruluşları arasındaki veri taşınabilirliği ve birlikte çalışabilirlik, hem de tüketicinin tek platform üzerinden dağınık halde bulunan verilerine bir arada erişebilirliğinin yolu açılmış ve buna ilişkin teknik yeterlilikler getirilmiş, uygulanmaya da başlamıştır.

[43] European Commission, 2017, Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_4961. (Son Erişim Tarihi: 20.03.2023)

[44] T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı 100. Yıl Türkiye Planı, On Birinci Kalkınma Planı (2019-2023) https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Plani-2019-2023.pdf

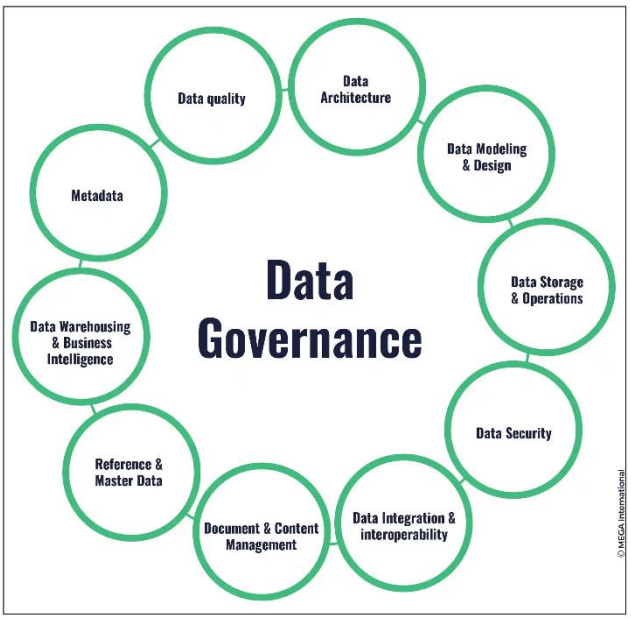
[45] 2020 Yılı Cumhurbaşkanlığı Yıllık Programı, 04.11.2019 tarih ve 30938 sayılı Resmi Gazete.

[46] https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Duyurular/Basin/2022/DUY2022-48

4.4 Veri Yönetişimi

Veri yönetişimi, bir kuruluştaki verilerin güvenli ve tutarlı olmasını sağlamak amacıyla geliştirilmiş bir dizi politika, prosedür, standart ve uygulamalardır. Veri yönetişim çerçevesi ise, önemli veri varlıklarının kuruluş genelinde resmi olarak yönetilmesini sağlayan süreç olarak tanımlanmaktadır. Veri yönetişimi ve çerçevesi, veri hizmetlerinin gerçekleşmesine hizmet eden temel unsurlardır. Bu bağlamda, veriler hem operasyonel hem de stratejik kararları etkilediği ifade edilebilir.[47]

Başarılı bir veri yönetişim programı iş süreçlerini yürütmek, doğru karar almak ve dijital dönüşümleri güçlendirmek için verileri daha güvenilir olmasını sağlar. Bu tür bir program, veri hacimleri – ve kaynakları – arttıkça ve teknolojiler geliştikçe, ölçeklendirme yapabilir ve uyum sağlayabilir. Veri yönetişiminin bileşenleri Şekil 9'da görülmektedir. [48]



Şekil 9: Veri Yönetişimi Bileşenleri

Avrupa veri uzayında yalnızca teknik yönlere değil, aynı zamanda kaynakların paylaşımı için yönetim, liderlik ve stratejiye de önem verilir. Bu anlamda Veri Uzayları Destek Merkezi[49] (Data Spaces Support Centre - DSSC) Avrupa veri uzayının yasal, teknik ve operasyonel olarak veri ekosistemi içinde veri paylaşımı için veri yönetişimini destekler. Güvenilir veri havuzu oluşturma, veri işleme ve paylaşmayı kolaylaştırmak için ilgili veri altyapılarının ve yönetişim çerçevelerinin bir araya getirilmesi gereklidir.[50]

Avrupa Veri Stratejisi, Avrupa veri uzayının, verilere erişim ve verilerin işlenmesine ilişkin hakları şeffaf ve adil bir şekilde belirleyen ve ilgili AB mevzuatı ile uyumlu veri yönetişim yapılarının oluşturulmasını öngörmektedir.[51] Ayrıca, verilerin yeniden kullanımı ve erişimine

[47] ŞEN Cem ve diğerleri, 2021:427.
[48] https://www.mega.com/blog/what-is-data-governance-and-why-is-it-important (Erişim: 08.07.2023)
[49] Data Spaces Support Centre, 2023:15
[50] European Commission, 2023:26
[51] https://eur-lex. europa.eu/legal-content/EN/TXT/ PDF/?uri=CELEX:52020DC0066 &from=EN (Erişim:07.07.2023)

ilişkin gereklilikleri belirlemek ve veri pazarındaki aktörler arasındaki güveni artırmak için bir çerçeve oluşturarak, örneğin güvenilir veri aracılık hizmet sağlayıcılarının (Data Intermediation Service Provider-DISP) kurulmasını ve "Veri Yönetişim Yasası" çıkartılmasını desteklemektedir.

Stratejinin çıkarmayı hedeflediği "Veri Yönetişimi Yasası" (Data Governance Act - DGA), 3 Haziran 2022 tarihinde Avrupa Birliği Resmî Gazetesi'nde yayımlanmış olup 15 aylık bir dönemin ardından Eylül 2023'ten itibaren yürürlüğe girmiştir. Yasa, veri paylaşımına olan güveni ve veri kullanılabilirliğini artırmaya yönelik mekanizmaları güçlendirmeyi ve verilerin yeniden kullanılmasının önündeki teknik engelleri kaldırmayı amaçlamaktadır. Veri Yönetişimi Yasası aynı zamanda sağlık, çevre, enerji, tarım, mobilite, finans, imalat, kamu yönetimi gibi sektörlerde hem özel hem de kamu oyuncularını içeren stratejik alanlarda ortak Avrupa veri alanlarının kurulmasını ve geliştirilmesini desteklemektedir.[52]

Veri yönetişimi;

- Veri uzayına erişim, kontrol ve kullanım şeklinin yönetimini,
- Veri uzayından değer üretmenin ve değerin aktörler arasında yeniden dağıtılmasının değerlendirilmesi ve kontrolünü,
- Kararları kimin verebileceğini,
- Verilere ve sanal alana nasıl erişileceğini, kontrol edileceğini, kullanılacağını,
- Verilerden nasıl yararlanılacağını etkileyebilecek veri uzayı hakkında derinlemesine düşünme ve karar verme sürecini belirler.

Bu nedenle, bir veri uzayını çalıştıran ve hedeflerini karşılayan farklı kuruluşlar tarafından gerekli eylemleri (ve etkileşimleri) yapılandırmak ve koordine etmek için veri yönetişimine ihtiyaç vardır.

Şubat 2022'de Avrupa Komisyonu, AB Konseyi'nin talebi üzerine, Avrupa veri uzayının gidişatına genel bir bakış sağlayan Personel Çalışma Belgesi (Staff Working Document - SWD) yayınlamıştır.[53]

Ortak Avrupa Veri Uzayına (SWD) ilişkin veri uzayı yönetişimi, ilgili paydaşların yeterli ve ayrımcı olmayan temsilini içermesi gerektiği belirtilmekte ve "veri havuzunu ve paylaşımını kolaylaştırmak için ilgili veri altyapıları ile yönetişim çerçevelerini bir araya getirmek" olarak tanımlamaktadır.

4.5 Türkiye'de Veri Uzayı Yönetimine İlişkin Değerlendirme

Veri uzayı yönetimi, kurumlar ve özel şirketlerin sistemlerinde barındırdıkları çok büyük hacimli yapılandırılmış, yapılandırılmamış ve yarı yapılandırılmış verileri (büyük veri) kapsar. Yüksek kapasiteli veri işleme teknikleri ve bulut tabanlı sistemler ile veri yorumlama ve yönetmeye yönelik yaklaşımlar ve uygulamalar sürekli olarak gelişme göstermektedir. Buna karşılık veri konusundaki belirsizlikler, politikaların ve düzenlemelerin yetersizliği ve karmaşıklığı ciddi sorunlara yol açmaktadır.[54]

[52] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act (Erişim:09.07.2023)
[53] European Commission, 2023:3
[54] Alkan ve diğerleri, 2020:2

Kamu kurumları vatandaşlara, küresel şirketler ise müşterilere ve kullanıcılara ilişkin çok büyük veri toplamaktadır. Bu verilerin güvenliğinin sağlanamaması ve ayrıntılı kullanıcı profili çıkarılması kişisel mahremiyet için tehdit oluşturmaktadır.[55] Bu ve benzer tehditleri ortadan kaldırmak için etkin bir veri uzayı yönetim sisteminin öncelikle ele alınması ve kurulması gerekmektedir. Veri uzayı yönetiminin en önemli bölümünü oluşturan kişisel veri yönetimi konusu ise ülkemiz açısından KVKK'nın GDPR ile uyumlu hale getirilmesini zorunlu kılmaktadır. Ayrıca etkin bir veri yönetişimi altyapısı kurum ve kuruluşların depoladıkları verilerin çeşitliliği, hızı ve hacminin sürekli artması nedeniyle her geçen gün daha etkili bir yönetim aracı kullanılmalıdır. Ülkemizde veri uzayı yönetiminin önündeki genel problemlerden bazıları şunlardır:[56]

- Veri yönetimi ve veri güvenliği ile ilgili öngörü eksikliği
- Veri yönetimi performans düzeylerini koruma konusundaki zorluk
- Değişen veri gereksinimlerine uyum sağlayamama
- Verileri kolayca işleme ve dönüştürme ihtiyacı
- Verileri sürekli olarak verimli bir şekilde depolama ihtiyacı
- Bilgi Teknolojileri (BT) alanındaki gelişmeler ve olaylara hızlı tepki verememe
- Maliyetleri optimize etme talebi
- Çalışanlar ve kullanıcılarda veri güvenliği konusunda farkındalık düzeyinin yetersizliği

Ülkemizde veri uzayı yönetiminin başarılı şekilde yürütülebilmesi için veri uzayı ile ilgili idari, teknik ve hukuki alanda çalışan kurum ve kuruluşların sorunların çözümü için bütünlük içerisinde ve koordineli olarak etkili ve hızlı şekilde çalışmaları gerekmektedir. Yapılacak çalışmaların özellikle kamu kurum ve kuruluşlarında bulunan sorunlara odaklanılarak aşağıdaki önerilerin uygulanmasının veri uzayı yönetimine güç kazandıracağını ifade etmek yerinde olacaktır.

- Veri uzayı yönetme ve veri işleme (verileri toplama, depolama, işleme, muhafaza etme, paylaşma, aktarma vs.) konusunda kamu ve özel sektör için bağlayıcı olan birincil ve İkincil mevzuat çalışmalarının tamamlanması,
- Ülkeler arası sözleşmelere ve standartlara uyum için gerekli adımların atılması,
- Veri ihlallerini minimum seviyeye indirmek amacıyla gerekli teknik, idari ve hukuki tedbirlerin alınması,
- Yönetici ve çalışanların bilgilendirmesi ve yetki ve sorumlulukların açık şekilde ortaya konması,
- Teknolojik gelişmelere adapte olmanın önündeki bürokratik ve finansal engellerin kaldırılması,
- Bu alanda uzman insan kaynağını artırmaya yönelik orta ve yükseköğretim ile mesleki eğitimin yaygınlaştırılması sağlanması,
- Uygulama alanında kamu, özel sektör ve akademi işbirliği için uygun bir mekanizma kurulması,
- Verinin yönetimi konusunda idari ve hukuki süreçlerin hızlandırılması,
- Etkili bir denetim mekanizmasının kurulması,
- Veri yönetişimi ile veri birlikte çalışabilirliğini sağlamaya yönelik teknik ve idari altyapı güçlendirilmesi

[55] Alkan ve diğerleri, 2020:16
[56] https://www.oracle.com/tr/database/what-is-data-management/ (Erişim:15.07.2023)

gerekmektedir.

5 Veri Uzayı Güvenliği, Gizliliği ve Mahremiyeti

Günümüzde kullandığımız teknolojilerin çoğu tamamen bilgiye ve veriye dayanmaktadır. Bilgi çağının en değerli madeni olan verinin güvenliği, büyük önem taşır. Doğal olarak da Veri uzayının güvenliği ve gizliliği önemle ele alınması gereken bir konu haline gelmiştir. Çok katmanlı veri uzayı hem ülke genelinde hem de kişisel anlamda güvenliğe ihtiyaç duymaktadır.

Veri güvenliği (data security), veri uzayının yıkıcı güçlerden ve siber saldırı veya veri ihlali gibi yetkisiz erişim, değiştirme, ifşa veya yok edilmeden korunmasını sağlayan bir dizi önlem ve uygulamayı içeren bir kavramdır. Veri güvenliği, bilgisayar sistemleri, ağlar, veritabanları, bulut depolama, mobil cihazlar ve diğer bilgi işlem altyapılarındaki verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı hedefler. Gizlilik, Bütünlük ve Erişilebilirlik olarak isimlendirilen üç temel unsurlardan herhangi biri zarar görürse güvenlik zaafiyeti oluşur.

Gizlilik: Bilginin yetkisiz kişilerin eline geçmesinin ve yetkisiz kişilerin erişime karşı korunmasıdır. Bilgiyi herhangi bir yerde sakladığımızda ya da iletmek istediğimizde bu bilginin yalnızca ilgili tarafın görmesini isteriz. Gizliliğin sağlanmasında kullanılan başlıca teknoloji olarak şifreleme teknolojisini söyleyebiliriz.

Bütünlük: Bilginin kişiler tarafından değiştirilmemesi, tam ve eksiksiz olmasıdır. Bilginin saklandığı alanda istenmeyen kişiler tarafından değiştirilmesi, tahrip edilmesi veya silinmesinin önlenmesi gerekir. Bütünlüğün korunmasında kullanılan teknolojiler arasında elektronik imza, açık anahtar altyapısı gibi kavramlar kullanılabilir.

Erişilebilirlik: Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır. Bilgiye istendiği anda ilgili kişinin ulaşım sağlaması gerekir. .

Her yıl on binlerce kullanıcının (gizli) verisi kötü niyetli siber saldırganlar tarafından ele geçirilmektedir. Bu durum finansal kayıpların yaşanmasında ve çoğu zaman kullanıcılarda güven azalmasına, kurum/kuruluşların itibarının zarar görmesine yol açmaktadır. Son yıllarda veri güvenliği alanında sosyal mühendislik, fidye yazılımı ve APT gibi gelişmiş tehditler yükselişe geçmiştir. Bunların tümü kurum/kuruluşların verilerinin korunmasında mücadele edilmesi zor olan ve yıkıcı hasara yol açabilen tehditlerdir.

5.1 Veri Güvenliği Tedbirleri

Veri güvenliği tedbirleri, verilerin yetkisiz erişim, değiştirme, ifşa veya yok edilme gibi tehditlere karşı korunmasını sağlayan önlemlerdir. Veri güvenliği tedbirleri, bireylerin, kurum/kuruluşların verilerini korumak için alınması gereken önemli adımlardır.

Küresel anlamda bu konuda yapılan çalışmalar incelendiğinde, yeterince büyük veri uzayları tanımlanarak, her veri uzayı için güvenlik ve gizlilik tedbirleri ayrı ayrı tanımlandığı görülmüştür.

Verilerin paylaşılmaması gereken durumlar: Veri paylaşımının özellikle paylaşan kişi açısından sıkıntı yaratacağı durumlar aşağıda üç madde halinde belirtilmektedir.

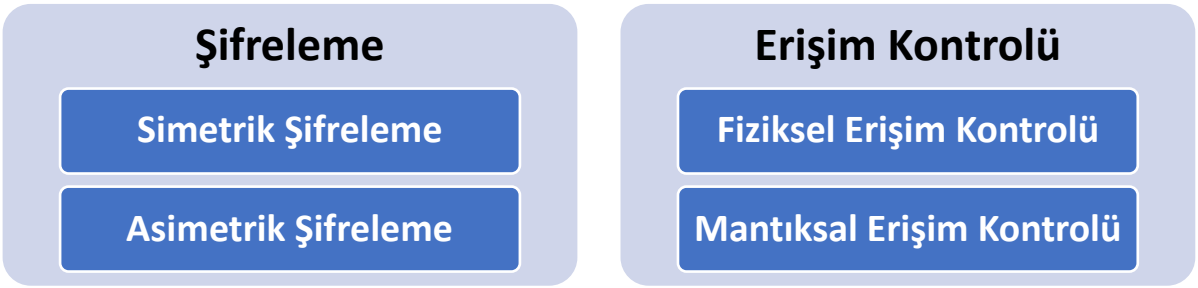
- Fikri mülkiyet haklarını veya ticari bir sözleşmeyi ihlal etme olasılığı varsa, verilerin finansal bir değerinin olması durumunda,

- Kişisel, hassas ve gizli verilerle ilgili etik sorunlar söz konusu olduğunda anonimleştirmenin yeterince gizlilik sağlayamadığı ya da mümkün olmadığı durumlarda, katılımcılara verilerin paylaşılacağını açık olarak ifade eden ve onaylarının alındığı aydınlatılmış onam imzalatılmamışsa,
- Veri sahibinin net olarak belirlenemediği durumlarda.

Veri'nin erişim bilgilerinin yer aldığı, "veri hakkında veri" olarak kullanılan, "Meta Veri" veya "Üst Veri" olarak adlandırılan bilgi ve veri hayatlarını beraber sürdürmelidir. Bu sayede verinin nasıl paylaşılacağı, nasıl kullanılacağı, kimlerin erişim yetkisinin olduğu, veri üreticisi (veya yayımcısı) tarafından belirtilebilmektedir. Bu tanımlamaya "Veri Lisanslaması" adı verilmektedir. Henüz çok fazla veri lisanslama modeli bulunmamaktadır. Ulakbim tarafından araştırma yapan akademisyenler için Açık Lisanslama[57] modelleri önerilmiştir. Bu gibi ortak lisans modelleri oluşturularak veri paylaşımının daha verimli olması sağlanabilir.

5.1.1 Şifreleme ve Erişim Kontrolü

Verilerinizi şifreleyebilen veya yok edebilen fidye yazılımı gibi saldırıların yanı sıra verilerinizi değiştirebilen veya bozabilen saldırılara karşı verilerinizi korumayı içerir. Daha önce de üzerinde durduğumuz gerekli olan kişilerin verilere erişebilmesini sağlar. Hassas verilerin şifrelenmesi, verilere yetkisiz erişimi önlemek için etkili bir tedbirdir.



Şekil 10: Şifreleme ve Erişim Kontrolü

Şifreleme; verileri okunabilir bir biçimden (düz metin) okunamayan kodlanmış bir biçime (şifreli metin) dönüştürme yöntemidir. Şifreleme, verileri anlaşılır halden şifreli bir forma dönüştürmek için bir şifreleme algoritmasını kullanır. Bu şifrelenmiş veriler, yalnızca doğru şifreye sahip olan kişiler tarafından çözülebilir ve okunabilir hale gelir. Yalnızca şifre çözme anahtarı kullanılarak şifrelenmiş verilerin şifresi çözüldükten sonra veriler okunabilir veya işlenebilir. Genel olarak, asimetrik veya simetrik anahtar kullanımı sağlanır.

Simetrik Şifreleme (Symmetric Encryption) algoritmalarında, veriyi şifrelemek ve çözmek için aynı anahtar kullanılır. Hem gönderici hem de alıcı aynı gizli anahtarın sahibi olmalıdır. En yaygın simetrik şifreleme algoritmalarından biri, Advanced Encryption Standard (AES) olarak bilinir.

[57] https://acikders.ulakbim.gov.tr/mod/page/view.php?id=102

Asimetrik Şifreleme (Asymmetric Encryption), veriyi şifrelemek için kullanılan bir gizli anahtar ve veriyi çözmek için kullanılan ayrı bir açık anahtar çifti vardır. Gönderici, alıcının açık anahtarını kullanarak veriyi şifreler ve alıcı, kendi özel anahtarıyla bu şifreyi çözer. Asimetrik şifreleme örnekleri arasında RSA ve ECC (Elliptic Curve Cryptography) bulunur.

Erişim Kontrolü, bilgisayar sistemleri, ağlar, fiziksel mekanlar veya diğer kaynaklara yetkisiz erişimi önlemek için kullanılan bir güvenlik yöntemidir. Erişim kontrolü, belirli kaynaklara kimlerin, ne zaman, nereden ve nasıl erişebileceğini kontrol etmek için kullanılır. Erişim kontrolü, genellikle iki ana kategori altında incelenir.

Fiziksel Erişim Kontrolü, fiziksel alanlara erişimi kontrol etmek için kullanılır. Örneğin, ofislerde, veri merkezlerinde veya diğer kritik mekanlarda, kimlerin bu alanlara girebileceği ve hangi saatlerde erişime izin verileceği gibi fiziksel güvenlik önlemlerini içerir. Bu tür erişim kontrolü, güvenlik kameraları, kartlı geçiş sistemleri, biyometrik kimlik doğrulama gibi teknolojilerle uygulanabilir.

Mantıksal Erişim Kontrolü, bilgisayar sistemleri, ağlar ve dijital verilere erişimi kontrol etmek için kullanılır. Bu tür erişim kontrolü, kullanıcıların kimlik doğrulamasını gerektiren parola, kullanıcı adı, çift faktörlü kimlik doğrulama gibi yöntemlerle gerçekleştirilir. Kullanıcılara sadece belirli yetkilerle erişim verilebilir ve hassas verilere veya işlevlere yalnızca yetkili kullanıcılar erişebilir.

5.1.2 Kimlik Doğrulama (Authentication)

Dijital dünyada güvenliği sağlamak ve yetkisiz erişimi önlemek için son derece önemli bir önlem ve prosedür olan kimlik doğrulama, kullanıcının veya cihazın, kendini iddia ettiği kimliğin gerçekliğini kanıtlama sürecidir. Bu süreç, bir sistem veya kaynağa erişmeye çalışan kişinin gerçekten kim olduğunu belirlemek ve doğrulamak için kullanılır. Doğrulanmış bir kimlikle sisteme giriş yapılmasını sağlamak hassas verileri korumak, yetkisiz erişimi engellemek ve güvenlik açıklarını minimize etmek için önemlidir.

Kimlik doğrulama genellikle şu yöntemlerle gerçekleştirilir:

1. **Parola Doğrulama:** Kullanıcının belirlenmiş bir parolayı girerek kimliğini doğruladığı temel yöntemdir. Parolalar, genellikle karmaşık ve güçlü olmalıdır.
2. **Çift Faktörlü Kimlik Doğrulama (Two-Factor Authentication - 2FA):** Parola dışında ek bir doğrulama adımı daha eklenir. Örneğin, bir parola ve SMS ile gönderilen doğrulama kodu gibi.
3. **Biyometrik Kimlik Doğrulama:** Parmak izi, yüz tanıma, retina taraması veya ses tanıma gibi fiziksel özelliklere dayalı kimlik doğrulama yöntemleridir.
4. **Kimlik Kartları ve Akıllı Kartlar:** Kimlik kartları, çipli kartlar veya akıllı kartlar kullanılarak kimlik doğrulama sağlanabilir.
5. **OAuth ve Tek Oturum Açma (Single Sign-On - SSO):** Bu yöntemde, kullanıcılar birden fazla uygulamaya veya sistemlere aynı kimlik bilgileriyle giriş yapabilirler.

5.1.3 Yetkilendirme

Yetkilendirme (Authorization), veri güvenliği ve sistem güvenliği için temel bir yapı taşıdır. Doğru ve güvenilir bir yetkilendirme mekanizması, yetkisiz erişimlerin önlenmesine, hassas bilgilerin korunmasına ve güvenli bir ortamın sağlanmasına yardımcı olur. Yetkilendirme (Authorization) kullanıcıların belirli kaynaklara veya sistemlere erişip erişemeyeceğinin

belirlendiği süreçtir. Kimlik doğrulama (authentication) adımından sonra, kullanıcının kimliği doğrulanmış olsa bile, bu kullanıcının hangi kaynaklara veya işlemlere erişim izni olduğunu belirlemek için yetkilendirme yapılması gerekir.

Yetkilendirme, erişim kontrolüne dayanır ve kullanıcılara belirli haklara veya izinlere sahip olma yetkisi verir. Kullanıcıların yetkilendirilmesi, kimlik doğrulama sonrasında sisteme erişim düzeyini tanımlar. Kullanıcılar, yetkilendirme politikaları tarafından belirlenen roller ve izinlerle, sistemdeki kaynaklara erişebilirler.

Yetkilendirmeyi doğru şekilde sağlamak için önemli noktalar;

İhtiyaca uygun yetki verilmeli: Yetkilendirme yöntemi, sistemin ihtiyaçlarına ve kullanım senaryolarına uygun olarak tasarlanmalıdır. Farklı sistemler ve uygulamalar, farklı yetkilendirme gereksinimleri ve karmaşıklık düzeyleri ile karşı karşıya kalabilir. Bu nedenle, yetkilendirme mekanizması, sistemin ihtiyaçlarına uygun ve ölçeklenebilir olmalıdır.

İlkeler belirlenmeli: Yetkilendirme politikaları ve izinler, "en az ayrıcalık" prensibiyle tasarlanmalıdır. Kullanıcılar, sadece işleri için gerekli minimum izinlere sahip olmalıdır. Bu, yetkisiz erişimi ve içerideki tehditleri en aza indirmeye yardımcı olur.

Rol tabanlı yetkilendirme yapılmalı: Kullanıcıları, roller ve bu rollerle ilişkilendirilmiş izinlerle gruplandırmak, yetkilendirme yöntemlerinin daha yönetilebilir ve esnek olmasını sağlar. Kullanıcıların rolleri, görevlerine veya sorumluluklarına göre belirlenmelidir.

Güvenlik denetimleri yapılmalı: Yetkilendirme işlemleri, güvenlik denetimleri ve kayıtlarla desteklenmelidir. Bu, kimin, ne zaman ve hangi kaynaklara erişim sağladığını izlemeyi ve takip etmeyi kolaylaştırır.

Sık güncelleme ve değerlendirme yapılmalı: Yetkilendirme politikaları ve izinler düzenli olarak gözden geçirilmeli ve kullanıcıların rolleri ve yetkileri, iş değişiklikleri veya organizasyonel yapıya göre güncellenmelidir.

Kullanıcı eğitimlerinin verilmesi: Kullanıcıların yetkilendirme mekanizmasını doğru şekilde kullanması için eğitilmeleri önemlidir. Güçlü parola kullanımı, izin istekleri ve diğer güvenlik bilincini artırmak için kullanıcıların bilinçlenmesi gerekir.

5.2 Veri Uzayında Gizlilik Koruması

5.2.1 Anonimleştirme ve Takma Adlandırma

Anonimleştirme bireye ulaşılmasını sağlayan tüm tanımlayıcı bağlantıların veriden kaldırılması anlamına gelir. Bununla birlikte tüm tanımlama yöntemlerinde olduğu gibi dolaylı tanımlayıcılar ve/veya ilgili veri kümelerine bağlantılar yoluyla bireyleri tanımlamak hala mümkün olabilir. Bu sebeple verilerin anonimleştirilmesi konusu tüm dünyada çeşitli tartışmalara konu olmaktadır. Buna rağmen araştırma verilerinin yönetimi süreçlerinde verilerin anonimleştirilmesi (anonymization) veya takma adlı hale getirilmesi (pseudonymization) büyük önem taşımaktadır. Anonimleştirme ile takma adlı hale getirme arasındaki temel fark Tablo 3'te gösterildiği gibidir.

Tablo 3. Anonimleştirme Ve Takma İsim Kullanarak Revize Etme Örnekleri

İsim	**Anonimleştirme**	**Takma isim kullanma**
Yılmaz, E	anonim	P31Y7
Şahin, D	n/a	Z41G9
Turan, H	anonymous	C98K9
Yetkin, S	xxx	H45B7

Anonimleştirme sürecinde yazara ilişkin hiçbir bilgi tutulmazken, takma isim kullanımında adlandırma araştırmacı tarafından üretilen takma isimlerle yapılır. Bu sayede bireyin gizliliği korunarak birden fazla veri kümesinde tanımlanmış verilerin aynı kişiye bağlanması olanaklı hale gelir.

Araştırma katılımcılarının kimliklerinin korunabilmesi için verilerin anonimleştirilmesi sürecinde aşağıda belirtilen konular büyük titizlikle değerlendirilmesi ve uygulanması gereklidir:

- Anonimleştirmenin kombinasyon halinde bir bireyi tanımlayabilen doğrudan ve dolaylı tanımlayıcıları veriden kaldırmak anlamına geldiği,
- Araştırmanın henüz tasarım aşamasında anonimleştirme sürecinin planlanması gerektiği,
- Gerektiğinde otomatik anonimleştirme araçlarının (Cornell Anonymization Toolkit veya ARX gibi) kullanılabileceği,
- Anonim veri paylaşmanın dahi sorun yaratabileceği durumlarda kontrollü erişim ortamları veya sınırlayıcı lisansların kullanılabileceği

Araştırmacılar, verilerini anonimleştirmeye ve anonimleştirilmiş verilerini yeniden tanımlama riskini yönetmeye yardımcı olmak için algoritma tabanlı araçları giderek daha fazla kullanıyor. Anonimleştirme araçlarının örnekleri şunları içerir:

- Cornell Anonymization Toolkit
- ARX open source data anonymization software

Veri anonimleştirildiğinde, kişi ile veri arasındaki bağlantı tamamen ortadan kalkar. Veri kümesinin kullanıcıları artık birden fazla kaydın aynı kişiye ait olup olmadığını anlayamaz. Veriler takma ad haline getirildiğinde, aynı kişinin mi yoksa farklı kişilerin mi yanıt verdiği açıktır. Ancak, hem anonimleştirilmiş hem de takma adlandırılmış veri setlerinin yeniden tanımlama riskleri içerdiğini unutmamak önemlidir.

Hukuki çerçevede ele alındığında, anonimleştirme ile takma adlandırma (psödonimizasyon) arasındaki fark şöyle ifade edilmektedir:

“Verilerin anonimleştirilmesi", ilgili olduğu kişinin kimliğinin tespit edilmesini geri dönülmez bir şekilde engellemek amacıyla işlenmesi anlamına gelir. Kimliği belirli veya belirlenebilir bir gerçek kişiyle ilgili değilse veya veri öznesinin kimliği belirlenemeyecek veya artık belirlenemez hale gelecek şekilde anonim hale getirilmişse, verilerin etkin ve yeterince anonimleştirilmiş olduğu kabul edilebilir.[58]

Anonimleştirme alanında belirli bir tekniğin veri sahiplerinin kimliğini korumada %100 etkili olacağını söylemek imkansızdır. Anonim hale getirme durumunda, 'tanımlama' ile bir kişinin adının ve/veya adresinin elde edilmesi olasılığının yanı sıra, ayırma, bağlantı kurulabilirlik ve çıkarım yoluyla potansiyel olarak belirlenebilirliği kastedilmektedir.[59]

“Psödonimizasyon” ise verilerin herhangi bir tanımlayıcı özelliğinin bir takma adla veya başka bir deyişle, veri öznesinin doğrudan tanımlanmasına izin vermeyen bir değerle değiştirilmesi anlamına gelir. GDPR, Psödonimizasyonu, (a) bu tür ek bilgilerin ayrı tutulması ve (b) kişisel verilerin kimliği belirli veya belirlenebilir bir bireye atfedilmemesini sağlamak için teknik ve organizasyonel önlemlere tabi olması koşuluyla, kişisel verilerin artık ek bilgiler kullanılmadan belirli bir veri sahibiyle ilişkilendirilemeyecek şekilde işlenmesi olarak tanımlar.

Psödonimizasyonun birçok kullanımı olmasına rağmen, dolaylı yollarla tanımlamaya izin verdiği için birçok durumda veri öznelerinin kimliği için yalnızca sınırlı bir koruma sağladığı için anonimleştirmeden ayırt edilmelidir. Psödonimizasyonun yapıldığı durumlarda, altta yatan veya ilgili verileri analiz ederek veri öznesini belirlemek genellikle mümkündür.

5.3 Gizlilik Düzenlemeleri ve Uyum

Gizlilik düzenlemeleri ve uyum konusu ele alındığında teknik gereklilikler ile birlikte bu gereklilikleri belirleyen, düzenleyen ve sonrasında denetleyen bir idari ve hukuki altyapı bulunduğu dikkate alınmalıdır.

Türkiye’de AB Veri Yönetişim Yasası muadili sayılabilecek bir düzenleme bulunmadığı, ancak, Türkiye’de 6698 Kişisel Verileri Koruma Kanunu’nun, 18 Ocak 2016'da tasarı olarak meclise girmiş ve 24 Mart 2016 tarihinde kabul edilmiş olduğu, 7 Nisan 2016 tarihinde ise 6698 sayılı kanun olarak 29677 sayılı Resmî Gazete' de yayımlanmış ve sonrasında yürürlüğe girmiş olduğu yukarıda ifade edilmiş idi. Kişisel Verileri Koruma Kurulu (KVKK), Türkiye'de kişisel verilerin korunmasını sağlamak ve denetlemek amacıyla kurulmuş olan resmi bir kurumdur. KVKK, kişisel verilerin işlenmesi, toplanması, saklanması, paylaşılması ve kullanılması süreçlerini düzenleyen yasal düzenlemelerin uygulanmasını ve uyumunu sağlamaktan sorumludur. Bu kapsamda, KVKK, kişisel verilerin güvenliği ve gizliliği konularında yönergeler ve politikalar geliştirir, denetimler yapar, cezai yaptırımlar uygular ve bireylerin veri haklarını korur. Amacı, hem bireylerin kişisel verilerinin korunmasını sağlamak hem de veri işleyen kurum ve kuruluşların uyumunu ve sorumluluğunu denetlemektir.

[58] Data Protection Commission, Guidance Note: Guidance on Anonymisation and Pseudonymisation, Haziran 2019, s. 2-3. https://www.dataprotection.ie/sites/default/files/uploads/2022-04/Anonymisation%20and%20Pseudonymisation%20-%20latest%20April%202022.pdf

[59] Data Protection Commission, Guidance Note: Guidance on Anonymisation and Pseudonymisation, Haziran 2019, s. 3. https://www.dataprotection.ie/sites/default/files/uploads/2022-04/Anonymisation%20and%20Pseudonymisation%20-%20latest%20April%202022.pdf

Bugüne kadar, Kişisel Verilerin Korunması Kanunu'nun farklı alanlarını uygulamaya koymak amacıyla çeşitli yönetmelikler yayımlanmıştır. Bunlar:

- Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik (Resmi Gazete'de 28 Ekim 2017 tarihinde yayımlanmış, 30224 sayılı)
- Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esasları Hakkında Yönetmelik (Resmi Gazete'de 16 Kasım 2017 tarihinde yayımlanmış, 30242 sayılı)
- Veri Sorumluları Sicil Kaydı Hakkında Yönetmelik (Resmi Gazete'de 30 Aralık 2017 tarihinde yayımlanmış, 30286 sayılı)
- Kişisel Verileri Koruma Kurumu'nun Teşkilatı Hakkında Yönetmelik (Resmi Gazete'de 26 Nisan 2018 tarihinde yayımlanmış, 30403 sayılı)
- Aydınlatma Yükümlülüğüne İlişkin Usul ve Esaslar Hakkında Tebliğ (Resmi Gazete'de 10 Mart 2018 tarihinde yayımlanmış, 30356 sayılı)
- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ (Resmi Gazete'de 10 Mart 2018 tarihinde yayımlanmış, 30356 sayılı)
- Kişisel Verileri İşleyen Veri Sorumlularının Özel Nitelikli Kişisel Verilerin İşlenmesinde Alacakları Uygun Önlemlere İlişkin Karar (Kişisel Verileri Koruma Kurulu'nun 31 Ocak 2018 tarihli, 2018/10 sayılı kararı)

Bunların yanı sıra, Türk Ceza Kanunu No. 5237 gibi genel kanunlar ve Elektronik Haberleşme Kanunu No. 5809 gibi sektörel kanunlar da veri korumasına değinmektedir.

Ülkemizde, mevcut düzenlemelerin güncel veri çalışmalarını kapsamaması nedeniyle, veriye ilişkin, güncel gelişmeleri ele alan ayrı bir veri yönetişim düzenlemesine ihtiyaç duyulmaktadır. Bu düzenleme, hızla değişen veri ortamında veri güvenliği, veri paylaşımı, veri saklama süreleri ve diğer ilgili konuları kapsayan kapsamlı bir çerçeve sağlayarak, Türkiye'nin veri yönetimine uygun bir altyapı oluşturmasını ve gelecekteki veri odaklı çalışmalara etkin bir şekilde yanıt vermesini sağlayacaktır.

Konu özellikle kamu kurumlarının birbirleri arasında ve özel sektör ile olan ilişkileri bağlamında veri yönetişimi açısından değerlendirildiğinde, Veri Yönetişim Yasası üzerinde, kamu kurumları özelinde yapılacak bir değerlendirmenin, Türk hukukundaki müstakbel düzenlemelerin dile getirilmesi açısından da önemli olacağı değerlendirilmektedir. konu, kişisel veri özelinde ele alındığında ise AB Veri Yönetişim Yasası'nda, bu düzenlemenin, GDPR ile düzenlenen hususlara halel getirmeden, diğer bir ifade ile GDPR ile uyumlu olarak uygulanacağı öngörülmektedir.

5.3.1 Veri Mahremiyeti

Mahremiyet, kişisel veri kapsamında geçerli olan bir kavramdır. Kişisel verilerin uygun şekilde kullanıldığını ve/veya işlenmiş olduğunu garanti eder. Örnek olarak sağlık sektörünü düşünecek olursak; Hastaların kişisel bilgilerinin doğru şekillerde toplanmasını, paylaşılmasını ve kullanılmasını sağlamak için politikalar oluşturmak ve yetkilendirme gereklilikleri oluşturmak gibi, bireyin kişisel verilerinin kullanımına ve yönetişimine odaklanır.

Kişisel veri çok genel bir tanımdır. Avrupa Birliği mevzuatında[60] tanımlanan GDPR'de 'kişisel veri'; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi anlamına gelir.

[60] http://www.privacy-regulation.eu/en/r26.htm

Tanımlama işlevi kişiden kişiye değişebilir. Genel bir tanım yapmak gerekirse;

- Doğrudan tanımlayıcı
- Dolaylı tanımlayıcı
- Yarı tanımlayıcı

gibi tanımlar yapmak gerekebilir. Bu tanımlayıcılar henüz Türkiye mevzuatında yer almıyor. Avrupa'da örneklerinin olduğunu görüyoruz.

Bir kişiyi tanımlamak için tek başına yeterli olan bilgiler, bir kişinin tam adını, TC Kimlik Numarasını, sosyal güvenlik numarasını, kişisel adını içeren e-posta adresini ve biyometrik tanımlayıcıları (parmak izleri, yüz görüntüsü, ses kalıpları, iris taraması, el geometrisi veya manuel imza) içerir. Bu tür verilere doğrudan tanımlayıcılar denir. Doğrudan tanımlayıcılar, açık bir şekilde bulunulmaması gerekli olduğu artık biliyoruz.

Bir kişiyi oldukça kolay bir şekilde tanımlamak için kullanılabilecek diğer bilgilere Dolaylı Tanımlayıcılar olarak adlandırılmaktadır. Bunlar; Örnek olarak; posta adresi, telefon numarası, araç tescil numarası, kişi tarafından bir yayının bibliyografik alıntısı, kişisel ad biçiminde olmayan e-posta adresi.

Bu bilgiler haricinde, öğrenci kimlik numarası, banka hesap numarası, Bilgisayar yerel IP adresi gibi bilgiler, bir grup içerisinden bir bireyi kesin tanımlamak için kullanılabilecek tanımlayıcılar olduğundan bunları da Dolaylı Tanımlayıcılar olarak değerlendirilebilir.

Yarı Tanımlayıcılar, kendi başlarına birinin kimliğini belirlemek için yeterli olmayan, ancak diğer mevcut bilgilerle bağlantılı olduğunda bir kişinin kimliğini anlamak için kullanılabilen türden bilgilerdir. Örneğin yaş, cinsiyet, eğitim, istihdam durumu, ekonomik faaliyet ve mesleki durum, sosyo-ekonomik durum, gelir, medeni durum, iş yeri veya öğrenim durumunu içerir.

Tarih, dolaylı bir tanımlayıcı veya yarı tanımlayıcı olarak değerlendirilebilir. Doğum tarihi en yaygın örnektir, ancak ölüm tarihleri ve haber değeri taşıyan olayların tarihleri de diğer bilgilerle birleştirildiğinde araştırma verilerinde dolaylı tanımlayıcılar olabilir. Sağlık ve tıbbi araştırmalarda, tedavi ve numune alma tarihleri de bazen başka bilgilerle bağlantılı olduğunda dolaylı tanımlayıcılar olabilir.

Ancak bu noktada unutulmamalıdır ki, bilhassa "kişisel veri" üzerinden konu değerlendirildiğinde, kişisel verinin yalnızca belirli olanlar açısından değil, "kişi"yi ve "kişisel"i belirlenebilir kılan unsurlar açısından da bu doğrudan/ dolaylı/ yarı tanımlayıcıların pek çok durumda entegre biçimde ele alınması gerekecektir.

5.3.2 Uyum Süreçleri ve Gizlilik Kavramları

Veri güvenliği noktasında anlık müdahaleler veyahut gerektiğinde yapılacak işlemlerden ziyade, uluslararası ve ulusal mecralarda düzenlemelerde yapılmaya çalışılan bütüncül uyum/ compliance süreçleridir. Bu sayede yalnızca teknik gereklilikler açısından değil, hukuki ve idari organizasyon bakımından da eş zamanlı ve eş yönetimli yürüyen bir süreç kurgulanmak ve yürütülmek durumundadır.

Bu doğrultuda, *Privacy by Design* (Tasarım Gereği Gizlilik) ve *Privacy by Default* (Varsayılan Olarak Gizlilik) kavramları Türk hukukunda yer almayan ve fakat GDPR ile düzenlenen iki ilkedir. Buna karşın Türkiye'de yapılan kişisel veri uyum süreçlerinde bu ilkeler dikkate

alınmamakta, bir kişisel veri ve/ veya veri güvenliği uyum süreci tümüyle yasal birtakım belgelerin teminine veyahut bazı programların cihazlara yüklenmesine indirgenmektedir.

GDPR Madde 25 uyarınca veri kontrolörü, son teknoloji, uygulama maliyeti ve işlemenin niteliği, kapsamı, bağlamı ve amaçları ile işlemenin gerçek kişilerin hak ve özgürlüklerine yönelik değişen olasılık ve şiddetteki risklerini dikkate alarak hem işleme araçlarının belirlenmesi sırasında hem de işlemenin gerçekleştiği sırada uygun teknik ve organizasyonel önlemleri uygulamak, veri koruma ilkelerini uygulamak için "pseudonymisation" (takma ad-rumuz kullanma, bulanıklaştırma)[61] gibi veyahut GDPR'ın gerekliliklerini karşılamak ve veri öznelerinin haklarını korumak için veri minimizasyonu gibi yollarla etkili bir şekilde ve gerekli güvenceleri işleme süreçlerine entegre etmek durumunda olacaktır. Diğer bir ifade ile, bir projenin/ faaliyetin/ veri işlemeye ilişkin sürecin en başından itibaren, veri koruma sürecinin tasarlanarak hayata geçirilmesi, projenin temeline atılan başat unsurlardan birinin veri güvenliği olması, alt yapının ilk baştan buna göre tasarlanmasıdır denilebilir. Bu ise külli bir çalışmayı gerektirir. Teknik gerekliliklerin, hukuki altyapının ve idari organizasyonun buna göre düzenlenmesini gerektirecektir.

Privacy by design'ın yedi temel ilkesi olduğu kabul edilmektedir:[62]

1. Proactive not reactive—preventative not remedial/ **Reaktif değil proaktif – düzeltici değil önleyici** (*saldırı olayını gerçekleşmeden önce tahmin et, tanımla, önle; olaydan sonra değil önce harekete geç*)
2. Lead with privacy as the default setting/ **Gizliliğin varsayılan/ fabrika ayarı olarak yönetilmesi** (*Kişisel verilerin tüm BT sistemlerinde veya iş uygulamalarında, herhangi bir kişi tarafından herhangi bir ek işlem yapılması gerekmeden otomatik olarak korunmasını sağla*).
3. Embed privacy into design/ **Gizliliğin tasarım sürecinde yerleştirilmiş olması** (*Mahremiyet önlemleri eklentiler değil, sistemin tam bileşeni/ unsuru olmalıdırlar*.)
4. Retain full functionality (positive-sum, not zero-sum)/ **Tam profesyonelliği sürdürmek (sıfır toplam değil pozitif toplam)** (*Privacy by Design, tüm meşru sistem tasarım hedeflerine yönelik bir "kazan-kazan" yaklaşımı kullanır; yani, hem mahremiyet hem de güvenlik önemlidir ve her ikisini de elde etmek için gereksiz ödünler verilmesi gerekmez.*)
5. Ensure end-to-end security/ **Uçtan uca-baştan sona güvenlik** (*Veri yaşam döngüsü güvenliği, tüm verilerin gerektiğinde güvenli bir şekilde saklanması ve artık ihtiyaç duyulmadığında imha edilmesi gerektiği anlamına gelir.*)
6. Maintain visibility and transparency—keep it open/ **şeffaflık ve görülebilirliğin devam ettirilmesi** (*Paydaşlara iş uygulamalarının ve teknolojilerin hedeflere göre çalıştığı ve bağımsız doğrulamaya tabi olduğu konusunda güvence verin.*)
7. Respect user privacy—keep it user-centric/ **Kullanıcı mahremiyetine saygı, kullanıcı merkezli olma** (*Her şeyi kullanıcı merkezli tutun; bireysel gizlilik çıkarları, güçlü gizlilik varsayılanları, uygun bildirim ve kullanıcı dostu seçeneklerle destekleyin.*)

[61] GDPR'ın ifade ettiği anlamda "pseudonymisation" anonimleştirmenin bir türü olarak karşımıza çıkmaktadır. Ayrıntılı bilgi için Bkz. Information Commissioner's Office, Chapter 3: pseudonymisation Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance, February 2022, https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf

[62] Deloitte – Ryerson University, Privacy by Design Setting A New Standard for Privacy Certification s2

Privacy by default da yine GDPR Madde 25 ile düzenlenmekte olup veri kontrolörü, by default/ fabrika ayarı olarak/ varsayılan biçimde işlemeyi, yalnızca, belirlediği her bir amaç özelinde yapabilecektir. Bu yükümlülük, toplanan kişisel verilerin miktarı (veri minimizasyonu), işlenme kapsamı, saklanma süresi ve erişilebilirliği için geçerlidir. Özellikle, bu tür önlemler, kişisel verilerin "*by default*", kişinin müdahalesi olmadan sınırsız sayıda gerçek kişiye erişime açılmayacağını garanti eder. Bir başka ifade ile, veri kontrolörü, tıpkı *privacy by design*'da olduğu gibi, daha işin başında en sıkı "önce gizlilik" prensibiyle hareket etmek ve gizlilik ve veri güvenliği ayarlarını en baştan sıkı biçimde yapmak zorundadır. Bu anlamda hem *privacy by design*'ın hem de *privacy by default*'un potansiyel risk değerlendirmesi ve potansiyel risklerin en aza indirilmesi süreci olduklarını söylemek yanlış olmayacaktır.

5.3.3 Veri Paylaşımı Sorunları

Veri paylaşımı, iş dünyası ve toplum için büyük öneme sahiptir. Doğru bir şekilde yönetildiğinde, veri paylaşımı işbirliğini teşvik eder, inovasyonu artırır ve daha etkili kararlar alınmasına yardımcı olur.

Veri paylaşım sürecini etkileyebilecek bir dizi sorundan söz edilebilmektedir. Bu sorunlar arasında, verinin ortak bir dil ve standardı olmaması, kurumlar arasında farklı teknolojilerin kullanılması ve veri entegrasyonunda yaşanan zorluklar yer almaktadır. Ayrıca, dijital okuryazarlık seviyesinin düşük olması ve hatalı veri girişlerinin olması, veri kirliliği sorununu beraberinde getirmektedir. Nitelikli BT personeli eksikliği, iş devir sürelerinin kısalığı ve buna bağlı olarak yaşanabilen kurumsal hafıza kayıpları da karşılaşılan sorunlardan biridir. Verinin potansiyel faydalarının bilinmemesi, veri mahremiyetine ilişkin farkındalığın düşüklüğü, KVKK uyumunun eksikliği ve iletişim eksiklikleri de veri paylaşımının etkinliğini etkileyen faktörler arasında yer almaktadır. Ayrıca, siber güvenlik altyapısının yetersizliği, veri tabanı yazılımlarının açık kaynak kodlu olmaması ve metaveri ile büyük veri kullanımının sınırlı olması da teknik sorunlar arasında gösterilebilir. Bu sorunların çözülmesi ve iyileştirilmesi, veri paylaşımının etkinliğini ve faydalarını artıracaktır.Bu sorunlarla başa çıkmak için, veri paylaşımı sürecinde uygun güvenlik önlemleri alınmalı, veri standardizasyonu ve entegrasyonu için ortak yöntemler ve protokoller benimsenmeli, veri kalitesi kontrol mekanizmaları oluşturulmalı, yasal ve düzenleyici uyum sağlanmalı, veri sahipliği ve sorumluluk konuları netleştirilmeli ve kültürel/organizasyonel engeller aşılmalıdır.

Kişisel verilerin aktarımı her hukuk sistemi içerisinde sorunlu görülen ve tartışılan hususlardan biridir. Gerek yurtiçi gerekse yurt dışı aktarım noktasında Türk hukuku ve GDPR düzenlemeleri ve uygulamaları açısından konunun ayrı ayrı değerlendirilmesi gerekmektedir.

GDPR Madde 44 ve devamında kişisel verilerin bir başka ülkeye veya uluslararası organizasyona aktarılması düzenlenmektedir. Buna göre, işlenmekte olan veya aktarıldıktan sonra işlenmesi amaçlanan kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarımı konusunda GDPR hükümleri uygulanacaktır (Madde 44). Madde 45 ile bir "yeterlilik kararı" kriteri getirilmiştir. Buna göre Komisyon, kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarımı konusunda söz konusu üçüncü ülkenin veyahut üçüncü ülke içindeki bir veya daha fazla belirli sektörün veya uluslararası kuruluşun yeterli düzeyde koruma sağladığına karar verecek ve bu yeterlilik kararı üzerine buralarla aktarım gerçekleşebilecektir. Böyle bir kararın varlığı halinde ayrıca bir devir/ aktarım kararı aranmayacaktır.

Komisyon bu yeterlilik kararını değerlendirirken şu kriterleri dikkate alır (Madde 45/2):

- Hukukun üstünlüğü, insan haklarına ve temel özgürlüklere saygı, kamu güvenliği, savunma, ulusal güvenlik ve ceza hukuku dahil olmak üzere hem genel hem de sektörel ilgili mevzuat ve kamu makamlarının kişisel verilere erişimi ve bunların uygulanması kişisel verilerin başka bir üçüncü ülkeye veya uluslararası kuruluşa daha sonra aktarılmasına ilişkin kurallar da dahil olmak üzere mevzuat, veri koruma kuralları, mesleki kurallar ve güvenlik önlemleri, o ülke veya uluslararası kuruluşta uyulan kurallar, içtihatlar, etkili ve uygulanabilir veriler kişisel verileri aktarılan veri sahipleri için konu hakları ve etkin idari ve yargısal tazminat;
- Etkin işleyiş ve hakların kullanılması ve Üye Devletlerin denetim makamlarıyla işbirliği yapmak için veri öznelerine yardımcı olmak ve tavsiyelerde bulunmak için yeterli uygulama yetkileri de dahil olmak üzere veri koruma kurallarına uyumu sağlamak ve uygulamakla yükümlü üçüncü ülkede veya uluslararası bir kuruluşun tabi olduğu bir veya daha fazla bağımsız denetim makamının varlığı,
- İlgili üçüncü ülke veya uluslararası kuruluşun üstlendiği uluslararası taahhütler veya yasal olarak bağlayıcı sözleşmelerden veya belgelerden ve özellikle kişisel verilerin korunmasına ilişkin olarak çok taraflı veya bölgesel sistemlere katılımından kaynaklanan diğer yükümlülükler.

Komisyon bu yeterlilik kararını en geç dört yıllık periyotlarla gözden geçirme mekanizması sağlar (Madde 45/ 3) ve mevzuatın takibini ülkeler/ bölgeler bazında sağlar (Madde 45/ 4).

GDPR Madde 46 ile ise uygun güvencelere tabi aktarımlar düzenlenmiştir. Hükme göre, Madde 45 ile öngörülen biçimde bir yeterlilik kararı bulunmaması halinde veri kontrolörü veya veri işleyen, kişisel verileri yalnızca kontrolör veya işleyenin uygun korumaları sağlaması halinde ve veri öznelerinin uygulanabilir hakları ve veri sahipleri için etkili yasal yollar olması kaydıyla aktarabilirler. Buradaki “uygun güvenceler” bir denetim makamından herhangi bir özel izin alınması gerekmediği ve gerektiği haller olarak iki fıkrada düzenlenmiştir.

Buna göre bir denetim makamından herhangi bir özel izin alınması gerekmeksizin aşağıdakiler tarafından sağlanabilir (Madde 46/2):

- Kamu makamları veya organları arasında yasal olarak bağlayıcı ve uygulanabilir bir araç;
- Madde 47 ile düzenlenen bağlayıcı kurumsal kurallar/ bağlayıcı şirket kuralları;
- Madde 93/ 2'de atıfta bulunulan inceleme prosedürüne uygun olarak Komisyon tarafından kabul edilen standart veri koruma hükümleri;
- Bir denetim makamı tarafından kabul edilen ve Madde 93/ 2'de atıfta bulunulan inceleme prosedürü uyarınca Komisyon tarafından onaylanan standart veri koruma maddeleri;
- Üçüncü ülkedeki kontrolörün veya işleyenin veri öznelerinin hakları da dahil olmak üzere uygun güvenceleri uygulamaya yönelik bağlayıcı ve uygulanabilir taahhütleriyle birlikte Madde 40 uyarınca onaylanmış bir davranış kuralları; veya
- Üçüncü ülkedeki kontrolörün veya işleyenin veri öznelerinin hakları da dahil olmak üzere uygun güvenceleri uygulamaya yönelik bağlayıcı ve uygulanabilir taahhütleri ile birlikte Madde 42 uyarınca onaylanmış bir belgelendirme mekanizması.

Yetkili bir denetim makamından izin alınması gereken hallerde ise uygun güvenceler şunlar tarafından sağlanabilir (Madde 46/ 3):

- Üçüncü ülke veya uluslararası kuruluştaki kontrolör veya işleyen ile kişisel verilerin kontrolörü, işleyeni veya alıcısı arasındaki sözleşme maddeleri; veya
- Kamu makamları veya organları arasındaki idari düzenlemelere eklenecek ve uygulanabilir ve etkin veri öznesi haklarını öngören hükümlerin varlığı.

GDPR Madde 47 bağlayıcı kurumsal kuralları/ bağlayıcı şirket kurallarını getirmiştir. Yetkili denetim makamı, belirli koşulların yerine getirilmesi kaydıyla bağlayıcı kurumsal kuralları/ bağlayıcı şirket kurallarını onaylayacak ve aktarım gerçekleşebilecektir. Bu kurallar yasal olarak bağlayıcıdır. Teşebbüsler grubunun ilgili her üyesi için (çalışanları da dahil olmak üzere ortak bir ekonomik faaliyette bulunan işletmeler grubu) geçerlidirler ve onlar tarafından uygulanırlar. Bu bağlamda kişisel verilerinin işlenmesiyle ilgili olarak veri öznelerine açıkça uygulanabilir haklar vermek durumundadırlar ve aynı zamanda Madde 47/ 2'deki şartların da gerçekleşmesi gerekmektedir.

- Ortak bir ekonomik faaliyette bulunan teşebbüsler grubunun veya teşebbüsler grubunun ve üyelerinin her birinin yapısı ve iletişim bilgileri;
- Kişisel veri kategorileri, işleme türü ve amaçları, etkilenen veri konularının türü ve söz konusu üçüncü ülke veya ülkelerin belirlenmesi dahil olmak üzere veri aktarımları veya aktarım grupları;
- Hem dahili hem de harici olarak yasal olarak bağlayıcı nitelikleri;
- Genel veri koruma ilkelerinin uygulanması, özellikle amaç sınırlaması, veri minimizasyonu, sınırlı saklama süreleri, veri kalitesi, tasarım gereği ve varsayılan olarak veri koruması, işlemenin yasal dayanağı, özel kişisel veri kategorilerinin işlenmesi, veri güvenliğini sağlamaya yönelik önlemler ve bağlayıcı kurumsal kurallara bağlı olmayan organlara ileriye dönük transferlerle ilgili gereklilikler;
- Madde 22 uyarınca profil çıkarma da dahil olmak üzere, yalnızca otomatik işlemeye dayalı kararlara tabi olmama hakkı dahil olmak üzere, veri öznelerinin işlemeye ilişkin hakları ve bu hakları kullanma araçları, yetkili denetim makamına şikayette bulunma hakkı, Madde 79 uyarınca Üye Devletlerin yetkili mahkemeleri nezdinde ve bağlayıcı şirket kurallarının ihlali nedeniyle tazmin ve uygun olduğu hallerde tazminat talep etme haklarının tanınması;
- Bir Üye Devlet topraklarında yerleşik kontrolör veya işleyenin, AB içinde yerleşik olmayan herhangi bir ilgili üye tarafından bağlayıcı kurumsal kuralların herhangi bir ihlaline ilişkin sorumluluğu kabul etmesi (kontrolör veya işleyen, yalnızca üyenin zarara yol açan olaydan sorumlu olmadığını kanıtlaması halinde, tamamen veya kısmen bu sorumluluktan muaf olacaktır);
- Bağlayıcı kurumsal kurallara ilişkin bilgilerin veri öznelerine nasıl sağlandığı;
- Madde 37 uyarınca atanan herhangi bir veri koruma görevlisinin veya ortak bir ekonomik faaliyette bulunan teşebbüsler grubu veya teşebbüsler grubu içindeki bağlayıcı kurumsal kurallara uygunluğun izlenmesinden sorumlu diğer herhangi bir kişi veya kuruluşun görevleri ve ayrıca izleme eğitimi ve şikayetleri ele alma;
- Şikâyet prosedürleri;
- Bağlayıcı kurumsal kurallara uygunluğun doğrulanmasını sağlamak için ortak bir ekonomik faaliyette bulunan teşebbüsler grubu veya teşebbüsler grubu içindeki mekanizmalar (Bu tür mekanizmalar, veri öznesinin haklarını korumak için düzeltici eylemlerin sağlanmasına yönelik veri koruma denetimlerini ve yöntemlerini içerecektir. Bu doğrulamanın sonuçları (h) bendinde atıfta bulunulan kişi veya kuruluşa ve bir grup teşebbüsün kontrol eden teşebbüsünün ortak bir ekonomik faaliyette bulunan şirketler

grubunun yönetim kuruluna bildirilmeli ve talep üzerine yetkili denetim makamına sunulmalıdır);
- Kurallardaki değişiklikleri raporlamak ve kaydetmek ve bu değişiklikleri denetim makamına bildirmek için mekanizmalar;
- Teşebbüsler grubunun herhangi bir üyesinin veya ortak bir ekonomik faaliyette bulunan işletmeler grubunun herhangi bir üyesinin, özellikle (j) bendinde atıfta bulunulan önlemlerin doğrulanmasının sonuçlarını denetim makamına sunarak uyumluluğunu sağlamak için denetim makamı ile işbirliği mekanizması;
- Ortak bir ekonomik faaliyette bulunan bir teşebbüsler grubu veya teşebbüsler grubunun bir üyesinin üçüncü bir ülkede tabi olduğu ve bağlayıcı kurumsal kurallar tarafından sağlanan garantiler üzerinde önemli ölçüde olumsuz bir etkiye sahip olması muhtemel herhangi bir yasal gerekliliğin yetkili denetim makamına bildirilmesine yönelik mekanizmalar;
- Kişisel verilere kalıcı veya düzenli erişimi olan personele uygun veri koruma eğitimi.

GDPR Madde 48 uyarınca, aktarım ile ilgili kurallarda öngörülen diğer aktarım gerekçelerine halel getirmeksizin bir kontrolör veya işleyenin kişisel verileri aktarmasını veya ifşa etmesini gerektiren herhangi bir mahkeme kararı ve üçüncü bir ülkenin idari makamının herhangi bir kararı, yalnızca uluslararası bir anlaşmaya (talepte bulunan üçüncü ülke ile Birlik veya bir Üye Devlet arasında yürürlükte olan karşılıklı adli yardım anlaşması gibi) dayalı olması halinde herhangi bir şekilde tanınabilir veya uygulanabilir olabilir.

Madde 45 uyarınca yeterlilik kararı ve Madde 46 uyarınca uygun güvencelerin bulunmaması halinde ise Madde 49'da öngörülen hallerde kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarımı şu koşullardan birinin varlığına bağlanmıştır:

- Veri öznesinin aydınlatılması üzerine, aktarıma açıkça rıza göstermesi (kamu makamlarının kamu yetkilerini kullanırken yürüttükleri faaliyetler hakkında uygulanmaz);
- Veri öznesi ile kontrolör arasındaki bir sözleşmenin ifası veya veri öznesinin talebi üzerine alınan sözleşme öncesi önlemlerin uygulanması için aktarımın gerekli olması (kamu makamlarının kamu yetkilerini kullanırken yürüttükleri faaliyetler hakkında uygulanmaz);
- Aktarımın, kontrolör ile başka bir gerçek veya tüzel kişi arasında veri öznesinin çıkarına akdedilen bir sözleşmenin akdedilmesi veya ifası için gerekli olması (kamu makamlarının kamu yetkilerini kullanırken yürüttükleri faaliyetler hakkında uygulanmaz);
- Kamu yararına yönelik önemli nedenlerle gerekli olması;
- Yasal iddiaların tesisi, kullanılması veya savunulması için gerekli olması;
- Veri öznesinin fiziksel veya yasal olarak rıza gösteremeyecek durumda olması durumunda, veri öznesinin veya diğer kişilerin hayati çıkarlarını korumak için aktarımın gerekli olması;
- Birlik veya Üye Devlet hukukuna göre halka bilgi sağlamayı amaçlayan ve genel olarak kamunun veya meşru menfaat gösterebilen herhangi bir kişinin danışmasına açık bir sicilden yapılan aktarımın, ancak yalnızca, Birlik veya Üye Devlet hukuku tarafından istişare için belirlenen koşulların belirli bir durumda yerine getirildiği ölçüde yapılması.

Görüldüğü üzere GDPR ile, yeterlilik kararı, uygun güvenceler ve bağlayıcı şirket kurallarının olmaması halinde de aktarımın gerçekleşebilmesi için çok sayıda hukuki sebep getirilmiş, bu hallerden en az birine dayanılması yeterli görülmüştür.

GDPR Madde 50 çerçevesinde de üçüncü ülkeler ve uluslararası kuruluşlarla ilgili olarak, Komisyon ve denetim makamları kişisel verilerin korunmasına yönelik mevzuatın etkili bir şekilde uygulanmasını kolaylaştırmak için uluslararası işbirliği mekanizmaları geliştirmek; kişisel verilerin ve diğer temel hak ve özgürlüklerin korunmasına yönelik uygun güvencelere tabi olarak, bildirim, şikayet yönlendirme, soruşturma yardımı ve bilgi alışverişi dahil olmak üzere, kişisel verilerin korunmasına yönelik mevzuatın uygulanmasında uluslararası karşılıklı yardım sağlamak; ilgili paydaşları, kişisel verilerin korunmasına yönelik mevzuatın uygulanmasında uluslararası işbirliğini ilerletmeyi amaçlayan tartışma ve faaliyetlere dahil etmek; üçüncü ülkelerle yetki çatışmaları da dahil olmak üzere, kişisel veri koruma mevzuatı ve uygulamasının değişimini ve belgelenmesini teşvik etmek konularında uygun adımları atacaklardır.

Türk hukukuna gelindiğinde ise yurt dışı aktarım hususunun tartışmalı ve kilitlenmiş bir durumda olduğunu söylemek mümkündür. Bu anlamda Türk mevzuatı açısından da konunun ele alınması gerekmektedir.

6698 sayılı KVKK. md. 9 uyarınca;

- Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.
- Kişisel veriler, 5'inci maddenin ikinci fıkrası ile 6'ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede; yeterli korumanın bulunması, yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.
- Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.
- Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine;
    - Türkiye'nin taraf olduğu uluslararası sözleşmeleri,
    - Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,
    - Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,
    - Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,
    - Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.
- Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.
- Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

Maddede, kademeli bir düzenleme öngörülmüştür. Buna göre, kural, kişisel verilerin, ilgili kişinin ancak açık rızası ile yurt dışına aktarılabilmesi, açık rızası yok ise aktarılamayacak oluşudur.

KVKK md. 5/ 1'de de kişisel verilerin işlenmesi yine açık rızaya bağlanmış ve fakat aynı maddenin 2. fıkrasında 7 bent halinde sayılan şartlardan birinin varlığı halinde ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu öngörülmüştür. Keza md. 6'da da özel nitelikli kişisel verilerin yine ancak açık rıza ile işlenebilecekleri, 3. fıkrada sayılan durumlarda ve sayılan kişilerce yapılacak işlemelerde ise ilgilinin açık rızasının aranmayacağı düzenlenmektedir. Bu noktada, KVKK md. 9'un GDPR düzenlemeleri ve Türkiye'nin kendi yapısal koşullarına göre düzenlenmesi gerekliliği, keza Türkiye'deki idari yapılanmanın da özel sektörün faaliyetlerini de güncelleyecek biçimde üzerine düşenleri yapması tavsiyesini dile getirmek gerekecektir.

Yurt dışına aktarımı düzenleyen md. 9/ 2 gereğince, kişisel verilerin, md. 5/ 2 ve 6/ 3'te belirtilen şartlardan birinin varlığı halinde ve kişisel verinin aktarılacağı yabancı ülkede;

- Yeterli korumanın bulunması kaydıyla veyahut
- Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'un izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabileceğinin düzenlendiği görülmektedir.

Madde 9/ 3 uyarınca, yeterli korumanın bulunduğu ülkeler KVKK (Kurul) tarafından belirlenerek ilan edilmek durumunda olup aynı maddenin 4. fıkrasında Kurul'un yabancı ülkede yeterli koruma bulunup bulunmadığına ve 2/ (b) bendi uyarınca yapılan taahhüt izni başvurusuna izin verilip verilmeyeceğine karar verirken kullanacağı kriterlere yer verilmiştir.

Buna göre Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve aktarım izni verilip verilmeyeceğine karar verirken;

- Türkiye'nin taraf olduğu uluslararası sözleşmeleri,
- Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,
- Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,
- Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,
- Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmekte ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almaktadır.

Madde 9/ 5 ile de kamu kurum ve kuruluşlarının görüşü aranmakta, kişisel verilerin, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak ve Kurulun izniyle yurt dışına aktarılabileceği öngörülmektedir.

Dolayısıyla Türk mevzuatındaki yurt dışı aktarım sürecinin şu sıralama ile öngörüldüğü söylenebilir:

- İlgili kişinin açık rızası alınacaktır.
- İlgili kişinin açık rızası olmaksızın aktarımın gerçekleşebilmesi için taahhütname usulü getirilmiştir. Eğer kişisel verilerin aktarılacağı yabancı ülkede yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının

yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'dan izin almaları gerekecektir.
- Kurul, "yeterli korumanın bulunduğu ülkeleri" belirleyerek ilan edecektir.
- Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda da kişisel veriler, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilecektir.

Halihazırda KVKK tarafından "yeterli korumanın bulunduğu ülkeleri" belirlenmemiştir. Konu GDPR açısından ele alındığında önceliğin yeterlilik kararı, taahhüt, bağlayıcı kurallar gibi mekanizmalara verildiği görülmektedir. GDPR, bu hallerin olmaması durumunda diğer aktarım nedenlerine yüzünü dönmektedir. Bu noktada Türkiye'de de ya bu kademelendirme artırılarak ağırlık kanun ve diğer yasal düzenlemelerin GDPR'a uyumlanmasına verilmelidir, ya da Kurul tarafından halihazırdaki kanun ile kendilerine verilen yetki uyarınca ülke belirlemesinden başlamak üzere işlem yapılmalı ve veri aktarım sorununun çözülmesi açısından adımlar atılmalıdır.

Diğer yandan taahhütname taleplerine ilişkin olarak Kurul'un yaptığı değerlendirmeler ve verdiği izinlerin dağılımı, 2021 yılı ve 2022 yıllarında göre, kendi faaliyet raporları uyarınca;

2022 yılı itibarıyla kanunun 9'uncu maddesinin ikinci fıkrasının (b) bendi uyarınca KVKK'ya sunulan yurt dışına veri aktarım taahhütnamelerinin sayısal dağılımına Tablo 4'te yer verilmiştir.

Tablo 4: 2022 Yılı İtibarıyla Yurt Dışına Veri Aktarım Taahhütnameleri Sayısal Dağılımı

Sunulan Taahhütname	İncelemesi Bitirilen	İncelemesi Devam Eden	Aktarıma İzin Verilen	Aktarıma İzin Verilmeyen
75	45	30	5	40

2021 yılında kanunun 9'uncu maddesinin ikinci fıkrasının (b) bendi uyarınca KVKK'ya sunulan yurt dışına veri aktarım taahhütnamelerinin sayısal dağılımına Tablo 5'te yer verilmiştir.

Tablo 5: 2021 Yılı İtibarıyla Yurt Dışına Veri Aktarım Taahhütnameleri Sayısal Dağılımı

Sunulan Taahhütname	İncelemesi Bitirilen	İncelemesi Devam Eden	Aktarıma İzin Verilen	Aktarıma İzin Verilmeyen
23	7	16	4	3

Görüldüğü üzere, taahhütname ile aktarıma izin verilen vaka sayısı başvurulara nispeten oldukça düşük orandadır. Öyleyse halihazırda Türk hukukunda taahhütname seçeneği ile de yurt dışına kişisel veri aktarımının gerçekleşmesi çok mümkün görünmemektedir. Buradan varılacak sonuçlar şöyle sıralanabilir:

- Öncelikle, "yeterli korumanın bulunduğu ülkeler" belirlemesi ve taahhütleşme yapılmadığında, Türk hukuku açısından yurtdışına kişisel veri aktarımının tek yolu olarak ilgili kişinin açık rızası yolu kalmaktadır. Yalnızca açık rızaya dayalı bir süreç ise ilk olarak pratik açıdan sorun, iş yükü olarak özel sektöre yüklenmektedir.
- Rızaya dayalı işlemeden söz edildiği noktada, rızanın geri alınması ("withdrawal of consent") sorunu doğmaktadır. Örneğin açık rıza ile kişisel verileri yurtdışına aktaran bir veri sorumlusu, ilgili kişi, hiçbir gerekçe göstermesine gerek olmaksızın rızasını geri

aldığını bildirirse ne olacaktır? Bunun takibi ve ve vakitlice gereğinin yapılması, açık rıza alınması yükümlülüklerinin doğrudan bir sonucu olarak yine işletmenin üzerine bir yük ve sorumluluk olarak gelmektedir.

- Bu noktada, Kurul, yeterli korumanın bulunduğu ülkeleri belirlememişken ve ne zaman belirleneceği konusunda da bir muğlaklık söz konusu iken ve aynı zamanda rıza ile aktarımın getirdiği pratik ve hukuki sorunlar halihazırda mevcut iken tek ara çözüm, en azından sektörel piyasaların büyük aktörlerinin taahhütname yoluyla veri aktarımını sağlamaları olmalıdır, demek yanlış olmayacaktır.
- Ayrıca bu süreçleri zorlaştırmak, bilhassa başat sektörlerde, fiilen tekel yaratılması sonucunu doğurma potansiyelini de içermektedir. Dolayısıyla taahhüt ve izinlerle ara süreçler yaratılması orta ve küçük düzey aktörlerin de uluslararası ticarete dahilini kolaylaştıracaktır.
- Ayrıca veri aktarımının zorlaşması, pek çok veri sorumlusunun, ihlal gerçekleşene veyahut rızayı dikkate almadan "yakalanana" kadar usulsüzce işlemi sürdürmesi sonucunu da uygulamada doğurmaktadır.

Bunlara ek olarak, mutlaka uluslararası çok büyük hacimli bir ticaretin söz konusu olmasına da gerek yoktur. Özellikle herkesin kullandığı uluslararası e-posta sunucularının, web sitesi alt yapılarının, mesajlaşma sistemlerinin, web servislerinin veri merkezlerinin yurtdışında olduğu ve bunlar üzerinden yapılan her türlü iş ve işlemlerin de yurtdışı aktarıma girdiği düşünüldüğünde sürecin zorlaştırmasının sistemi durmaya veya sorumlular ve ilgililerce "gittiği yere kadar" (ihlal ederek) kullanıma zorlayacağı da açıktır.

Öyleyse yasal ve güncel duruma yeniden dönüldüğünde şu an için Türk hukukuna göre kişisel verilerin yurtdışına aktarımının tek yolu ve seçeneği olarak ilgili kişilerin “yurt dışı aktarım özelinde alınmış” açık rızalarının bulunması halidir.

Diğer yandan KVKK’nin Amazon Turkey hakkında verdiği ve yurt dışına aktarım temelinde gelişen kararı da bu bağlamda değerlendirilebilecek bir örnektir. Kişisel Verileri Koruma Kurulu’nun Amazon Turkey Perakende Hizmetleri Limited Şirketi (“Amazon”) hakkında tesis ettiği 27.02.2020 tarih ve 2020/173 sayılı kararında; amazon.com.tr “Gizlilik Bildirimi” sayfasının “Amazon Kişisel Bilgilerinizi Paylaşıyor mu?” kısmının “Kişisel Bilgilerin Türkiye Dışına Aktarılması” alt başlığı altında yer alan, “Kişisel bilgilerinizi saklamak ve işbu Gizlilik Bildirimi’nde açıklanan amaçlar çerçevesinde işlemek için Avrupa Birliği’ne ve Avrupa Birliği’nden Amerika Birleşik Devletleri’ne aktarabiliriz” şeklindeki ifadeden kişisel verilerin yurt dışına aktarıldığının anlaşıldığı; ancak hâlihazırda amazon.com.tr internet sitesi ve bağlı mobil uygulamalar aracılığı ile sunulan hizmetlere ilişkin ne üyelik hesabı oluşturulurken ne de alışveriş yapılırken, kişisel verilerin yurt dışına aktarılması için açık rıza alınmadığı; yurt dışına aktarıma ilişkin olarak Kurul izni alınmamış ise, herhangi bir açık rıza da alınmadığından bu durumun 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 9. maddesini ihlal ettiği iddiasından hareket edilmiştir. Buna mukabil Amazon ise kayıtlı müşterilerin kişisel verilerinin Türkiye dışına aktarıldığından/ aktarılabileceğinden sadece haberdar olmakla kalmayıp aynı zamanda “Gizlilik Bildirimi”ni onaylayarak bu hususu kabul etmiş oldukları ve aynı zamanda Amazon Turkey’in yurt dışına veri aktarım taahhütnameleri ile ilgili yazışmalarının Kişisel Verileri Koruma Kurumu ile sürdürülmekte olduğu şeklinde savunma sunmuştur.

Nitekim Kurul tarafından yapılan inceleme sürecinde de veri sorumlusu Amazon Türkiye'nin yurtdışına veri aktarımını sağlamak amacıyla Kurul’un onayını almak üzere taahhütname mektuplarını Kurula sunduğu görülmüştür. Ancak Kurulun henüz bu taahhütname başvurusu

ile ilgili bir karar vermediği ve yeterli korumaya sahip ülkelerin de henüz belirlenmediği değerlendirildiğinde kişisel verilerin yurtdışına aktarılması için tek dayanak ilgilinin açık rızasının alınması olarak değerlendirilmektedir. Amazon'un "zımni irade beyanı ile onay" alması ve "battaniye rıza (genel nitelikli, konusu belirsiz, ilgili işlemle sınırlı olmayan rıza)" ile tamamlaması, bunun açık rızayı karşılayıp karşılamadığı ayrı bir tartışma konusu olarak bir tarafa bırakılacak olursa Amazon Türkiye'nin ihlal nedeniyle yaptırıma tabi tutulması, Kurul'un, kanun hükmü gereğince zorunlu olduğu halde belirlemediği bir liste ve veri sorumlusunun yaptığı ve fakat henüz incelemediği bir taahhüt izin başvurusu söz konusu olduğunda bile takdirini cezalandırmadan yana kullanacağı yönünde önemli bir örnektir.

5.3.4 Veri Güvenliğinin Sağlanmasında Kişisel Verilerin Korunması

Veri güvenliği açısından kişisel verilerin korunması özelinde bazı başlıkların ayrıca incelenmesinde fayda vardır. Bu noktada seçilen iki sorun, Türk hukukunda ve uluslararası mecrada farklı biçimlerde kendini gösteren kişisel verilerin işlenme nedenlerinin temelini oluşturan rıza/ açık rıza; diğeri ise kamu kurumlarının işledikleri kişisel veriler açısından doğan ve/ veya doğmayan sorumluluklarıdır.

Türk hukukunda ilk olarak, Anayasa'nın 20. maddesine 2010 değişikliği ile eklenen 3. fıkra ile kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği düzenlemesi getirilmiştir. Sonrasında KVKK'nın da pek çok maddesinde "açık rıza"dan söz edilmiştir. Kanunun 5/ 1 maddesinde kişisel verilerin açık rıza olmaksızın işlenemeyeceği[63], 6/2 maddesi ile özel nitelikli kişisel verilerin açık rıza olmaksızın işlenemeyeceği, 8 ve 9. maddelerinde ise yine açık rıza olmaksızın (yurtiçi ve yurtdışında) aktarılamayacağı hükümlerine yer verilmiştir. Aynı Kanun'un 3/1 (a) bendinde ise "açık rıza" tanımlanmıştır. Buna göre "açık rıza", "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"yı ifade etmektedir.[64]

Kişisel Verileri Koruma Kurulu'nun yayınladığı Açık Rıza Rehberi[65] uyarınca da açık rıza, rıza veren kişinin "olumlu irade beyanı"nı içerecektir. Yine Rehber'e göre, veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması, kişinin özgür bir şekilde rıza gösterebilmesi için, neye rıza gösterdiğini de bilmesi ve kişinin hem konu hem de göstereceği rızanın sonuçları hakkında tam bir bilgi sahibi olması gerekliliği vurgulanmıştır. Buna göre, bilgilendirme, veri işleme ile ilgili bütün konularda açık ve anlaşılır bir biçimde gerçekleştirilmeli, mutlaka verinin işlemesinden önce yapılmalıdır. Bilgilendirme işleme ve kullanma amaçlarını açıkça içermeli, okunaklı, anlaşılır olmalıdır ki Türk hukukunda bilhassa aydınlatma yükümlülüğü ve bu yükümlülüğün yerine getirildiğinin ispatı üzerinden yaşanan uygulama sorunları da bu açıdan incelenmelidir.

GDPR ise "rıza" ve "açık rıza" kavramlarını (*consent* - *explicit consent*), aynı veyahut ikame edilebilir kavramlar olarak kullanılmamaktadır. İkisine de farklı anlamlar ve boyutlarda yer vermektedir. GDPR Madde 4/ 11'de veri öznesinin "rızası" tanımlanmış olup "rıza", veri sahibinin bir beyan yoluyla ya da açık bir (olumlu) onay eylemiyle ("opt-in") kendisine ait kişisel

[63] Bununla birlikte 5/ 2 maddesinde ise rızanın aranacağı hallerin çok sayıda istisnasına yer verildiği de eklenmelidir.
[64] Muammer Ketizmen – Aslıhan Kart, Rızaya Yüklenen Koruyuculuk İşlevi ve Kişisel Verilerin Korunması, Lexpera Blog, 14.01.2022, https://blog.lexpera.com.tr/rizaya-yuklenen-koruyuculuk-islevi-ve-kisisel-verilerin-korunmasi/
[65] https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf

verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık göstergedir. Yine Madde 6 uyarınca veri öznesi, bir ya da daha fazla sayıda spesifik amaca yönelik olarak kişisel verilerinin işlenmesine onay verebilecektir. Madde 7 uyarınca ise rızanın koşulları şöyle sıralanabilir:

- İşlemenin rızaya dayandığı hallerde, veri öznesinin, kişisel verilerinin işlenmesine rıza gösterdiğini ispat yükü veri sorumlusundadır.
- Veri öznesinin rızası, başkaca hususları da içeren bir metin ile birlikte alınıyor ise kişisel verilere ilişkin rıza talebinin ayırt edilebilir biçimde anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanılarak sunulması gerekmektedir. Aksi halde GDPR açısından bağlayıcı olmayacaktır.
- Veri minimizasyonu yine önemlidir. Bir sözleşmenin ifası için ihtiyaç olmayan kişisel verilerin de işlenmesine yönelik olarak rıza alınması gerekip gerekmediği veri sorumlusu tarafından değerlendirilmek zorundadır. Sözleşmenin ifası için gerekenden fazla verinin işlenmesi rızaya dayansa bile, bunun özgür iradeye dayalı bir rıza olup olmayacağı ve bunun ispatı konusu da kanımızca, tartışma yaratacaktır.

GDPR Madde 12'de düzenlenen veri sahibinin haklarının kullanımına ilişkin şeffaf bilgilendirme, bildirim ve yöntemler; Madde 13'te veri sahibinden kişisel verilerin toplandığı hallerde sağlanacak bilgiler; Madde 14'te kişisel verilerin veri sahibinden alınmadığı hallerde sağlanacak bilgiler; Madde 17'de silme hakkı (unutulma hakkı) bağlamında da "*rıza*" vurguları görülmektedir.

GDPR'ın, rıza ile ilgili gerekçeleri ("recital") incelendiğinde, buradan da şu açıklamalara ulaşılmaktadır:

a. Rec. 32, rıza ile ilgili olarak, yine bilgilendirilmiş ve net bir olumlu eylemle verme açıklaması yer almakta, bunun elektronik yollar da dahil olmak üzere yazılı veya sözlü de olabileceği belirtilmektedir. Rıza aynı amaç veya amaçlar için yapılacak işlemeyi içermeli; birden fazla farklı amaç için işleme söz konusu ise rıza bunlar için de olmalıdır.
b. Rec. 33'te bilimsel araştırmalar için gösterilecek irade yine "rıza" bağlamında ele alınmıştır.
c. Rec. 42, kontrolörün rıza aldığını ispatı açısından önemli bir açıklamadır. Özgür irade, açık sade dil kullanımı gibi açıklamaların yanı sıra veri kontrolörünün, veri sahibinin rızasına dayandığı hallerde işlemeye rıza gösterdiğini gösterebilmesinin gerektiği ifade edilmektedir.
d. Rec. 51'e göre, özel nitelikli kişisel veri kategorilerinin işlenmesine yönelik genel yasaklamalara getirilen istisnalar, veri sahibinin açık rızasına dayalı işlemelerde de açıkça belirtilmelidir.
e. Rec. 71 uyarınca, otomatik işlemeye dayanan hallerde (iş performansı, ekonomik durum, sağlık, kişisel tercih analizleri gibi), veri sahibinin, bu profillemeye ilişkin olarak "*explicit consent/ açık rıza*"sının alınmasından söz edilmektedir.
f. Rec. 111 ile kişisel veri aktarımı konusunda; adli, idari, düzenleyici kurumlar önünde veya mahkeme dışı prosedürler de dahil olmak üzere aktarımın sözleşme veya yasal taleplerle ilgili olarak daimi olmayan aktarımlarda veri sahibinin açık rızasını mümkün kılan hükümlerin olması gerektiği belirtilmektedir.

Rızanın alınmasına ve alındığının ispatına ilişkin yükümlülükler tümüyle veri sorumlusuna bırakıldığından ve örneğin Türk hukukunda rıza ve aydınlatma yükümlülüklerinin yerine

getirilmemesi hukuki, idari ve cezai pek çok sorumluluğu da beraberinde getirdiğinden bunların ispatı da işletmeler açısından ayrı bir yükü doğurmaktadır. GDPR, bilgilendirilmiş rıza gerekliliğini yerine getirmek için bilgilerin sunulması gereken biçimi veya şekli belirlememiştir. Öyleyse geçerli bilgiler, yazılı veya sözlü ifadeler ya da sesli veya görüntülü mesajlar gibi çeşitli şekillerde sunulabilecektir. GDPR Madde 7/2 kapsamında yazılı sözleşme, kişisel verilerin işlenmesine ilişkin rıza ile ilgili olmayan pek çok başkaca hususu içeriyorsa, rıza konusu açıkça öne çıkan bir biçimde veya ayrı bir belgede yer almalıdır. Elektronik yollarla rıza istendiğinde de rıza talebinin ayrı olması veya somut duruma göre katmanlı bir yol düşünülmesi gerekmektedir. Burada da log kayıtlarının tutulması ve saklanması önem taşıyacaktır. Yine veri sorumlusuna, "açık rıza"nın alınması için, ilgili kişiye her seferinde aydınlatma yapma yükümlülüğü yüklenmesi de verinin yönetimi açısından sorunlu noktalar arasında olacaktır.

Rızanın geri alınması konusunda ise GDPR Madde 7/ 3'te "iptal işlemi(nin), rızanın verilmesi kadar basit olma(sı)" gerektiği hükme bağlanmıştır. Nitekim Madde 7'nin 1 ve 2. fıkralarında da rızanın koşullarının hali hazırda düzenleniyor olması, 3. fıkrayı da anlamlı kılmaktadır.

Türk hukukunda ise rızanın şekli konusunda da, geri alınması konusunda da bir hüküm yer almamakta, belirsizlik bulunmaktadır. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 12. maddesinde "Kişisel verileri işleme şartlarının tamamı ortadan kalk(ması)" haline ilişkin bir silme, yok etme ve anonimleştirme yükümlülüklerinden söz edilmekte, ancak yine rıza ve açık rıza kavramlarına ilişkin bir bağlam görülememektedir. Rızanın geri alınması haline ilişkin net bir düzenleme mevcut değildir.

Bir diğer başlık ise kamunun sorumlulukları üzerinedir. Kamunun en büyük veri işleyen ve dolayısıyla veri kontrolörü olduğu ve özel sektörün faaliyetlerinin de kamu ile ilişkilere bağlı/ bağımlı olduğu dikkate alındığında, KVKK kapsamının istisnaları ve yaptırımlar açısından, kamu kurumlarının ve pek çok kamu hizmetinin kısmen veya tamamen kanundan istisna tutulduğuna değinilmelidir. KVKK md. 18 uyarınca idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanacaktır. Kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları ise yalnızca kendi memurları üzerinde yürütmeleri gereken bir disiplin sorumluluğu vardır. Diğer bir deyişle, kişisel verilerin korunmasına ilişkin ihlallerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi halinde, sayılan kamu sektörü kuruluşları açısından yalnızca disiplin soruşturması/ kovuşturması yapma ve bu disiplin sürecini Kişisel Verileri Koruma Kurulu'na bildirme yükümlülüğü getirilmektedir. Diğer yaptırımlar kamu kurumlarına uygulanmayacaktır.

KVKK'nin istisna kapsamı da md. 28 ile düzenlenmiştir. Burada da pek çok kamu hizmetinin ve kamu kuruluşunun KVKK kapsamı dışında tutulduğu, yani kişisel verilerin korunması ile ilgili düzenlemelere tabi olmadıkları görülmektedir. Bunun sonuçlarından biri özel sektörün zamanla, kamuyla verisini paylaşmak istememeye doğru yönelecek olmasıdır. Kendisine yüklenen her türlü hukuki, mail, idari, cezai ve ticari sorumluluğa karşılık sorumluluğu olmayan bir kamuyla veri paylaşımına girmek, kişiler arasında bir eşitsizlik ve dengesizlik duygusu yaratacaktır.

GDPR'da ise Türk hukukunda kamu kurumlarına getirilen bu istisnanın yer almadığı görülmektedir. Bununla birlikte "kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı korunma dahil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturması veya cezai yaptırımların infazı amacıyla yetkili makamlar tarafından" yapılacak

işlemeler hariç tutulmuştur. Ancak Türk hukukundaki gibi kamu özelinde tanınmış bir bağışıklık söz konusu değildir ki, hatta GDPR Madde 83/ 7 uyarınca denetim makamlarının Madde 58/ 2 uyarınca düzeltici yetkilerine halel gelmeksizin, her Üye Devlete, o Üye Devlette yerleşik kamu makamlarına ve organlarına idari para cezalarının verilip verilmeyeceğine ve ne ölçüde uygulanacağına ilişkin kuralları belirleme yetkisi de açıkça tanınmıştır. Bunun örnekleri de görülmektedir. Örneğin İtalyan Kişisel Verileri Koruma Kurulu (*Garante per la Protezione Dei Dati Personali*) 25.02.2021 tarihli bir kararında[66], Ulusal Sosyal Güvenlik Kurumu (INPS) aleyhine hüküm kurmuştur. Bu uyuşmazlıkta, INPS'in, soruşturmaya konu faaliyetlerinin veri minimizasyonu ilkesine aykırı olarak veri işlemek olduğundan bahisle kamu kurumu hakkında veri minimizasyonuna aykırı verilerin tümünün silinmesi, veri etki değerlendirmesinin yapılması, GDPR Madde 83 uyarınca 300.000 Euro idari para cezası uygulanmasına, ihlal ve cezanın ilanına karar verilmiştir.

5.4 Veri Güvenliği

Veri uzayı yönetiminin en önemli bileşenlerinden birisi de elbette veri güvenliğidir. Veri güvenliği (data security), verinin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemektir. Veri güvenliği Gizlilik, Bütünlük ve Erişilebilirlik olarak isimlendirilen üç temel unsurdan meydana gelir. Bu unsurlardan herhangi biri zarar görürse güvenlik zaafiyeti oluşur.[67]

- **Gizlilik**: Bilginin yetkisiz kişilerin eline geçmemesi ve yetkisiz erişime karşı korunmasıdır.
- **Bütünlük**: Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.
- **Erişilebilirlik**: Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

Veri güvenliği (data security), kurumsal verilerin korunması ve yetkisiz erişim yoluyla veri kaybının önlenmesi sürecini ifade eder. Verileri güvenli hale getirmek; verileri şifreleyebilen veya yok edebilen fidye yazılımı gibi saldırıların yanı sıra verileri değiştirebilen ya da bozabilen saldırılara karşı da korumak demektir. Tüm bunların amacı, işletmelerde verilere erişimi olan herkesin bu bilgilere güvenli bir biçimde ulaşmasını kolaylaştırmaktır.[68]

Bazı kurumlar, ülkeler tarafından uygulanan veri koruma düzenlemelerine uymak ve yüksek düzeyde veri güvenliği sağlamak zorundadır. Örneğin, ödeme kartı bilgilerini saklayan kuruluşlar, bu verileri güvenli bir şekilde muhafaza etmeli ve belirli standartlar altında verileri güvence altına almalıdır. Kurum faaliyet gösterdiği alana bağlı olarak veri güvenliği konusunda herhangi bir düzenleme veya uyumluluk standardına tabi olmasa bile varlığını sürdürebilmesi veri güvenliğine bağlıdır.

Her yıl on binlerce kullanıcının gizli verisi kötü niyetli siber saldırganlar tarafından ele geçirilmektedir. Bu, finansal kayıpların ötesinde çoğu zaman kullanıcılarda güven azalmasına ve kurum/şirket itibarının zarar görmesine yol açmaktadır. Son yıllarda veri güvenliği alanında sosyal mühendislik, fidye yazılımı ve APT gibi gelişmiş tehditler yükselişe geçmiştir. Bunların tümü mücadele edilmesi zor olan ve bir kuruluşun verilerinde yıkıcı hasara yol açabilen tehditlerdir.

[66] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556958
[67] https://www.tkdk.gov.tr/Kurumsal/BGYS (Erişim:09.07.2023)
[68] https://www.komtas.com/glossary/veri-guvenligi-nedir (Erişim:11.07.2023)

5.4.1 Veri Güvenliğine Karşı Tehditler

İnternet ortamı size hesaplara, iletişim yöntemlerine ve bilgi paylaşma ve kullanma yollarına erişim sağlar. Çeşitli siber saldırılar ve içeriden riskler paylaştığınız bilgilerin risk altına girmesine sebebiyet verir.[69]

- Korsanlık Yapma (Hacking): Bilgisayar korsanlığı, veri çalma, ağları veya dosyaları bozma, bir organizasyonun dijital ortamını ele geçirme veya verilerini ve faaliyetlerini bozmak için bilgisayar aracılığıyla yapılan girişimler anlamına gelir. Bilgisayar korsanlığı yöntemleri arasında kimlik avı, kötü amaçlı yazılım, kod kırma ve dağıtılmış hizmet reddi saldırıları yer alır.
- Kötü amaçlı yazılım (Malware): Kötü amaçlı yazılım yetkisiz kullanıcıların ortamınıza erişmesini sağlayan solucanlar, virüsler ve casus yazılımlar için kullanılan bir terimdir. Bu kullanıcılar, sisteminize giriş yaptıktan sonra BT ağınızı ve uç nokta cihazlarınızı bozma veya dosyalarda kalmış olabilecek kimlik bilgilerini çalma potansiyeline sahiptir.
- Fidye yazılımı (Ransomware): Fidye yazılımı fidye ödeyene kadar ağınıza ve dosyalarınıza erişimi engelleyen kötü amaçlı bir yazılımdır. Bir e-posta ekini açmak ve bir reklama tıklamak, fidye yazılımının bilgisayarınıza indirilmesine neden olan yollardan biridir. Genellikle dosyalara erişim sağlayamadığınızda veya ödeme talep eden bir mesaj gördüğünüzde keşfedilir.
- Kimlik avı (Phishing): Kimlik avı kredi kartı numarası ve şifre gibi bilgileri vermeleri için kişi veya organizasyonları kandırma eylemidir. Burada amaç, kurbanın tanıdığı saygın bir şirket gibi davranarak hassas verileri çalmak veya bunlara zarar vermektir.
- Veri sızıntısı: Veri sızıntısı, bir organizasyondaki verilerin harici bir alıcıya kasıtlı veya kazara aktarılmasıdır. Bu, e-posta, internet ve dizüstü bilgisayarlar ve taşınabilir depolama cihazları gibi cihazlar kullanılarak gerçekleştirilebilir. Şirket dışına çıkarılan dosya ve belgeler de bir tür veri sızıntısıdır.
- İhmal: İhmal, bir çalışanın şirkete zarar verme amacı olmasa da bilinçli bir şekilde bir güvenlik ilkesini ihlal ettiği durumlardır. Örneğin, hassas verileri bu verilere erişimi olmayan bir iş arkadaşıyla paylaşabilir veya güvenli olmayan bir kablosuz bağlantı üzerinden şirket kaynaklarına giriş yapabilirler. Buna bir başka örnek ise, bir kişinin rozet göstermeden binaya giriş yapmasına izin vermektir.
- Dolandırıcılık: Dolandırıcılık, internetin sağladığı anonimlik ve gerçek zamanlı erişilebilirlikten yararlanmak isteyen ileri düzey kullanıcılar tarafından yürütülen eylemlerdir. Risk altındaki hesapları veya çalıntı kredi kartı numaralarını kullanarak işlemler oluşturabilirler. Organizasyonlar, garanti dolandırıcılığı, geri ödeme dolandırıcılığı veya bayi dolandırıcılığının kurbanı olabilir.
- Hırsızlık: Hırsızlık, verilerin, paranın veya fikri mülkiyetin çalınmasıyla sonuçlanan bir iç tehdittir. Kişisel menfaat sağlamak için organizasyona zarar verme amacıyla gerçekleştirilir. Örneğin, güvenilir bir satıcı karanlık ağda müşterilerin sosyal güvenlik numaralarını satabilir veya kendi işini kurmak için müşteriler hakkındaki şirket içi bilgileri kullanabilir.
- Doğal afetler: Doğal afetler, meydana gelmeden önce herhangi bir uyarı vermediğinden her ihtimale karşı verilerinizi koruma konusunda önceden hazırlıklı olmanız akıllıca olacaktır. İster bir kasırga, deprem, sel veya başka bir yıkım türü olsun,

[69] https://www.microsoft.com/tr-tr/security/business/security-101/what-is-data-security (Erişim:11.07.2023)

verilerinizin şirket dışında yedeklenmesi, iş sürekliliği planınızın uygulanmasına yardımcı olacaktır.

5.4.2 Veri Güvenliği İçin Alınacak Tedbirler

Veri güvenliği risklerinin önüne geçilebilmek için gerekli zaman, kaynak ve uzmanlığın sağlanarak uygun teknik ve idari tedbirlerin alınması gerekmektedir. Bu tedbirler, her zaman yüksek maliyet gerektirmemekte olup, söz konusu tedbirlerin masrafsız ya da düşük maliyetli olarak alınması veya halihazırda sistemlerde mevcut olması da mümkündür.[70] Kişisel verilerin güvenliği için önerilen bu tedbirler genel anlamda tüm verilerin güvenliği için de geçerli olan önerilerdir.

- İdari tedbirler: Veri yönetimi sürecinde alınması gereken en önemli idari tedbirler; mevcut risk ve tehditlerin belirlenmesi, çalışanların eğitilmesi ve farkındalık çalışmaları, kişisel veri güvenliği politikalarının ve prosedürlerinin belirlenmesi, kişisel verilerin mümkün olduğunca azaltılması ve veri işleyenler ile ilişkilerin yönetimidir.
- Teknik tedbirler: Veri yönetimi sürecinde alınması gereken teknik tedbirler ise; siber güvenliğin sağlanması, kişisel veri güvenliğinin takibi, kişisel veri içeren ortamların güvenliğinin sağlanması, bilgi teknolojileri sistemleri tedariği, geliştirme ve bakımı, kişisel verilerin yedeklenmesi ile verilerin bulutta depolanmasına ilişkin alınması gereken tedbirlerdir. Bulutta depolanan verilerin neler olduğunun detaylıca bilinmesi, yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanması önerilmektedir.

Bunların yanı sıra verinin güvenliği sağlama tedbirleri arasındaki en genel başlığın imha üzerinden geliştiği de eklenmelidir. 6698 sayılı KVKK md. 7 ile kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi düzenlenmiştir.

- Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.
- Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.
- Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.

Kanun'da anonimleştirme dışında bir kavramın tanımına yer verilmemiştir. Md. 3/ 1 (b)'de yer alan tanıma göre anonim hâle getirme, "kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi"dir.

28.10.2017 tarih ve 30224 sayılı Resmi Gazete'de yayınlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik ile de detaylar düzenlenmiş ve kanunda yer almayan bazı tanımlara bu yönetmelikte yer verilmiştir. Buna göre;

[70] KVKK, 2018:3

Yönetmelik md. 4/ 1 (c) uyarınca;

> "İmha", "*Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini*";

Yönetmelik md. 8/ 1 uyarınca;

> "kişisel verilerin silinmesi" "*kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini*";

Yönetmelik md. 9/ 1 uyarınca;

> "kişisel verilerin yok edilmesi", "*kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini*";

Yönetmelik md. 10/ 1 uyarınca;

> "kişisel verilerin anonim hale getirilmesi", "*kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini*" ifade etmektedir.

Bu tanım KVKK'daki anonim hale getirme tanımı ile aynıdır. Yönetmelik md. 10/ 2'de de daha detaylı bir açıklama yapılmıştır ancak bu detay kapsamı biraz daraltmaktadır. "*Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir*" denilen açıklamada eylemi yapabilecek kişiler veri sorumlusu, alıcı veya alıcı grupları ile sınırlı tutulmuştur. Aynı yönetmelikte kayıt ortamı da "*tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı*" olarak tanımlanmakta ve kayıt ortamı ile sektörel alan da dikkate alınarak uygun anonimleştirme tekniklerinin kullanılması gerektiği düzenlenmiştir.

Bu tanımlara göre **silme**, "*ilgili kullanıcıların erişememesi ve kullanamamaması*"; **yok etme**, "*hiç kimsenin erişememesi, geri getirememesi ve tekrar kullanamamaması*"; **anonim hale getirme**, "*ilişkilendirmenin ortadan kaldırılması*"; **imha** ise "*silme, yok etme anonim hale getirme eylemlerinin üst başlığı*" anlamına gelmektedir.

Genel olarak "işleme" eylemlerinden olan saklama ve imha süreçleri hakkında veri sorumlusunun bir saklama ve imha politikası oluşturması, bu politikaya uygun olarak hareket etmesi, periyodik imha sürelerini belirlemesi (bu süre herhalde altı ayı geçemez), kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemleri kayıt altına alması ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklaması gerekmektedir (Yönetmelik md. 7).

Diğer yandan, verilerin yok edilmesiyle ilgili tek düzenleme 6698 sayılı Kanun ile ona bağlı ikincil mevzuat değildir. 5237 sayılı Türk Ceza Kanunu md. 138 ile verileri yok etmeme suçu düzenlenmiştir.

- Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

- Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.

Genel Kanun olarak TCK'deki 6698 sayılı KVKK da md. 17/ 2 ile bu maddeye atıf kurmuş, KVKKn md. 7 hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır, denilmiştir. Bu atıflar olmasaydı da Türk Ceza Kanunu zaten uygulanacak olmakla birlikte bu atıflar, genelde kişisel verilerin korunması, özelde ise verilerin imhası noktasında sağlanmaya çalışılan cezai korumayı vurgulamaktadır.

Ancak KVKK ve Yönetmelik'te ortaya çıkan kavram karmaşası TCK'de de farklı bir veçhesi ile görülmektedir. KVKK ve Yönetmelik imha, silme, yok etme, anonim hale getirme gibi farklılaştırılmış birtakım işlem, yöntem ve yükümlülüklerden bahsederken ve her birini farklı tanımlarken, bu düzenlemelerden 10 yılı aşkın süre önce TCK'ye eklenen md. 138'de verileri yok etmeme suçundan söz edilmektedir. Buradaki "yok etme" kavramı ile KVKK ve Yönetmelik'teki yok etme kavramı aynı mıdır, yoksa TCK'deki yok etme ile örneğin aslında şu an bir çatı kavram olarak tanımlanan imha mı kastedilmektedir gibi sorular cevaplanmaya muhtaçtır. Bu da öncelikle terim birliği ile sağlanabilecektir.

GDPR'da kişisel verilerin güvenliği konusunda pseudonymisation (psödonimizasyon) ve şifrelemeden (encryption) (Madde 32) bahsedilmektedir. Madde 4/ 5 ile 'pseudonymisation' (psödonimizasyon) tanımlanmıştır. Türkçe'de takma ad-rumuz kullanma-bulanıklaştırma gibi anonim hale getirme yöntemlerine denk düşen terim GDPR'daki tanımı ile kişisel verilerin, ek bilgiler kullanılmadan, bu tür ek bilgilerin ayrı tutulması ve kişisel verilerin kimliği belirli veya belirlenebilir bir gerçek kişiye atfedilmemesini sağlamak için teknik ve organizasyonel önlemlere tabi olması kaydıyla; artık belirli bir veri sahibi ile ilişkilendirilemeyecek şekilde işlenmesini ifade etmektedir.

6 Veri Analitiği ve Veri Uzayında Öngörüler

Veri analitiği genel olarak İstatistiksel Yöntemler ve yeni yöntemler olarak adlandırılan, veri madenciliği ve makine öğrenmesi algoritmalarını içermektedir.

Veri analizi çalışması, ister istatistiksel analiz, isterse makine öğrenmesi metotları, yapay zeka yöntemleri ile yapılsın, veri uzayında veri analitiği çalışmalarını yaparken veri analiz yöntemi büyük önem arz etmektedir. Bir analiz yöntemine dayanmayan çalışmalar istenilen sonuca varamaz ve verilen emeklerin ve harcanan kaynakların israf olmasına sebep olur.

Bu başlık altında, önce veri analiz yöntemi ile ilgili genel bir çerçeve önerilecek, istatistiksel veri analiz yöntemlerinden bahsedilecek, makine öğrenmesi algoritmaları ile ilgili bilgi verilecek, sonraki bölümde veri analiz ve görselleştirme araçlarını bütünleştiren, makine öğrenmesi ile istatistik yöntemleri veri analizinde uygulamamızı sağlayan, iş zekası platformlarından bahsedilecektir. Son bölümde ise değerlendirme ve öneriler sunulacaktır.

6.1 Veri Analizi

Veri analizi, gerekli araçlar yardımıyla, ham verinin içinde gömülü olan yararlı bilginin ya da veri modellerinin gün yüzüne çıkarılmasıdır. Tek başına kullanışsız olan bilgilerin eyleme dönüştürülebilir, değerli veriler haline getirilmesi başarılı bir kuruluş için veri analizinde temel maddelerden biridir. Gelişmiş bir veri analizinin aşamaları şunlardır:[71]

Amaçların Belirlenmesi

Analiz işlemlerine başlanmadan önce, yararlı bilginin diğerlerinden ayırt edilebilmesi için veri gereksinimleri belirlenmelidir. Analiz girdileri ve değişkenleri kategorik ya da sayısal olabilmektedir.

Analizi yapılacak konunun kapsamı, analiz yapma nedeni, ölçme tekniği ve hedeflenen sonuç tüm paydaşlarla beraber kararlaştırılmalı, çalışma işbirliği içinde yürütülmelidir.

Veri analizinin beklenen sonuca çıkması için bu süreçte amaca yönelik sorular yöneltmek kilit noktalardandır. Hangi soruların cevaplanması gerektiğini belirlemek, analiz boyunca takip edilecek yolun sınırlarını çizeceği için bu aşamadaki başarı, analiz sonucundaki başarı ile doğru orantılıdır.

Veri Toplama

Bu aşama; veri tabanları, web sayfaları, medya, müşteri anketleri, arşivler, birinci taraf şirket verileri gibi farklı kaynaklardan elde edilen dağınık ham bilginin toplandığı aşamadır. Bu aşamadan sonra elde edilen veriler temizleme işlemine tabi tutulacak olsa da veri havuzuna çekilecek olan bilgilerin belirli kriterler doğrultusunda, amaca uygun seçilmesini sağlamak öncelik olmalıdır. Analiz edilmesi planlanan verilerin hangi zaman aralığından seçileceği belirlenmelidir.

Veri İşleme

Toplanan tüm verilerin işlendiği ve analize uygun olacak biçimde yapılandırıldığı aşamadır.

[71] https://www.natro.com/blog/veri-analizi-nedir-veri-analizleri-nasil-yapilir/

Verileri Temizleme

Veri işleme aşaması tamamlanan verilerde hata payını azaltmak için tekrar bir tarama yapılır ve hatalar sistemden uzaklaştırılır. Topladığınız verilerin türüne bağlı olarak farklı temizleme işlemleri yapılmaktadır.

Veri Modelleme

Veriler işlenip organize edildikten ve temizlendikten sonra modelleme aşaması başlar. Bu aşamada fazlalık olduğuna kanaat getirilen veriler elendiği için veri analizine başlanabilir. Modellemenin hızlandırılması ve maliyetinin düşürülebilmesi için;

- Veri yönetimi kontrolünün sağlanabileceği bir rota belirlemek,
- Efektif teknolojiyi (donanım ve yazılım) entegre etmek önemlidir.

Belirlenen araçlar kullanılarak analiz gerçekleştirilir ve sonrasında sonuçlar, gereksinimlere göre yorumlanır.

KPI Belirleme

KPI (Temel Performans Göstergesi) belirlendiği zaman veri analizinin belirlenen hedef doğrultusundaki ilerlemeyi inceleyerek, hedefe ulaşma oranını ortaya koyar. Performans takibi yapabilmek ve analiz adımlarındaki randımanı dinç tutabilmek için KPI'ların belirlenmesi önemlidir.

Optimizasyon ve Tekrarlama

Adımların herhangi birinde aksaklık olması, tüm analizin doğruluğunu tehlikeye atacağı için bazı aşamaların tekrarlanması, analiz sürecinin tekrarlanması demek olabilir. Veri analizi, yinelenmesi gereken bir işlemdir.

İletim

Elde edilen veri analizi sonuçları, hedef kitleye göre değişik formatlarda sunulmak üzere hazırlanır. Verilerin grafikler, tablolar ve görsellerle zenginleştirilerek anlaşılması kolay ve hızlı tüketilebilen bilgi halinde sunulması tercih edilen yöntemlerdendir. Ayrıca bir sunum metni hazırlanarak tüm sürecin hikâye haline getirilmesi, bilginin daha kalıcı, takip edilmesi, kolay bir forma dönüşmesini sağlayacaktır.

6.2 İstatistiksel Analiz ve Yöntemleri

İstatistiksel analiz sistemli bir şekilde sayısal veriler toplamaktır. Belirli bir amaç için çeşitli veriler toplanır. Bu veriler tablo ve grafik haline getirilir. Sonuçlar sınıflandırılır ve çözümlenir. Son olarak ortaya çıkan bu sonuçlar yorumlanarak veriler arası ilişkilere ve genellemelere ulaşılır. Elde edilen sonuçlar gözlem yapmaya ve geleceğe yönelik varsayımlarda bulunmaya yardımcı olur.

İstatistik, iş dünyasından ekonomi platformuna, kamu araştırmalarından vergi sistemlerine kadar pek çok alanda uygulanabilir bir bilim dalıdır. İstatistiğin temel amacı, detaylı araştırmalar sonucu elde edilen verilerin istatistiksel analiz yöntemleriyle en doğru şekilde ve amaca uygun olarak yorumlanabilesidir.

İstatistiksel çalışmaların ortak noktalarından biri nedenselliği bulmak ve bağımsız değişkenlerdeki bir değişimin bağımlı değişken üzerindeki etkilerini incelemektir. Nedenselliği ele alan temelde iki tür ana istatistiksel yöntem bulunur. Bunlar deneysel çalışmalar ve gözleme dayalı çalışmalardır.

İki çalışma türünde de bağımsız değişken veya değişkenlerdeki farklılıkların, gözlenen bağımlı değişken üzerindeki etkisi incelenir. Bu çalışma türlerinde oluşan fark ise yöntemin uygulanma biçimidir. Yöntemlerin ikisi de sağlıklı veriler ortaya koyabilir.

Deneysel çalışmalar sırasında araştırmaya konu sisteme dışarıdan müdahale edilebilir. Sistemde yapılacak bilinçli değişikliklerle bağımsız değişkenlerden kaynaklanan farklılıkların, bağımlı değişken üzerindeki etkiler incelenebilir. Gözleme dayalı çalışmalarda durum tam tersidir. Araştırma konusu sisteme kesinlikle müdahale edilmez. İstatistiksel yöntemler kullanılarak veriler toplanır. Bağımlı ve bağımsız değişkenler arasındaki ilişkiler çözümlenir.

İstatistiksel analiz yöntemleri, toplanan verilerin anlamlandırılmasına ve açıklanmasına yardımcı olur. Bunun için genel olarak 5 temel istatistiksel analiz yöntemi kullanılır. [72]

6.2.1 Betimsel Analiz Yöntemi

Betimsel analiz yöntemi araştırmaların ilk basamağıdır. İlgili veriler toplanır ve çözümlenir. Araştırmalar sonucunda ulaşılan sayısal veriler grafik veya tablo halinde özetlenir. Betimsel analizin temel hedefi ulaşılan veri değerlerini veya sıralaması yapılmış bir veri setini tablo, grafik veya nicel şekilde ifade etmektir. Bu yöntem çeşitli tablolardan ve grafiksel araçlardan faydalanır. Ortalama, Aritmetik Ortalama, Mod, Medyan, Standart Sapma, Varyans ve Korelasyon Katsayısı betimsel analizde kullanılan temel ölçülerdir.

6.2.2 Çıkarımsal Analiz Yöntemi

Çıkarımsal analiz yönteminde elde edilen veriler ve ortaya çıkan sonuçlar üzerinde çıkarımlar yapılır. Araştırmalar sonucu elde edilen veriler ve bu verilerin dağılımının özellikleri anlama sürecine dahil edilir, tümevarım mantığıyla anakütle hakkında çıkarımlara ve varsayımlara ulaşılır. Elde edilen veriler hedef anakütleyi ifade eden örneklem olarak kabul edilir. Bu yöntem çıkarımsal kestirim ve parametrik/parametrik olmayan hipotez testlerinden faydalanır.

Çıkarımsal Kestirim; momentler yöntemi, en büyük olabilirlik, en büyük artçıl, Bayes-tipi kestirimci, minimum uzaklık, maksimum aralık verme, kestirim, güven aralığı ve inanılır aralık kavramlarını kapsar.

6.2.3 Fark Analizi Yöntemi

Araştırmaya konu olan iki grup arasında farklılık olup olmadığı, eğer farklılık varsa bunun hangi sebeplerden kaynaklandığı hakkında istatistiksel verilere ulaşmayı sağlayan analiz yöntemidir. Grup ortalamaları, gruplar içi/gruplar arası varyasyonlar ve bunlara bağlı olan işlemleri analiz etmek için kullanılır. Araştırma konusu gruplar arasındaki farklılıkların tespitinde F Testi, T Testi ve Varyans Analizi kullanılır. Varyans Analizi, ANOVA olarak da isimlendirilir. ANOVA, anakütle ortalamaları arasında farkın olup olmadığını denemek için kullanılır.

Varyans analizi deneysel verilerin analiz edilmesi için özellikle pratikte çok defa tercih edilen özel bir istatistikel hipotez denemesi şeklidir. Varyans Analizi'nde verinin normal dağılım gösteren bir anakütleden geldiğini ve ancak farklı ortalamalar dolayısıyla ayrım

[72] https://www.istatistikavm.com/istatistiksel-analiz/

yapılabileceğini varsayan Sabit Etki Modeli; verinin bir farklar hiyerarşisi ile sınırlanmış olan değişik hiyerarşi içeren anakütlelerden geldiğini varsayan Rastgele Etki Modeli; sabit etkileri hem de rastgele etkiler kapsayan Karışık Etki Modeli kullanılır.

6.2.4 İlişki Analizi Yöntemi

Üzerinde araştırma yapılan veriler arasındaki ilişkileri tespit etmekte kullanılan bu yöntem, değişkenler arasındaki sistematik bağlantıların çözümlenmesinde yardımcı olur. Çapraz tablolama ve korelasyon tekniklerini içerir.

Korelasyon, olasılık kuramı ve istatistikte iki rastgele değişken arasındaki doğrusal ilişkinin yönünü ve gücünü belirtir. Genel istatistiksel kullanımda korelasyon, bağımsızlık durumundan ne kadar uzaklaşıldığını gösterir. Farklı durumlar için farklı korelasyon katsayıları geliştirilmiştir. Bunlar arasında en popülerleri Pearson çarpım-moment korelasyon katsayısı ve Sıralama korelasyonu katsayıdır.

Pearson çarpım-moment korelasyon katsayısı iki değişkenin kovaryansının, yine bu değişkenlerin standart sapmalarının çarpımına bölünmesiyle elde edilir. Korelasyon katsayısı, bağımsız değişkenler arasındaki ilişkinin yönü ve büyüklüğünü belirten katsayıdır.

Bu katsayı, (-1) ile (+1) arasında bir değer alır. Pozitif değerler direkt yönlü doğrusal ilişkiyi; negatif değerler ise ters yönlü bir doğrusal ilişkiyi belirtir. Korelasyon katsayısı 0 ise söz konusu değişkenler arasında doğrusal bir ilişki bulunmaz.

Pearson'un korelasyon katsayısı iki değişken arasındaki doğrusal ilişkinin gücünü göstermekle beraber, kestirim olarak bulunan katsayı değeri bu ilişkiyi tam olarak açıklamak için yeterli değildir. Bu sonuç eğer veriler normal dağılım göstermiyorlarsa daha da önem kazanmaktadır.

Sıralama korelasyonu ise istatistik bilimi içinde aynı istatistik birimlerinin değişik kriter değişkene göre iki değişik sıralama arasında bulunan bağlantıyı inceler. Örneklem verisi kullanarak hesaplanan sıralama korelasyon katsayısı iki sıralama arasındaki doğrusal ilişkiyi ölçer ve elde edilen katsayının istatistiksel anlamlılığını değerlendirir.

En çok kullanılan iki sıralama korelasyon katsayısı, Spearman'in ρ (rho) Sıralama korelasyon katsayısı ve Kendall'in τ (tau) sıralama korelasyon katsayısıdır. Her iki katsayı da [-1, +1] aralığı içinde tek bir değer alır. Katsayı değeri -1 ise birinci sıralama ikinci sıralamanın tümüyle tersidir ve iki seri sıralaması arasında mükemmel anlaşmazlık bulunur. Katsayı değeri 0 ise iki sıralama birbirinden tümüyle bağımsızdır. Son olarak eğer katsayı değeri +1 ise birinci sıralama ikinci sıralamanın tümüyle aynıdır ve iki seri sıralaması birbiriyle aynıdır. Sıralama korelasyon katsayısı ne kadar büyük olursa sıralamalar arasındaki uyum o denli büyük olur.

6.2.5 Tahmin Analizi Yöntemi

İstatistiksel araştırmalar sonucu elde edilen verilerin kullanılarak geleceğe yönelik tahminlerde bulunulmasına olanak sağlar. Regresyon analizi tekniklerinden faydalanılır. Regresyon analizi, iki ya da daha çok değişken arasındaki ilişkiyi ölçmek için kullanılan analiz metodudur. Değişken sayısına göre tek değişkenli regresyon veya çok değişkenli regresyon olarak adlandırılır.

Regresyonda, değişkenlerden biri bağımlı diğerleri bağımsız değişken olmalıdır. Regresyon; Doğrusal ve Doğrusal Olmayan olarak ikiye ayrılır.

Doğrusal regresyon; anakütle doğrusal regresyon modeli, İki değişkenli regresyon katsayı kestirimleri, çok değişkenli regresyon katsayı kestirimleri, hatalar varyansı ve toplam kareler, kestirim denklemin genel uyum iyiliğinin çıkarımsal kontrolü, interpolasyon ve ekstrapolasyon, ağırlıklı en küçük kareler yöntemi, değişkenlerde-hatalar modeli, genelleştirilmiş doğrusal model, güçlü regresyon ve ayrık bağımlı değişken gibi işlemler ve bunların alt dallarını barındırır.

Testleri; sıfır hipotez, I. tür ve II. tür hata, anlamlılık seviyesi ve p-değeri gibi kavramlar içerir. Hipotez testlerinde değişkenin tek veya ikili oluşuna ve parametrik olup olmamasına göre μ testi, π testi, μ1-μ2 testi, π1-π2 testi, medyan testi, ki-kare testi, Pearson ki-kare testi, Phi katsayısı, σ1/σ2 testi, Wald testi, Mann-Whitney U testi ve Wilcoxon'in işaretli sıralama testi gibi testler uygulanır.

6.3 Makine Öğrenmesi

Makine öğrenimi, bilgisayar sistemlerinin açık talimatlar yerine, düzenlere ve çıkarıma bağlı olarak görevleri gerçekleştirmek için kullanacağı algoritmalar ve istatistiksel modeller geliştirme bilimidir. Bilgisayar sistemleri büyük miktarda geçmiş veriyi işlemek ve veri düzenlerini tanımlamak için makine öğrenimi algoritmalarını kullanır. Böylece belirli bir girdi veri kümesinden, sonuçları daha doğru olarak tahmin edebilirler. Örneğin, veri bilimcileri bir tıbbi uygulamayı milyonlarca tarama görüntüsünü ve bunlara karşılık gelen teşhisleri saklayarak röntgen görüntülerinden kanseri teşhis edecek şekilde eğitebilir. Makine öğrenmesi ile ilgili önemli hususlar aşağıdaki gibidir.[73]

6.3.1 Makine Öğrenimi Neden Önemlidir?

Makine öğrenimi; büyümeyi destekleyerek, yeni gelir akışlarını açığa çıkararak ve zorlu sorunları çözerek işletmelere yardımcı olur. Veri her ne kadar işle ilgili kararların şekillenmesinde kritik bir rol oynasa da şirketler geleneksel olarak müşteri geri bildirimi, çalışanlar ve finans gibi çeşitli kaynaklardan aldıkları verileri kullanmaktadır. Makine öğrenimi araştırmaları bu süreci otomatik hale getirir ve optimize eder. İşletmeler çok yüksek hacimli verileri yüksek hızlarda analiz eden yazılımlar kullanarak daha hızlı sonuçlar elde edebilir.

6.3.2 Makine Öğrenimi Nerede Kullanılır?

Makine öğreniminin bazı ana sektörlerdeki kullanım alanları aşağıda incelenmiştir.

Üretim: Makine öğrenimi, üretim sektöründe tahmine dayalı bakımı, kalite kontrolü ve yenilikçi araştırmaları destekleyebilir. Makine öğrenimi teknolojisi ayrıca şirketlerin varlıklar, tedarik zinciri ve envanter yönetimi dahil olmak üzere lojistik çözümlerini iyileştirmesine yardımcı olur. Örneğin, bir üretim devi olan 3M, zımpara kağıdında yeniliklere imza atmak için makine öğrenmesini kullanmaktadır. Makine öğrenimi algoritmaları, 3M araştırmacılarının zımpara kağıdının şekli, boyutları ve yönünde yapılan küçük değişikliklerin aşındırıcılığı ve dayanıklılığı nasıl iyileştirdiğini analiz etmesine olanak sağlamaktadır. Bu gibi öneriler, üretim sürecinin bilgiye dayalı olarak geliştirilmesine yardımcı olur.

Sağlık hizmetleri ve yaşam bilimleri: Gün geçtikçe sayısı artan giyilebilir sensörler ve cihazlar önemli miktarda sağlık verisinin ortaya çıkmasına neden olmuştur. Makine öğrenimi programları bu bilgileri analiz edip teşhis ve tedavi konusunda doktorlara gerçek zamanlı olarak destek olabilir. Makine öğrenimi araştırmacıları kanser tümörlerini algılayan ve göz

[73] https://aws.amazon.com/tr/what-is/machine-learning/

hastalıklarını teşhis eden çözümler geliştirmektedir ve bu gibi çözümler, insan sağlığı sonuçlarında önemli iyileştirmeler sağlamaktadır. Örneğin, Cambia Health Solutions, sağlık sektöründeki start-up'lara destek olmak için makine öğrenimini kullanarak bu start-up'ların gebe kadınlar için tedaviyi otomatik hale getirmesine ve tedaviyi özelleştirmesine olanak sağlamıştır.

Finansal hizmetler: Finansal makine öğrenimi projeleri, risk analizlerinde ve regülasyonda iyileştirmeler sağlar. Makine öğrenimi teknolojisi, yatırımcıların borsa hareketlerini analiz ederek, serbest yatırım fonlarını değerlendirerek veya finansal portföyleri ayarlayarak yeni fırsatları belirlemesine olanak tanıyabilir. Ek olarak, yüksek riskli kredi müşterilerinin belirlenmesine ve dolandırıcılık belirtileri taşıyan işlemlerin tespit edilmesine yardımcı olabilir. Finansal yazılım lideri Intuit, daha kişiselleştirilmiş finansal yönetim hizmetleri oluşturmak ve son kullanıcıların finansal durumlarını iyileştirmesine yardımcı olmak için makine öğrenimini kullanmaktadır.

Perakende: Perakende sektöründe müşteri hizmetlerini, stok yönetimini, yukarıya satış ve çapraz kanallı pazarlama uygulamalarını iyileştirmek için makine öğreniminden faydalanılabilir. Örneğin, Amazon Fulfillment (AFT), yanlış konuma yerleştirilmiş envanterlerin tespit edilmesine yönelik bir makine öğrenimi modelini kullanarak altyapı maliyetlerini yüzde 40 azaltmıştır. Bu model, yılda milyonlarca global sevkiyat işlense de Amazon'un tüm ürünleri müşterilere gönderim için hazır bulunduracağına ve zamanında teslim edeceğine dair sözünü yerine getirmesine yardımcı olmaktadır.

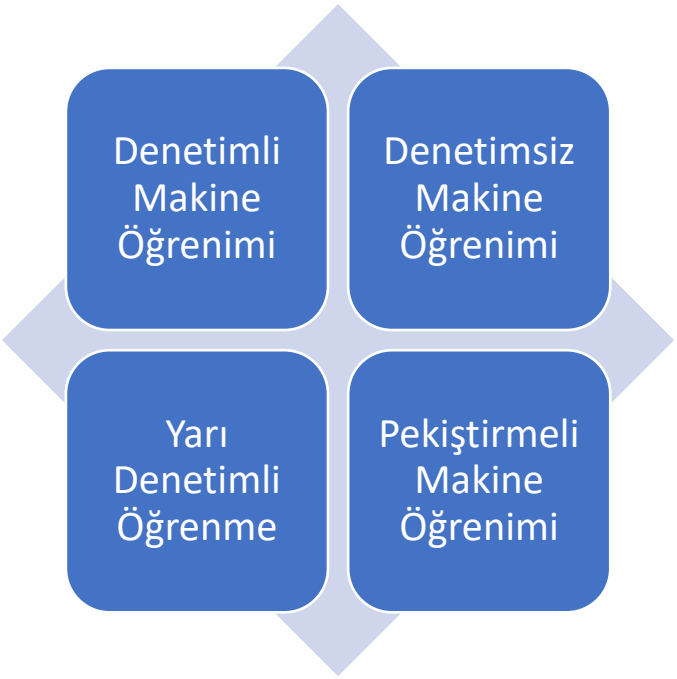
Medya ve eğlence: Eğlence şirketleri kendi hedef kitlelerini daha iyi anlamak ve sürükleyici, kişiselleştirilmiş ve istek üzerine içerik sunmak için makine öğrenimine başvurmaktadır. Makine öğrenimi algoritmaları, fragmanlar ve diğer reklamların tasarlanmasına, tüketicilere kişiselleştirilmiş içerik önerilerinde bulunulmasına ve hatta üretimin hızlandırılmasına yardımcı olacak şekilde dağıtılmaktadır.

Örneğin, Disney, ortam kitaplıklarını arşivlemek için derin öğrenme platform servisi kullanmaktadır. Alınan derin öğrenme servisi araçları, medya içeriklerini otomatik olarak etiketleyerek, açıklamalarla ilişkilendirerek ve tasnif ederek Disney yazarlarının ve animasyoncularının Disney karakterlerini hızlıca aramasına ve tanımasına olanak sağlamaktadır.

6.3.3 Makine Öğrenimi Nasıl Çalışır, Algoritma Türleri Nelerdir?

Makine öğreniminin altında yatan ana fikir, girdi ve çıktı verisi kombinasyonları arasındaki mevcut matematiksel ilişkiye dayalıdır. Makine öğrenimi modeli bu ilişkiyi önceden bilmez fakat yeterli veri kümesi sağlanması halinde tahmin edebilir. Bu durum, her makine öğrenimi algoritmasının değiştirilebilir bir matematik fonksiyonu üzerine kurulduğu anlamına gelir.

Makine öğrenimi algoritmaları, beklenen çıktı ve girdi türüne bağlı olarak dört ayrı öğrenme tarzı altında gruplandırılabilir.



Şekil 11: Makine Öğrenimi Algoritmaları

6.3.3.1 Denetimli Makine Öğrenimi

Veri bilimciler algoritmalara, bağıntıları değerlendirmeleri için etiketlenmiş ve tanımlı veriler sağlar. Örnek verilerde algoritmanın hem girdi hem de çıktısı belirtilir. Örneğin, el yazısı içeren şekillerin görüntülerine açıklamalar eklenerek bu şekillerin hangi rakama karşılık geldiği belirtilir. Bir denetimli öğrenme sistemi, yeterli örnek verilmesi halinde her bir rakamla ilişkili piksel ve şekil kümelerini tanıyabilir. Bunun sonucunda 9 ile 4 veya 6 ile 8 gibi rakamları birbirinden güvenilir bir şekilde ayırt ederek elle yazılmış rakamları tanıyabilir.

Denetimli öğrenmenin avantajları basitlik ve tasarım kolaylığıdır. Olası bir sınırlı sonuç kümesini tahmin ederken, verileri kategorilere ayırırken veya başka iki makine öğrenimi algoritmasından gelen sonuçları birleştirirken yararlı olur. Ancak, milyonlarca veri kümesinin etiketlenmesi zor olabilir. Şimdi buna daha yakından bakalım:

Veri etiketleme, girdi verilerini karşılık gelen tanımlı çıktı değerleriyle kategorilendirme sürecidir. Denetimli öğrenme, etiketli eğitim verileri gerektirir. Örneğin, milyonlarca elma ve muz görüntüsünün "elma" veya "muz" sözcüğüyle etiketlenmesi gerekecektir. Bu işlem tamamlandığında makine öğrenimi uygulamaları bir meyve görüntüsü verildiğinde bu eğitim verilerini kullanarak meyvenin adını tahmin edebilir. Ancak, milyonlarca yeni verinin etiketlenmesi zaman alan zorlu bir görevdir. Amazon Mechanical Turk gibi kitle kaynak hizmetleri, denetimli öğrenme algoritmalarının bu sınırlamasının üstesinden bir dereceye kadar gelebilir. Bu hizmetler tüm dünya geneline yayılmış uygun maliyetli büyük bir iş gücü havuzuna erişim sağlayarak veri ediniminin biraz daha kolaylaştırmaktadır.

6.3.3.2 Denetimsiz Makine Öğrenimi

Denetimsiz öğrenme algoritmaları, etiketsiz veriler kullanılarak eğitilir. Bu algoritmalar yeni verileri tarayarak girdiler ve önceden belirlenmiş çıktılar arasında anlamlı bağlantılar kurmaya çalışır. Düzenleri tespit edebilir ve verileri kategorilendirebilirler. Örneğin, denetimsiz

algoritmalar farklı haber sitelerindeki haber yazılarını spor, suç vb. genel kategoriler altında gruplandırabilir. Bir yazıdaki anlamı ve duyguyu anlamak için doğal dil işleme araçlarını kullanırlar. Perakende sektöründe, denetimsiz öğrenme müşterilerin satın alma işlemlerinin düzenlerini tespit edebilir ve "müşteri tereyağ satın alıyorsa büyük olasılıkla ekmek de satın alacaktır" gibi veri analizi sonuçları sağlayabilir.

Denetimsiz öğrenme, düzenlerin tanınmasında, anormalliklerin saptanmasında ve verilerin otomatik olarak kategorilere ayrılmasında yararlı olur. Eğitim verisi, etiketleme gerektirmediği için kurulum süreci kolaydır. Bu algoritmalar ek modelleme için verileri otomatik olarak temizlemek ve işlemek amacıyla da kullanılabilir. Bu yöntemin sınırlaması kesin tahminler sunamamasıdır. Ek olarak, belirli veri sonucu türlerini bağımsız olarak ayıramaz.

6.3.3.3 Yarı Denetimli Öğrenme

Adından da anlaşılacağı gibi bu yöntemde denetimli ve denetimsiz öğrenme bir arada kullanılır. Teknik, küçük miktarda etiketli veri ve büyük miktarda etiketsiz veri kullanarak sistemlerin eğitilmesine bağlıdır. İlk olarak etiketli veriler kullanılarak makine öğrenimi algoritması kısmen eğitilir. Daha sonra, kısmen eğitilen algoritmanın kendisi etiketsiz verileri etiketler. Bu sürece psödo-etiketleme adı verilir. Model daha sonra açıkça programlanmadan ortaya çıkan veri karışımı üzerinde yeniden eğitilir.

Bu yöntemin avantajı büyük miktarda etiketli veriye ihtiyaç duyulmamasıdır. İnsanlar tarafından okunup etiketlenmesi çok uzun zaman alacak uzun belgeler gibi verilerle çalışılırken yararlı olur.

6.3.3.4 Pekiştirmeli Öğrenme

Pekiştirmeli öğrenme, algoritmanın geçmesi gereken farklı adımlara ödüllerin iliştirildiği bir yöntemdir. Dolayısıyla, modelin amacı mümkün olduğunca fazla ödül puanı biriktirerek nihai hedefe ulaşmaktır. Video oyunları dünyası son on yılda pekiştirmeli öğrenmenin en çok uygulandığı alan olmuştur. Gelişmiş pekiştirmeli öğrenme algoritmaları, genellikle insan rakiplerini farklı şekilde yenerek klasik ve modern oyunlarda etkileyici sonuçlar elde etmiştir.

Bu yöntem, en iyi performansını belirsiz ve karmaşık veri ortamlarında göstermese de iş bağlamında nadiren uygulamaya konulmaktadır. İyi tanımlanmış görevler için verimli değildir ve geliştirici yanlılığı sonuçları etkileyebilir. Veri bilimci, ödülleri tasarlarken sonuçları etkileyebilir.

6.3.4 Makine Öğrenimi Modelleri Deterministik Midir?

Bir sistemin çıktısı tahmin edilebilir nitelikteyse bu sistemin deterministik olduğu kabul edilir. Çoğu yazılım uygulaması kullanıcının eylemine tahmin edilebilir bir şekilde yanıt verir, dolayısıyla "Kullanıcı bunu yaparsa şu olacak" denilebilir. Ancak, makine öğrenimi algoritmaları deneyim ve gözlem yoluyla öğrenir. Bu nedenle, yapıları gereği olasılıkçıdırlar. Yukarıdaki ifade bu durumda şu şekilde değişir: "Kullanıcı bunu yaparsa %X olasılıkla şu meydana gelecektir."

Makine öğreniminde, determinizm yukarıda açıklanan öğrenme yöntemleri uygulanırken izlenen bir stratejidir. Denetimli, denetimsiz ve diğer eğitim yöntemlerinden herhangi biri, işletmenin arzu ettiği sonuçlara bağlı olarak deterministik yapılabilir. Araştırma sorusu, veri alımı, yapı ve depolama kararları bir deterministik stratejinin mi yoksa deterministik olmayan bir stratejinin mi izleneceğini belirler.

Deterministik yaklaşım, toplanan verilerin doğruluğuna ve miktarına odaklıdır, dolayısıyla verimlilik belirsizlikten daha önceliklidir. Diğer taraftan, deterministik olmayan (veya olasılıkçı) süreç ise şans faktörünü yönetecek şekilde tasarlanır. Makine öğrenimi algoritmalarına öğrenme ve gözlem sırasında belirsizliği ölçme ve tanımlamada yardımcı olacak yerleşik araçlar entegre edilir.

6.3.5 Derin Öğrenme Nedir?

Derin öğrenme, insan beyni üzerine modellenmiş bir makine öğrenimi tekniğidir. Derin öğrenme algoritmaları, insan beyni tarafından kullanılan benzer bir mantık yapısıyla verileri analiz eder. Derin öğrenme tekniğinde bilgileri katmanlar halinde işlemek için yapay sinir ağları adı verilen akıllı sistemler kullanılır. Girdi katmanındaki veriler, çıktı katmanına gelmeden önce birden fazla "derin" gizli sinir ağı katmanından geçer. Ek gizli katmanlar, standart makine öğrenimi modellerine kıyasla çok daha yüksek kapasiteli öğrenmeyi destekler.

Derin öğrenme, makine öğreniminin bir alt kümesidir. Derin öğrenme algoritmaları, makine öğrenimi algoritmalarının gelişmiş ve matematiksel olarak karmaşık bir evrimi olarak kabul edilebilir.

6.3.6 Yapay Sinir Ağı Nedir?

Derin öğrenme katmanları, insan beynindeki nöronlar gibi çalışan yapay sinir ağı (ANN) düğümleridir. Düğümler bir donanım ve yazılım kombinasyonu şeklinde olabilir. Bir derin öğrenme algoritmasındaki her katman ANN düğümlerinden meydana gelir. Her düğüm veya yapay nöron birbirine bağlıdır, ayrıca ilişkili bir değer sayısına ve eşik sayısına sahiptir. Bir düğüm etkinleştirildiğinde kendi değer sayısını girdi olarak sonraki katman düğümüne gönderir. Düğüm yalnızca çıktısı belirtilen eşik değerinin üzerindeyse etkinleştirilir, aksi takdirde veri iletilmez.

6.3.7 Bilgisayarlı Görme Nedir?

Bilgisayarlı görme, derin öğrenmenin gerçek dünyada kullanılan bir uygulama alanıdır. Tıpkı yapay zeka bilgisayarların düşünmesine olanak sağladığı gibi, bilgisayarlı görme de bilgisayarların görmesine, gözlem yapmasına ve yanıt vermesine olanak sağlar. Otonom otomobiller yol tabelalarını "okumak" için bilgisayarlı görmeden yararlanır. Otomobilin kamerası tabelanın fotoğrafını çeker. Bu fotoğraf otomobilin derin öğrenme algoritmasına gönderilir. İlk gizli katman kenarları tespit eder, sonraki katman renkleri ayırt eder ve üçüncü katman ise tabeladaki yazıların ayrıntılarını tanımlar. Algoritma, örneğin, tabelada DUR yazısının bulunduğunu tahmin eder ve otomobil fren mekanizmasını devreye sokarak yanıt verir.

6.3.8 Makine Öğrenimi ve Yapay Zeka Aynı Şey Midir?

Kısa cevap hayırdır. Makine öğrenimi ve yapay zeka (AI) terimleri birbiri yerine kullanıyor olsa da ikisi aynı şey değildir. Yapay zeka, makineleri daha insanımsı kılmak için kullanılan farklı strateji ve tekniklere yönelik kapsayıcı bir terimdir. Yapay zeka, Alexa gibi akıllı asistanlardan robot süpürgelere ve otonom otomobillere kadar her şeyi kapsamaktadır. Makine öğrenimi, yapay zekanın birçok dalından biridir. Makine öğrenimi, yapay zeka olsa da tüm yapay zeka etkinlikleri makine öğrenimi olarak tanımlanamaz.

6.3.9 Makine Öğrenimi Ve Veri Bilimi Aynı Şey Midir?

Hayır, makine öğrenimi ve veri bilimi aynı şey değildir. Veri bilimi, verilerden anlam ve öngörüler çıkarmak için bilimsel bir yaklaşımın izlendiği bir araştırma alanıdır. Veri bilimciler,

veri analizi için çok çeşitli araçlar kullanır ve makine öğrenimi de bu araçlardan biridir. Veri bilimciler, veriyle ilişkili iş modeli, ilgi alanı ve veri toplama gibi büyük resim bileşenlerini anlamaya çalışırken, makine öğrenimi yalnızca ham verilerin ele alındığı bir hesaplama sürecidir.

6.3.10 Makine Öğreniminin Avantajları ve Dezavantajları Nelerdir?

Makine öğreniminin yapabildiği ve yapamadığı bazı şeylere göz atalım:

Makine öğrenimi modellerinin avantajları:

a. İnsanların gözden kaçırabileceği veri trendlerini ve düzenlerini tanımlayabilir.
b. Kurulum sonrasında insan müdahalesi olmadan çalışabilir. Örneğin, siber güvenlik yazılımlarında makine öğrenimi, yönetici girdisi olmadan ağ trafiğini sürekli olarak izleyip düzensizlikleri tespit edebilir.
c. Sonuçların doğruluk oranı zamanla artabilir.
d. Dinamik, yüksek hacimli ve karmaşık veri ortamlarında çok çeşitli veri formatlarını işleyebilir.

Makine öğrenimi modellerinin dezavantajları:

a. İlk eğitim maliyetli ve zaman alan bir süreçtir. Yeterli veri bulunmaması halinde uygulanması zor olabilir.
b. Donanımın şirket içinde kurulması durumunda ciddi miktarda bir başlangıç yatırımı gerektiren, yoğun işlem kullanımlı bir süreçtir.
c. Uzman yardımı olmadan sonuçları doğru yorumlamak ve belirsizlikleri ortadan kaldırmak zor olabilir.

6.4 İş Zekası Araçları

Veri analizi araçları konu alınan veriden anlamlı sonuçlar çıkarmak, geleceğe yönelik tahminler üretmek ve gerekirse görselleştirmek için kullanılan bilgisayar yazılımlarıdır. Bu yazılımların desktop tabir edilen bir tek bilgisayara veya bilgisayar gruplarına yüklenebilen formatta olduğu gibi, web üstünden online hizmet olarak sağlanan tipleri de vardır. İş zekası araçları çeşitli özelleştirilmiş araçlar ile iş verilerini kolay bir şekilde analiz etmeye yarayan pratik ve işlevsel veri analiz araçlarıdır. Son yıllarda İş zekası platformları birçok makine öğrenmesi algoritmasını üzerine entegre ederek iş verileri üstünde kolay analiz ve görselleştirme yapılmasını sağlayarak işte verimliliği arttırma hedefiyle sürekli gelişmektedir. Bu bölümde veri analiz ve makine öğrenmesi araçları olarak genel iş zekası platformları konu alınmıştır.

İş zekası (Business Intelligence, BI), daha iyi iş kararlarını desteklemek için veri toplama, entegre etme ve analiz etme sürecini ifade eder. İşletmelerin finans, satış, pazarlama ve diğer departmanlardan farklı iş alanlarının başarısı için hayati önem taşıyan bilgilere erişmesine izin veren çoklu yaklaşımları kapsar.[74]

İş zekası ile işiniz, iyileştirilmiş eyleme geçirilebilir verilerle güçlendirilir ve iş planlama stratejinizle iyi bir şekilde bütünleştirebileceğiniz trendler hakkında daha fazla içgörü elde etmenizi sağlar.

[74] https://bulutistan.com/blog/is-zekasi-business-intelligence/

Örneğin, bir restoran sahibi, müşterilerinin tercihlerini, beğendikleri mutfak türünü ve o belirli mutfağı neden sevdiklerini anlamak ister. Bu noktada restoran, iş zekası yazılımını kullanarak bir anket yaparak müşterilerden farklı mutfak türleri hakkında geri bildirim sağlayabilir. Yazılımda öne çıkan özellikleri kullanan restoran, müşteri zihniyetini analiz eder ve restoranda servis edilen mutfaklar hakkında değerli bilgiler edinebilir. Hangi mutfağın hangi insanlar tarafından beğenildiği ve hangi mutfağın en çok hangi gün sipariş edildiği vb. bilgilerle güçlenerek, müşterileri için hem çekici hem de tatmin edici ve işletmesi için kârlı olan iş stratejileri oluşturabilir.

İş zekasının amacı, bilgi toplamak ve analiz etmektir; böylece işletmeler daha iyi iş kararları verebilir.

İş zekası ile ilgili trendlerden bazıları aşağıdakileri içerir:

a. Yapay zeka teknolojisi
b. Büyük veri
c. Veri yönetişimi
d. Self servis iş zekası yazılım ve araçlarında artış
e. Veri yorumlama
f. İşbirlikçi iş zekası (Collaborative business intelligence)
g. Gömülü iş zekası (Embedded business intelligence)
h. Bulut analizi (Cloud analytics)

6.4.1 İş Zekası Türleri ve Metodolojileri

Stratejik iş kararları vermek ve rekabet avantajı elde etmek için bir işletmenin pazar eğilimleri, müşteri ihtiyaçları ve tüketici görüşleri hakkında net bir fikre sahip olması gerekir.

İş bilgileri toplamak için çeşitli yöntemlere erişebileceğiniz çeşitli çevrimiçi iş zekası araçları vardır. Aşağıda iş zekası ile ilgili yaygın olarak kullanılan ve yaygın olarak önerilen metodolojilerden bazılarını bulabilirsiniz:

6.4.1.1 Veri Toplama

İş zekasının ilk adımı veri toplamaktır. İstatistiksel analiz için güvenilir bilgiler sağlayabilecek ve bir işletmenin veriye dayalı kararlar almasına yardımcı olabilecek veri toplamanın çeşitli yöntemleri vardır.

Anketler: Çevrimiçi anket, daha geniş bir kitleye ulaşarak veri toplamanız için en güvenilir, ekonomik ve yaygın olarak kullanılan yöntem olmaya devam etmektedir. Anket sonuçlarını manuel olarak oluşturmak, dağıtmak ve analiz etmek karmaşık olduğundan, araştırmacıların çoğu işi yapmak için anket oluşturma araçlarına bağımlıdır. Bir çevrimiçi iş zekası toplama platformu kullanmanın başlıca faydaları, sonuçların gerçek zamanlı analizi, maliyet verimliliği, kullanım kolaylığı ve esnekliktir. Anketlerden elde edilen sonuçlar, müşterilerin hizmetin mevcut durumu hakkında ne düşündüklerini, iyileştirilmesi gereken alanları, müşterilerin beklentilerini ve ihtiyaçlarının neler olduğunu analiz etmeye katkıda bulunur. Tüm bu içgörüler, şirketin bazı değişikliklere girmesine, stratejiler uygulamasına ve daha müşteri odaklı bir organizasyon olma yolunda başarılı bir yolculuk sağlayan çalışan bağlılığını başlatmasına olanak sağlar.

Formlar: Formlar da bir tür ankettir, ancak genellikle görüşler, tutumlar, değerler vb. sonuçları içerir. Örneğin, bir banka, bir banka hesabı açmak için müşterisi ile ilgili belirli bilgilere ihtiyaç

duyar. Böyle bir senaryoda, müşteriye bankanın hesap açmak için ihtiyaç duyduğu belirli bilgileri toplaması için bir form verilir.

6.4.1.2 Analiz

Analiz, tüm verilerin tek bir platform altında toplandığı adımdır. Bir iş zekası yazılımı, aynı yazılıma gömülü gelişmiş analitik araçlarla veri toplamanın yanı sıra analiz etmenizi de sağlar. Çeşitli yöntemlerle toplanan verileri analiz etmek, bir işletmenin müşterilerinin görüşlerini anlamasına ve iyileştirilmesi gereken alanları bulmasına yardımcı olur. Bu şekilde, işletmenizin herhangi bir zamanda müşterileriniz arasında nerede durduğuna dair sağlam bir anlık görüntü elde edersiniz.

Örneğin, turizm endüstrisi, müşteri deneyimini ve memnuniyetini sürekli olarak ölçmelidir. İşletme, müşteri memnuniyeti puanlarını tutarlı bir şekilde analiz ederek ve izleyerek, müşterilerinin deneyimini iyileştirebilir ve daha yüksek gelir ve müşteri sadakati elde etmek için daha müşteri odaklı hale gelebilir.

6.4.1.3 Raporlama ve Sunum

Analizden sonraki adım, metriklerin ne anlama geldiğini anlamaktır. Bu adım çok önemlidir, çünkü verilerin yanlış yorumlanması işletmenizi uçuruma sürükleyebilir. Verileri görsel infografiklere dönüştürmek bazen bir kişinin anlamasını kolaylaştırabilir. Bu tür bir anlayış, organizasyonun en acil ticari, operasyonel ve pazarlama sorularına yanıt bulmasını sağlar.

Bu adımlar, iş zekası yazılımını etkin bir şekilde kullanmaya başlamanıza yardımcı olacaktır, ancak bu son adım değildir. Bir işletmenin rekabette kalmak ve sürekli değişen müşteri ihtiyaçlarını karşılamaya devam etmek ve hatta gelecek için bir sonraki en iyi adımları bulması için gerçek zamanlı verileri sürekli olarak izlemesi ve analiz etmesi gerekir. İş zekasını etkin bir şekilde kullanmak için bu yolu izlemek, bir organizasyonun daha akıllıca para ve zaman harcamasını ve gelecekteki hedefleri, ihtiyaçları ve eğilimleri başarılı bir şekilde ele almasını sağlayacaktır.

6.4.2 İş Zekasının Avantajları

İş zekası, bir işletmenin stratejik, taktiksel ve operasyonel iş kararları üzerinde doğrudan bir etkiye sahiptir. Varsayımlar ve içgüdüsel duygular yerine geçmiş verileri kullanarak gerçeklere dayalı karar vermeyi destekler. Bu araçlar, kullanıcılara işin doğası hakkında ayrıntılı bilgi sağlamak için veri analizi yapar ve raporlar, özetler, gösterge tabloları, haritalar, grafikler ve çizelgeler oluşturur.

Bir işletmedeki farklı departmanlar için belirtilen avantajların yanı sıra, iş zekasının birkaç avantajı daha vardır:

1. Doğru bir iş zekası yazılımı, toplanan verileri raporlar, analitik panolar ve infografikler kullanarak işletmedeki üretkenliği artırmaya yardımcı olur.
2. Çeşitli departmanlara, ürünlere, hizmetlere vb. bölümlere ayrılmış, şirketin bütünsel bir görünümüne sahip bir organizasyon sağlar ve dikkat edilmesi veya iyileştirilmesi gereken alanların belirlenmesini kolaylaştırır.
3. Bir işletmedeki karmaşık süreçler, bir şirketin daha hızlı ve verimli iş süreçlerine yol açan zaman ve çabayı azaltmasına olanak tanıyan gelişmiş otomatik analitik kullanılarak düzene sokulabilir.
4. BI yazılımı kullanılarak görsel infografikler ve anlaşılması kolay raporlar oluşturulabilir ve teknik bilgisi olmayan kişilerin bile metriklerinin anlamını anlamalarını sağlar.

6.4.3 İş Zekasının Önemi

Günümüzün sürekli değişen iş ortamında, rekabet avantajından yararlanmak için iş zekasına ihtiyaç vardır. İş zekası, bir işletmenin müşteri görüşlerini, pazarı ve müşteri davranışını değerlendirmesine yardımcı olur ve bu da onlara daha yüksek pazar payları kazanma ve daha yüksek gelir elde etme konusunda üstünlük sağlar. İş zekasının herhangi bir işletme için bir varlık olmasının bazı nedenleri aşağıdaki şekildedir:

1. **Eyleme geçirilebilir içgörüler toplama:** İş zekası, iş odaklı ham verileri kullanılabilir bilgilere dönüştürür. Ham veriler size iş parametreleriniz hakkında eyleme geçirilebilir içgörüler vermez, ancak BI bir işletmeye daha müşteri odaklı stratejiler tasarlamak için kullanılabilecek sorunlu noktaları veya fırsatları belirlemek için kapsamlı bir veri analizi sağlar.
2. **İşletmenin derinlemesine anlaşılması:** Genellikle gözden kaçanlar da dahil olmak üzere işin her bir bileşenini bilmiyorsanız, işi bir bütün olarak anlamak zordur. İş zekası, bir işletmenin dikkat gerektiren her bileşeni tanımlamasını ve buna göre iyileştirmeler yapmasını sağlar.
3. **Satış ve pazarlama hedeflerine ulaşma:** Şirket hedef pazarı, trendleri veya sürekli değişen müşteri ihtiyaçlarını anlamıyorsa, bu satış ve pazarlama hedeflerine ulaşmak zordur. İş zekası, bir işletmenin satışlarını başlatmak, pazarlama işlevinin performansını artırmak ve bu satış ve pazarlama hedeflerine ulaşmak için her iki ekibin senkronize edilmesine yardımcı olmak için derinlemesine analiz sunar.
4. **Alıcı davranışını ve eğilimlerini tahmin etme:** Müşteri katılımı, günümüzün iş dünyasında sıklıkla tartışılan bir kelimedir. Bu nedenle, zorlu bir satışa dayalı eski modası geçmiş tekniklere güvenmek yerine potansiyel müşterileri size çekmek önemlidir. Bir iş zekası yazılımı, bir şirketin müşteri yolculuğu sırasındaki her etkileşime veya her geri bildirime dayalı olarak bütünsel müşteri profilleri oluşturmasını sağlar. Bu, onlara alıcı davranışı ve eğilimleri hakkında ayrıntılı bilgiler sağlayan değerli istihbarat toplamalarına olanak tanır ve böylece satış, pazarlama veya büyüme stratejilerini buna göre geliştirmelerine olanak tanır.
5. **Genel üretkenliği artırma:** Birçok işletme, bir kuruluşun büyümesini engelleyen verimsiz darboğazlara, eski geleneksel süreçlere ve manuel rutin görevlere sahiptir. İş zekası yazılımı, bu darboğazları ortadan kaldırabilir, rutin görevleri otomatikleştirebilir ve herkesin işine yeni organizasyon seviyeleri ve önceliklendirme getirerek süreçleri iyileştirebilir. Bu, verimli ve son derece duyarlı müşteri hizmetleri, insan kaynaklarının daha iyi kullanılması, pazarlama kampanyalarının doğru bir şekilde ölçülmesini sağlayarak işletme genelinde genel üretkenliği artırır.
6. **Veri yönetimi ve düzenlemeleri:** Yeni GDPR ve KVKK düzenlemeleri, kişisel verilerin toplanma, kullanılma, saklanma, işlenme ve paylaşılma şekline birçok kısıtlama getirdi. Yeni yasalar, verilerin doğru ve güncel tutulması, verilerin işlenmesi için gerekçelerin gösterilmesi ve daha iyi şeffaflık için net bir gizlilik politikası formüle edilmesi için gereklilikleri içerir. GDPR ve KVKK uyumlu bir iş zekası yazılımı, tüm verileri merkezileştirmenize yardımcı olur, bu da şeffaflığı artırır ve yanlışlıklar ve boşlukları ortaya çıkarır. Ayrıca, bir işletmenin düzenleyiciler ve müşteriler tarafından kara listeye alınmamak için küresel düzenlemeleri ve yasaları karşılayan bir konumda olmasını sağlar.
7. **Hızlandırılmış ROI:** İş zekası analiz ve modelleme yoluyla günlük verimliliği, satış dönüşüm ölçümlerini ve müşteri deneyimini yöneterek bir işletmenin ROI'yi hızlandırmasına yardımcı olur.

6.4.4 İş Zekası İşletmenize Nasıl Yardımcı Olur?

BI yazılımı, işletmelerin veri toplamasına, depolamasına ve analiz etmesine yardımcı olur, ancak hepsi bu kadar değildir. BI çözümleri, şirketlerin bu bilgileri metriklere, puan kartlarına, gösterge tablolarına, raporlara ve içgörülere dönüştürmesine yardımcı olur. Bu, işletmenin ve çalışanların kararları ve davranışları doğru bir şekilde görselleştirmesini, yorumlamasını, anlamasını ve bilgilendirmesini daha iyi sağlar. Yazılım platformları ayrıca verileri daha etkin bir şekilde işlemek, eğilimleri ortaya çıkarmak, içgörüler oluşturmak ve performansı tahmin etmek için genellikle yapay zeka ve makine öğrenimi teknolojilerini içerir.

6.4.5 İş Zekasının İş Yapma Biçimini Nasıl Geliştirir?

Günümüzde iş zekası araçları sayesinde bilgi analizi ve performans değerlendirmesi hızlandığından, kurumların verimsizlikleri azaltmalarına, potansiyel sorunları tespit etmelerine, yeni gelir akışları bulmalarına ve geleceğe yönelik büyüme alanlarını belirlemelerine yardımcı olması açısından değerlidir.

İşletmelerin BI kullanırken elde ettiği avantajlardan bazıları şunlardır:[75]

a. Operasyonel süreçlerde daha yüksek verimlilik.
b. Müşteri davranışı ve alışveriş alışkanlıkları hakkında içgörü.
c. Satış, pazarlama ve finansal performansın doğru takibi.
d. Geçmiş ve mevcut verileri temel alan net karşılaştırmalar.
e. Veri anormallikleri ve müşteri sorunları hakkında anında uyarılar.
f. Departmanlar arasında gerçek zamanlı olarak paylaşılabilen analizler.

Geçmişte, iş zekası araçları öncelikle veri analistleri ve BT kullanıcıları tarafından kullanılıyordu. Artık, self servis BI platformları iş zekasını, iş zekası yöneticilerinden operasyon takımlarına kadar herkes için kullanılabilir hale getirimiştir.

İş zekasının altı temel alanda iş yapma biçimini nasıl geliştirdiği aşağıda açıklanmıştır:

a. **Müşteri deneyimi:** Tüm müşteri bilgilerinize tek bir yerden erişerek kaynakları müşteri etkileşimini ve desteğini olumlu yönde etkileyecek önemli alanlara yönlendirin.
b. **Satış ve pazarlama:** Satış ve pazarlama performansı, tüketici davranışı ve satın alma eğilimleri hakkında görünürlük elde edin. Bu görünürlük, gelecekteki pazarlama girişimlerinin etkili olmasını ve geliri artırmasını sağlar.
c. **Operasyon:** Rutin analiz görevlerini otomatikleştirerek, süreçleri iyileştirerek, verimsizlikleri azaltarak ve üretkenliği artırarak operasyonu geliştirin.
d. **Finans:** Kurumun finansal durumuyla ilgili bütüncül bir görünüm elde etmek, geçmiş verileri incelemek, riski hesaplamak ve eğilimleri tahmin etmek için özel dashboard'ları kullanın.
e. **Stok denetimi:** Stok yönetimini iyileştirmek, karşılamayı hızlandırmak ve satın alma eğilimlerini tahmin etmeye yardımcı olmak için veri analizini ve raporlamayı otomatikleştirin.
f. **Güvenlik ve uyumluluk:** Doğruluğu ve şeffaflığı artırmak için verileri merkezileştirerek hataları, güvenlik sorunlarını kolayca ortaya çıkarın ve uyumluluk risklerini azaltın.

[75] https://powerbi.microsoft.com/tr-tr/what-is-business-intelligence/

7 Gelişen Trendler ve Gelecek Görünümü

21. yüzyıl, tarihimizde en hızlı teknolojik ve sosyoekonomik değişimlere tanıklık eden bir dönem olarak karşımıza çıkmaktadır. Küresel ekonomi, teknoloji, çevre ve toplum, düşünülenden daha hızlı bir şekilde dönüşüm sergilemekle birlikte; bilgi ve iletişim teknolojileri, yapay zekâ, sürdürülebilirlik ve yeşil dönüşüm, genetik mühendislik ve küreselleşme gibi faktörler, bu değişim sürecinin önemli aktörleri haline gelmiştir.

Gözlemlenen bu önemli trendlerin toplumlarımız, ekonomilerimiz ve çevremiz üzerindeki potansiyel etkileri de oldukça büyüktür. Bir yandan bu trendler, inanılmaz olanaklar ve potansiyel büyüme alanları sunarken, diğer yandan da eşitsizlik, iş güvencesizliği ve çevresel krizler gibi büyük zorlukları da beraberinde getirmektedir.

Teknolojik alanda ortaya çıkan gelişmelerin ve bu gelişmelerin yaratacağı zorlukların anlaşılması, geleceğimizi nasıl şekillendirebileceği konusunda bizlere bilinçli bir bakış açısı yaratacaktır.

Gelişen trendlerin ve gelecek görünümünün kapsamlı bir analizi, mevcut durumumuzu daha iyi anlamamıza ve gelecekte karşılaşabileceğimiz zorluklara karşı daha iyi hazırlanmamıza olanak sağlayacaktır. Dolayısıyla bu gelişim öncesinde çıkarılacak öngörüler de akademisyenler, politikacılar, iş dünyası liderleri ve genel olarak geleceği anlamak ve şekillendirmek isteyen herkes için değerli bir kaynak olacaktır.

Gelişen trendlerin toplumda olumlu ve olumsuz etkiler yaratacağı aşikârdır. Bu hızlı gelişim, hem kişisel yaşantıları hem de toplumun genel yapısını yeniden şekillendirmektedir. Yeni gelişmelerin yaratacağı değişimlere ve toplum üzerinde yaratacağı genel etkiye detaylıca değinmemiz gerekecektir.

Teknolojik Dönüşüm ve Kişisel Hayat: Yapay zekâ (AI) ve makine öğrenmesi teknolojileri, günlük hayatımızı hızla değiştirmektedir. Akıllı evler, yapay zekâ destekli kişisel asistanlar ve kişiselleştirilmiş öğrenme platformları, bu teknolojilerin hayatlarımızı daha verimli ve rahat hale getirebileceğinin somut örnekleridir. Ayrıca, sağlık hizmetleri alanında da kendine kullanım alanı bulan yapay zekâ ve makine öğrenmesi, hastalıkların teşhis ve tedavisini daha erken ve etkili bir hale getirmekte, böylece yaşam kalitesini artırmaktadır.

Çalışma Hayatında Değişim: Gelişen teknolojiler, iş dünyasında da büyük bir etki ortaya çıkarmaktadır. Otomasyon ve robotik teknolojiler, belirli sektörlerde işleri tehdit ederken, aynı zamanda daha önce var olmayan yeni meslekler ve yetenekler yaratmaktadır. Veri bilimi, siber güvenlik ve yapay zekâ gibi alanların, geleceğin iş dünyasında kilit rol oynayacağı sarihtir. Dijitalleşme ve internet teknolojilerinin, esnek ve uzaktan çalışma imkânlarını artırması, iş ve özel hayat arasında denge sağlanmasına yardımcı olurken diğer yandan daha geniş iş imkânları yelpazesine erişim olanağı sunmaktadır.

Ekonomik Modelde Dönüşüm: Paylaşım ekonomisi, mülkiyet kavramına alternatif olarak erişim modeline dayalı bir ekonomik yapının ortaya çıkmasını sağlamıştır. Uber, Airbnb ve benzeri platformlar aracılığıyla, kişiler, kendi varlıklarını (araba, ev vb.) başkalarıyla paylaşarak gelir elde etme yoluna gitmektedirler. Bunun yanında, kripto paralar ve merkezi olmayan finans (DeFi) sistemleri, finansal işlemleri ve yatırımları demokratikleştirirken, herkesin bu hizmetlere olan erişimini de kolaylaştırmaktadır.

Sürdürülebilir Yaşamın Yükselişi: Çevresel sürdürülebilirlik ve yeşil teknolojiler, enerji tüketiminden atık yönetimine kadar yaşamlarımızın çeşitli alanlarında değişikliklere yol açmaktadır. Yenilenebilir enerji kaynaklarına dayalı elektrikli araçlar ve enerji verimli evler, karbon ayak izinin azaltılmasına yardımcı olmaktadır. Sirküler ekonomi modeli, atıkları minimuma indirirken kaynakların daha etkin kullanılmasını sağlamaktadır.

Bu kapsamda gelişen teknolojilerin, işten günlük yaşama, tıbbi uygulamalardan eğitime, hemen her sektörde gelişim gösterdiği ortadadır. Bu alanlardaki gelişimlerde Yapay Zekâ Teknolojileri (AI)'nin etkisi açıkça hissedilmektedir. Yapay zekâ, geniş veri setlerini işleme, öğrenme ve karar verme yetenekleri sayesinde birçok uygulama için devrim niteliğinde bir araçtır.

Yapay zekâ, birçok sektörde sürdürülebilirlik, verimlilik ve kişiselleştirme talepleriyle baş etmek için hayati bir rol oynamaktadır. Örneğin, imalat sektöründe yapay zeka, makinelerin hataları önceden tahmin etmesine ve böylece üretim süreçlerini optimize etmesine olanak sağlar. Sağlık sektöründe ise görüntü işleme ve genetik verilerin analizi ile hastalıkların erken teşhisi için önemli bir araç haline gelmiştir. Bu tür uygulamalar, hizmet kalitesini artırırken maliyetleri düşürmeye yardımcı olur.

Eğitim, e-ticaret ve ulaşım gibi alanlarda da, kişiselleştirilmiş deneyimler elde etmek amacıyla yapay zekâ kullanılmaktadır. Öğrencilerin bireysel öğrenme stillerine uygun eğitim materyalleri sunan yapay zekâ tabanlı eğitim platformları, öğrenme deneyimini daha etkili hale getirmektedir. E-ticarette müşterilere öneriler sunmak ve müşteri hizmetlerini otomatikleştirmek için kullanılırken, ulaşımda, otomatik sürüş sistemleri ve trafik akışını optimize etmek amacıyla kullanılmaktadır. Bu noktada yapay zekâ teknolojisi, daha etkili, güvenli ve kişiselleştirilmiş hizmetler sağlamak için önemli bir araçtır.

7.1 Yapay Zekâ ve Makine Öğrenmesinin İnsan Yaşamına Etkisi

Teknolojik ilerleme çağında, yapay zekâ (AI) ve makine öğrenmesi (ML) tüm dünyada hayatı dönüştüren kilit araçlar haline gelmiştir. Bu alandaki ilerlemeler, sağlık hizmetlerinden eğitime, iş dünyasından kişisel yaşamlarımıza kadar etkileyerek geleceğimizi şekillendirmektedir. Yapay zekâ (AI) ve makine öğrenmesi (ML), veri biliminden, doğru kararlar almak için kullanılan araçlara kadar geniş bir yelpazede kullanılmaktadır. Bu teknolojilerin sürekli olarak gelişmesi, toplumların gelecekte neye benzeyeceği konusunda önemli soruları gündeme getirmektedir. Yapay zekâ ve makine öğreniminin yaygınlaşmasının ortaya çıkaracağı dönüşümler ve sonuçları analiz etmek büyük önem arz etmektedir.

Bununla birlikte, bu teknolojilerin yaygınlaşmasının getireceği potansiyel sorunları ve etik konuları da göz önünde bulundurmak gerekir. Özellikle, yapay zekâ ve makine öğreniminin etik kullanımı, algoritmaların önyargılarını ve toplum üzerindeki potansiyel etkilerini ele almak, bu alandaki araştırmaların ayrılmaz bir parçasını oluşturmaktadır.

Endüstride Yapay Zekâ ve Makine Öğrenmenin Etkisi: Endüstri alanında (AI) ve (ML), üretim süreçlerini optimize etmek, hataları azaltmak ve üretim süreçlerinde verimliliği artırmak amacıyla kendine kullanım alanı bulmaktadır. Makine öğrenmesi algoritmaları, verilerden öğrenmekte ve zaman içinde daha doğru tahminler yapabilmektedir. Bu sistem öngörücü bakım modelleri oluşturmak için kullanılır. Bu kullanım şekli, arızaların önceden belirlenmesine ve bakımın zamanında yapılmasına olanak sağlar. Bu noktada asıl hedef maliyetlerin düşmesi ve verimliliğin artırılmasıdır.

Sağlıkta Yapay Zekâ ve Makine Öğrenmenin Etkisi: Sağlık hizmetlerinde (AI) ve (ML), daha doğru teşhisler, kişiye özel tedavi planları ve hastalıkların erken teşhisi gibi alanlarda devrim yaratmaktadır. Bu noktada makine öğrenmesi algoritmaları, tıbbi görüntüleri analiz ederek, doktorların bir hastalığı teşhis etmesine yardımcı olabilir. Ayrıca, genetik verinin analizi, genetik hastalıkların erken teşhisine ve kişiselleştirilmiş tedavi yaklaşımlarının geliştirilmesine yardımcı olabilir.

Eğitimde Yapay Zekâ ve Makine Öğrenmenin Etkisi: Eğitim sektöründe (AI) ve (ML), kişiselleştirilmiş öğrenme deneyimleri sunma amaçlı olarak kullanılmaktadır. Herhangi bir öğrencinin öğrenme stilini ve ihtiyaçlarını anlar ve bu bilgiyi öğrenciye en uygun öğrenme materyallerini ve kaynaklarını sağlamak için kullanır. Bunun yanında yapay zekâ, eğitimcilerin öğrenci performansını izlemelerine ve gelişim alanlarını belirlemelerine de yardımcı olabilir.

Akıllı şehirler ve sürdürülebilir yaşam konularını düşündüğümüzde yapay zekâ (AI) ve makine öğrenmesi (ML), şehirlerin daha etkin ve sürdürülebilir hale gelmesine yardımcı olabilmektedir. Bu teknolojiler, trafik yönetiminden enerji tüketimine, her bir bireyin yaşam kalitesini artırmak için kentsel çevreyi daha akıllı hale getirme potansiyeline sahiptir. Ayrıca, iklim değişikliği gibi büyük ölçekli çevresel sorunlara yanıt verme konusunda hayati bir rol oynayabilirler.

Yapay zekâ ve makine öğrenmesi, iş süreçlerini dönüştürmekte ve organizasyonların operasyonel verimliliğini artırmak amacıyla kullanılabilmektedir. Bunlar, otomasyon, veri analizi ve karar verme süreçlerinde yardımcı olabilmektedir. Ayrıca, makine öğrenmesi algoritmaları, tüketici davranışlarına ilişkin bilgileri analiz edebilir ve işletmelerin müşteri deneyimlerini kişiselleştirmesine yardımcı olabilir.

Yapay zekâ ve makine öğrenmesinin gelecekteki etkileri, geniş kapsamlı ve dönüştürücü olabilir. Ancak, bu teknolojilerin etik ve toplumsal etkilerinin yanı sıra, onların sorumlu ve etik bir şekilde nasıl kullanılacağı konusunda dikkatli düşünülmesi gerekmektedir. Gelecekteki teknolojik ilerlemelerin, (AI) ve (ML)'nin gelişimine bağlı olarak şekilleneceği ve bu teknolojilerin potansiyelini anlamanın, her sektör için hayati önem taşıyacağı ortadadır.

7.2 Nesnelerin İnternetinin Veri Uzayına Entegrasyonu

Nesnelerin İnterneti veya literatürde en sık kullanılan haliyle IoT, birbirine bağlanmış fiziksel ve akıllı varlıklardan (ağa bağlanabilen her türlü cihaz, alet, araç, gereç, sensör vb.) oluşan dünya çapında bir ağ öngörüsünün ifadesidir. Bu varlıkların uygulamaları esnasında çok büyük miktarlarda veri üretilmekte ve böylelikle IoT teknolojisinin yayılma ivmesi artıp üretilen verinin ölçeği giderek daha da büyümektedir.[76] Hatta öyle ki, yapay zekâ ve ağ teknolojilerinde yaşanan hızlı gelişme ile birlikte IoT teknolojisinin gelecekte sosyal yaşamın başlıca gelişim unsuru olacağı öngörülmektedir.[77]

Nesnelerin İnterneti (IoT) ve veri biliminin birleşimi, birçok sektörde paradigmaları yeniden şekillendirmiştir. IoT cihazlarının artan kullanımı, dünya çapında devasa miktarlarda veri üretilmesine neden olmaktadır. Bu veri birikimi, veri biliminin gelişmesine ve IoT verisinin entegrasyonunun daha fazla anlam kazanmasına sebebiyet vermektedir.

[76] Siow, E., Tiropanis, T., & Hall, W. (2018). Analytics for the Internet of Things: A Survey. ACM Computing Surveys (CSUR), 51(4), 74:1–74:36. https://doi.org/10.1145/3204947

[77] Yan, Y., Huang, C., Wang, Q., & Hu, B. (2020). Data mining of customer choice behavior in internet of things within relationship network. International Journal of Information Management, 50, 566-574. https://doi.org/10.1016/j.ijinfomgt.2018.11.013

IoT, nesnelerin birbirleriyle ve çevreleriyle iletişim kurmasını sağlayan teknolojilerin birleşimidir. Bu tanım, otomatik ev sistemlerinden endüstriyel otomasyon sistemlerine kadar her şeyi içermektedir. Bu cihazlar ve sistemler, kullanıcı davranışları, sistemin durumu ve çevresel faktörler hakkında sürekli veri üretmektedir. Bu, işletmelerin ve kuruluşların, operasyonlarını optimize etmek ve hizmetlerini geliştirmek için kullanabilecekleri bir veri kaynağı oluşturur.

Veri bilimi, işletmede ortaya çıkan gerçek iş problemlerini verilerle anlamlandıran ve bu problemlere çözüm sunacak veri uygulamaları geliştiren, içinde bilgisayar bilimleri, istatistik, matematik ve bilişim bilimleri dâhil olmak üzere birçok bilim dalını içeren disiplinlerarası bir çalışma alanıdır.[78] İstatistiksel analiz, makine öğrenmesi ve yapay zekâ gibi teknikler, verinin yorumlanmasını ve kullanılmasını sağlar. IoT'nin veri bilimine entegrasyonu, bu cihazların ürettiği verinin, iş dünyasında, hükümetlerde ve diğer kuruluşlarda daha etkili bir şekilde kullanılmasını sağlar.

IoT ve veri bilimi arasındaki bu sinerji, birçok endüstride verimliliği artırmak, maliyetleri düşürmek ve hizmet kalitesini iyileştirmek için yeni yollar sunar. Örneğin, bir üretim tesisindeki IoT cihazları, ekipmanın durumu hakkında veri sağlayabilir. Bu veri, veri bilimi teknikleriyle analiz edilerek, ekipmanın bakım zamanlamasını optimize etmek ve üretim hattının genel verimliliğini artırmak için kullanılabilir.

Ancak, IoT'nin veri alanına entegrasyonu da bir dizi zorluk ve sorunları beraberinde getirir. Gizlilik ve veri güvenliği konuları, hızla büyüyen bir endişe haline gelmiştir. Bu ve diğer potansiyel zorlukları anlamak ve ele almak, IoT ve veri biliminin etkin bir şekilde entegrasyonu için kritik öneme sahiptir.

Veri Bilimi ve Analiz: Veri bilimi, bu sürekli üretilen veriyi anlamak ve işlemek için kullanılan bir araçtır. Veri bilimciler, istatistiksel analiz, makine öğrenmesi, veri madenciliği ve yapay zekâ gibi bir dizi teknik kullanarak, IoT cihazlarından gelen ham veriyi kullanılabilir ve anlamlı bilgilere dönüştürmektedir. Bu bilgiler, daha etkili kararlar almayı, performansı iyileştirmeyi ve hatta gelecekteki eğilimleri ve davranışları tahmin etmeyi sağlar.

IoT'nin Veri Bilimine Entegrasyonunun Etkileri: IoT'nin veri bilimine entegrasyonunun pek çok etkisinin bulunduğunu söyleyebiliriz. İlk olarak, daha büyük ve daha karmaşık veri setlerinin analiz edilmesi mümkün hale gelmiştir. Bu, daha derinlemesine ve daha doğru analizler yapmayı, daha karmaşık ve sofistike modeller oluşturmayı ve daha hassas tahminler yapmayı mümkün kılar. İkinci olarak ise IoT cihazlarının yaygınlaşmasıyla birlikte, gerçek zamanlı veya neredeyse gerçek zamanlı veri analizinin önemi artmıştır. Bu, operasyonel verimlilik, önleyici bakım ve anında müşteri geri bildirimi gibi konularda önemli avantajlar sağlamaktadır.

Zorluklar ve Gelecek Görünümü: Elbette, IoT'nin veri bilimine entegrasyonu aynı zamanda yeni zorlukları ve sorunları da beraberinde getirmektedir. Veri güvenliği, gizlilik ve etik, bu alanda ele alınması gereken kritik konulardır. Ayrıca, bu devasa veri akışını yönetmek, depolamak ve analiz etmek için gereken altyapı ve kapasite de önemli bir sorundur.

[78] Hamilton, Booz Allen. (2015). The Field Guide to Data Science, 126. Retrieved from papers3://publication/uuid/1941BECE-325A-45B6-B10C-5A850FA5D609

IoT ve veri bilimi, teknoloji ve toplumun geleceğinin iki önemli yapı taşıdır. Birlikte, iş dünyasından sağlık hizmetlerine, enerji yönetiminden çevresel sürdürülebilirliğe kadar birçok alanda derin ve kalıcı değişiklikler yaratma potansiyeline sahiptir. Ancak, bu potansiyeli tam olarak gerçekleştirmek için, bu teknolojilerin getirdiği zorlukları anlamak ve ele almak, onları etik ve sürdürülebilir bir şekilde kullanmak önemlidir.

IoT ve veri biliminin birlikte uygulanması, daha derinlemesine ve daha doğru analizler yapmayı, daha karmaşık ve sofistike modeller oluşturmayı ve daha hassas tahminler yapmayı mümkün kılmaktadır. Bunun yanı sıra, bu entegrasyon iş dünyası, sağlık hizmetleri, enerji yönetimi ve çevresel sürdürülebilirlik gibi alanlarda çok sayıda uygulama ve olasılığı beraberinde getirmektedir.

Ancak, bu potansiyeli tamamen gerçekleştirmek için, IoT'nin veri bilimine entegrasyonu sürecinin getirdiği zorlukların da dikkatlice ele alınması gerekmektedir. Gizlilik, veri güvenliği ve etik gibi konuların yanı sıra veri yönetimi, depolama ve analiz için gereken altyapı ve kapasite de bu zorluklar arasında yer almaktadır.

Kısacası, IoT'nin veri bilimine entegrasyonu, yeni ve heyecan verici olasılıklarla dolu, ancak aynı zamanda karmaşık zorlukları da beraberinde getiren bir gelişmedir. Ancak, bu zorlukları başarılı bir şekilde ele almayı başarabilirsek, IoT ve veri bilimi, hem bugünün hem de geleceğin dünyasını şekillendiren önemli araçlar olmaya devam edecektir.

7.3 Veri Uzayının Etik ve Sosyal Etkileri

Teknolojik gelişmeler ve dijital çağ, veriyi bilgi çağının temel taşı haline getirmiştir. Günlük yaşamda ve iş dünyasında veri, giderek daha merkezi bir konuma taşınmış ve önemli bir “para birimi” haline gelmiştir. Ancak bu değişim, verinin etik ve sosyal etkilerinin de derinlemesine analiz edilmesini gerektirir. Makalemizin bu bölümünde, verinin toplanması, kullanılması ve paylaşılmasının etik ve sosyal boyutlarının ele alınması amaçlanmaktadır.

Veri toplama, bireysel ve toplumsal yaşamın çeşitli alanlarında her geçen gün daha önemli bir hale gelmektedir. Bu süreçte, veri toplamanın kişisel gizlilik hakları üzerindeki etkisini de detaylı analiz etmek gerekmektedir. Gizlilik, dijital çağda birçok kişi ve kurum için birincil endişe haline gelmiştir. Ancak, gizlilik endişeleri tek başına yeterli değildir. Veri toplamanın etik ve sosyal sonuçları, verinin nasıl kullanıldığına ve kimlerin erişebildiğine de bağlıdır. Veri güvenliği konusu, hükümetler, şirketler ve bireyler için büyük bir öneme sahiptir.

Verinin etik ve sosyal etkileri, sadece veri toplama ve güvenliği ile sınırlı değildir. Veriye dayalı algoritmalar ve makine öğrenmesi, giderek daha fazla karar verme sürecine dahil olmaktadır. Bu durum, algoritmaların etik ve sosyal sonuçlarını da önemli kılar. Algoritmalara dayalı kararların, eşitsizlik ve adaletsizlik yaratma potansiyeli vardır. Özellikle algoritma temelli kararların, bireysel ve toplumsal önyargıları pekiştirebileceği endişesi, adil algoritmalara duyulan ihtiyacı da beraberinde getirmektedir.

Makine öğrenmesi ve yapay zekanın hızla gelişmesi, algoritmaların ve verinin etik ve sosyal etkilerinin analizini daha da karmaşık hale getirmektedir. Veri bilimi ve veriye dayalı teknolojiler, sosyal normları, değerleri ve yapıları etkileyebilir. Verinin sosyal etkisi, bireylerin yaşamlarından toplumların işleyişine kadar geniş bir yelpazede olabilir. Buna ek olarak, verinin etik ve sosyal etkileri, demografik ve coğrafi çeşitliliği de içerir. Farklı toplumlar ve demografik gruplar, verinin etkilerini farklı şekillerde yaşayabilirler. Bu nedenle, verinin etik ve sosyal etkilerini analiz ederken bu çeşitliliği dikkate almak büyük önem arz etmektedir.

Veri biliminin etik ve sosyal etkilerini ele alırken, geleceğe yönelik tahminler ve beklentiler de önemlidir. Veri biliminin ve veriye dayalı teknolojilerin gelecekteki gelişiminin, etik ve sosyal sonuçlarının analizini etkileme olasılığı yüksektir.

Veri Toplama ve Gizlilik: Bir veri bilimcisi için, ham veri en değerli hammadde haline gelmiştir. Ancak, veri toplamanın artan kolaylığı ve yaygınlığı, birçok gizlilik endişesini de beraberinde getirmiştir. Kişisel bilgiler, alışkanlıklar, ilgi alanları ve daha fazlası gibi konulara dair detaylı veriler toplanmaktadır ve bu durum, bireylerin gizlilik haklarını ihlal edebilir. Bu durum, gizliliği koruma ve aynı zamanda verinin değerinden yararlanma arasında hassas bir denge kurma gereksinimini doğurur.

Algoritmalara Dayalı Kararlar ve Adillik: Veri bilimi ve makine öğrenmesi, giderek daha fazla algoritma tabanlı karar mekanizması oluşturmuştur. Ancak, bu algoritmaların tasarımında ve eğitiminde kullanılan veriler, önyargıları ve adaletsizlikleri içerebilir. Örneğin; bir algoritma, belirli bir etnik grupla ilgili önyargılı verilere dayanarak adaletsiz kararlar verebilir. Bu durum, algoritmaların tasarım ve uygulamasında adilliği sağlama zorunluluğunu gündeme getirmektedir.

Veri Güvenliği ve Manipülasyon: Veri bilimindeki gelişmeler, aynı zamanda, veri güvenliği ve manipülasyon konularında da endişeleri artırmıştır. Veri ihlalleri, ‘hack’lemeler ve kimlik hırsızlığı gibi durumlar, bireyler ve kuruluşlar için ciddi riskler oluşturur. Ayrıca, verilerin yanıltıcı bir şekilde manipüle edilmesi, toplumlar ve demokratik süreçler üzerinde zararlı etkiler yaratabilir.

Veri Uzayının Etik ve Sosyal Etkileri ve Veri Uzayının Önemi: Günümüzde, dijitalleşme ve veri tabanlı teknolojiler, yaşamımızın her alanını dönüştürmektedir. Bu gelişmelerin etik ve sosyal etkileri, veri biliminin kapsamlı bir alanını oluşturur. Veri kullanımı ve analizi, bireysel haklar ve toplumsal etkiler bakımından birçok sorunu gündeme getirirken, bu durum aynı zamanda "veri uzayı" adını verdiğimiz konseptin de önemini ortaya koyar.

Veri toplamanın ve analizinin artması, bireylerin ve toplumların gizlilik, ayrımcılık ve bilgi güvenliği gibi konularda karşılaştığı etik ve sosyal sorunlara dikkat çekmektedir. Örneğin, veri toplama ve analizi yoluyla, bireylerin özel yaşamlarına müdahale edilmesi veya hassas bilgilerin kötüye kullanılması gibi durumlar ortaya çıkabilmektedir. Bu durum, verinin etik kullanımına dair tartışmaları da beraberinde getirir.

Öncelikle, veri uzayının tam olarak anlaşılması ve etkin bir şekilde kullanılması, veri analizinin daha doğru ve etkili olmasını sağlar. Ancak, veri uzayının boyutları arttıkça, analiz daha karmaşık hale gelir ve bu durum, yanıltıcı sonuçlara veya hatalı yorumlara yol açabilir. Algoritmik önyargılar bakımından bu husus büyük önem arz ettiğinden, veri bilimcilerin veri uzayını dikkatli bir şekilde ele alması gerekmektedir.

Sonuç olarak, veri alanı ve veri uzayı, etik ve sosyal etkiler bakımından birçok önemli sorunu gündeme getirir. Veri biliminin bu sorunları ele alması ve veri uzayını etkin bir şekilde kullanması hem bireylerin hem de toplumların yararına olacaktır. Veri analizinin etik ve adil bir şekilde yapılması, veri tabanlı teknolojilerin bize sunduğu fırsatları en iyi şekilde değerlendirmemizi sağlar.

7.4 Yapay Zeka İyi Uygulama Örnekleri

Son olarak, örnek olması ve ilham vermesi açısından Dünyada kamu yararına yapılan yapay zeka iyi uygulama örnekleri aşağıda verilmiştir.

Veri analizi ve makine öğrenmesi araçlarını kullanarak devlet sektöründe birçok uygulama yapılmıştır. Bu uygulamalar sayesinde toplumsal sorunlara etkin çözümler bulunabilmekte, aynı zamanda kaynak tasarrufu sağlanabilmektedir.

Yapay zeka, iklim değişikliğini durdurmaktan vahşi hayatı korumak ve engellilerin hayatını kolaylaştırmaya kadar onlarca alanda kullanılabilir. Yapay Zeka birçok toplumsal soruna farklı bir açıdan bakmamızı sağlayabilir.

ABD merkezli Forbes dergisi de yapay zekanın faydalı amaçlar için kullanılabileceği 10 alanı aşağıdaki gibi özetlemiştir.[79]

1. **Kanser Taraması**

Derin öğrenme algoritmaları ile donanmış yapay zeka çoktandır sağlık hizmetlerine kullanılıyor. Özellikle yapay zekanın görüntüleme yeteneği, kanser tanımlaması ve taramasında umut verici sonuçlar alıyor. New York'taki Mount Sinai Üniversitesi'nden bilim insanları, karaciğer, prostat ve bağırsak kanseri hastalıklarını yüzde 94 doğrulukla önceden haber verebilen derin öğrenme temelli yapay zeka algoritmalarını kullanmayı başardı.

2. **Arıları Kurtarmak**

Dünya Arı Projesi arıları kurtarmak için yapay zekadan yararlanıyor. Dünyadaki arı nüfusu azalıyor ve bu da gezegenimiz için kötü bir haber. Oracle ile işbirliği yapan Dünya Arı Projesi, arıların hayatta kalması ve gelimesine yardımcı olmayı öğrenmek için mikrofonlar, kovanlara konulan kameralar ve nesnelerin interneti sensörlerinden sağlanan verilerden yararlanıyor. Bir buluta aktarılan verilerdeki örüntüler ve eğilimler, arıların hayatta kalmasına erken safhada yardımcı olabilecek şekilde yapay zeka tarafından analiz ediliyor.

3. **Engelli İnsanlar İçin Araçlar**

Yapay zekanın faydalı amaçlarla kullanımına bir örnek de engelli kişilerin engellerinin üstesinden gelemeye yardımcı olmak.

Huawei yapay zekayı kullanarak sağır çocukların okumayı öğrenmesine yardımcı olmak için ücretsiz bir akıllı telefon uygulaması geliştirdi. StorySign adlı uygulama yazıyı işaret diline çevirerek sağır çocukların okumayı öğrenmesine fayda sağlıyor.

Huawei ayrıca Track.Ai adını verdiği, kullanımı kolay ve ucuz cihazla, çocuklardaki göz bozukluklarını tanımlayarak bu hastalıkların körlüğe yol açmasından önce tedavi edilebilmesini sağlıyor.

[79] https://www.indyturk.com/node/200346/bilim/yapay-zekan%C4%B1n-iyi-ama%C3%A7l%C4%B1-kullan%C4%B1m%C4%B1na-10-%C3%B6rnek

4. İklim Değişikliği

Dünyanın şu andaki en büyük sorunlarından biri de iklim değişikliği. Yapay zeka yardımıyla bu sorunun çözümünde çok büyük ilerleme kaydedilebilir.

Makine öğrenimi, iklim enformasyonlarını geliştirebilir. Hükümetlerarası İklim Değişikliği Paneli'nin kullandığı makine öğrenimi algoritmaları yaklaşık 30 iklim modelini çalıştırabiliyor.

Yapay zeka aynı zamanda iklim değişikliğinin farklı bölgelerdeki sonuçlarını tahmin etme ve öğretmeye de yardımcı olabilir. Montreal Öğrenme Algoritmaları Enstitüsü'nden araştırmacılar yapay zekayı şiddetli fırtınalar ve yükselen deniz seviyelerinin verdiği zararı canlandırmada kullanıyor.

5. Vahşi Yaşamı Koruma

Yapay zekanın iyi amaçlı kullanımına bir örnek de vahşi yaşamın korunması alanında kullanılan teknolojiler. Yapay zeka yeterli mali destek alamayan doğa koruyucularına verileri ucuza analiz etme imkanı tanıyor.

Hawaii'deki Kauai Nesli Tehlike Altındaki Deniz Kuşlarını Kurtarma Projesi, deniz kuşları ve elektrik hatları arasındaki çarpışmaları tespit etmek için, 600 saatlik ses kayıtlarını analiz ederken yapay zekadan yararlandı.

Wild Me ve Microsoft'un yapay zekasıysa insanların internete koyduğu fotoğraflardaki neslli tükenme tehdidi altındaki hayvanları tanıyıp kayda geçirebiliyor ayrıca takip edebiliyor.

6. Açlıkla Savaşmak

Yapay zeka, en iyi mahsulü almak, tohum geliştirmekve yabani otların kimysal maddeyle öldürülmesinin düzgüncee uygulanmasını sağlamak için milyonlarca veriyi analiz edebilir.

Bu alanda kullanılan çok sayıda uygulama bulunuyor. Beslenme Erken Uyarı Sistemi adlı sistemse mahsul alınmaması, yükselen gıda fiyatları ve kuraklık nedeniyle farklı bölgelerdeki gıda sayısındaki azalma riskini büyük veriler ve makine öğrenimi sayesinde tespit ediyor.

7. Yoksulluğu ve Eşitsizliği Azaltmak

Yapay zeka eşitsizlikleri azaltmada da yardım sunabilir. Chicago Üniversitesi'nin Veri Bilimi ve Kamu Politikası Merkezi'nin Aequitas projesi ve IBM'in Adalet 360 adlı yapay zekası, önyargıları takip edip düzeltmek için açık kaynaklı yazılımlar sunuyor.

Akıllı yazı editörü Textio ise iş tanımlarını daha kapsayıcı yapıyor. Örneğin bu editör, bir yayınevi şirketinin işe aldığı kadın personelin sayısını bir önceki alıma göre yüzde 10 artırdı.

Standford Üniversitesi'nin bir projesindeyse yapay zeka, farklı bölgelerdeki yoksulluğu ölçmek için uydu fotoğraflarını analiz ediyor. Böylece ekonomik yardımın yapılacağı yerler arasında öncelikler belirlenebilir.

8. Sahte Haberleri Tespit Etmek

Yapay zeka, kitlelere sahte haberleri yayabileceği gibi, Google, Microsoft ve bazı yerel hareketlerin yaptığı gibi bu haberlerdeki gerçeği değerlendirmek için de kullanılabilir.

Trilyonlarca paylaşımı izlemesi gereken Facebook sahte haber göstergesi olan kelime ve örüntüleri bulmak için yapay zekadan yararlanıyor.

9. Tıbbi Görüntüleme

Almanya merkezli Siemens Healthineers adlı tıbbi teknoloji şirketi yapay zekayı bu alanda kullanan şirketlerden biri. Şirketin AI-Rad Companion.4 adlı teknolojisi bir radyolog asistanı.

Rutin olarak tıbbi görüntülemeler yapan yapay zeka personelin de iş yükünü hafifletiyor

10. Yenilemeleri Geliştirmek

Güney Kaliforniya Üniversitesi'ndeki Artificial Intelligence in Society (CAIS) Merkezi'nde de yapay zeka bir deprem anında Los Angeles kentinde su dağıtımının nasıl yapılacağını çözmekle görevlendirildi.

Zira kentin altyapısı yaşlanıyor. Projeyle bu kritik anda boru hatları yenilenmesi gereken stratejik bölgelerin belirlenmesi amaçlanıyor.

8 Sağlık Alanında Veri Uzayı Uygulaması

Sağlık alanında veri birçok boyutu ile sağlık sistemlerini etkileyen son derece önemli bir role sahiptir. Bu verinin sayısal ortamda olması ve bilgisayar sistemleri tarafından yönetilmesi ve anlamlandırılmasıyla, verinin sağlık sistemlerine olan etkileri çok daha büyük bir önem kazanmaktadır. Ancak günümüzde, bilgisayar ve teknoloji alanındaki gelişmeler ve sağlık sistemlerinin kendisine özgü gereksinimleri nedeniyle bu etkileri en üst seviyeye çekebilmek için hem teknolojik gelişmeleri hem de sağlık sistemlerine özgü gereksinimleri çok iyi anlamak gerekmektedir. Bu bölümde, verinin sağlık alanındaki önemi, sağlık sistemlerine muhtemel etkileri ve bu veri uzayında sağlık sektöründeki verimliliği artırmak amacıyla yapılması gerekenler irdelenerek sağlık sektöründe veri uzayı çalışmaları tüm boyutları ile incelenmektedir.

8.1 Veri Uzayı Sektörel Uygulamaları

Sağlık sistemleri hata toleransı olmayan ve insan sağlığını doğrudan etkileyen bir özelliğe sahip olması nedeniyle, kendisine özgü standartlara ve regülasyonlara sahiptir. Günümüzde nüfus artışları ile birlikte sağlık hizmeti sayısında da hızlı bir artış olmaktadır. Dolayısıyla, mevcut sağlık sistemleri tarafından büyük hacimli yapılandırılmış ya da yapılandırılmamış çeşitlilikte ve farklı standartlar ile desteklenen yoğun bir veri üretimi söz konusudur. Bu veri uzayını yönetmek, analiz etmek ve özümsemek, doğru araçlar ve yöntemler ile anlamlandırmak sağlık sistemleri ve hizmetleri kalitesi açısından son derece önemlidir. Bu durum sağlık verilerini daha iyi anlamayı ve anlamlandırmayı gerekli kılar. Sağlık verileri çeşitlilik içermektedir. Sağlık veri uzayı kapsamında üretilen farklı veri yapıları ve uygulamalar aşağıdaki gibi özetlenebilir.

8.1.1 Elektronik Sağlık Verileri

1990'larda ABD'de kurumlar arası, kapsamlı ve hasta merkezli bir sağlık kaydı kavramı ile ortaya atılmış olan elektronik sağlık kayıtları - ESK (*Electronic Health Records-EHRs*) fikri hastanın sağlık geçmişinin sürekli olarak kayıt altına alınması ve erişilebilir olması, hasta sağlık hizmetlerinin desteklenmesi ve kalitesinin korunması ve iyileştirilmesini hedeflemektedir.[80] 1990'larda başlayan bu ilk ESK kavramlarından bu yana, bu kayıtların içeriği, yapısı ve teknolojisi ciddi değişimlere ve gelişimlere uğramıştır. Günümüzde ESK, bir hastanın sağlık ve sağlık hizmeti verilerinin kapsamlı, kurumlar arası ve boylamsal olarak toplanması kavramını tanımlar. Bu nedenle ESK, bir hastanın herhangi bir tıbbi tedavisine özgü olarak değil, hastanın genel olarak sağlığıyla da ilgili verileri içerir. Maliyet, sağlık hizmetlerinde her zamankinden daha fazla kritik bir faktör haline gelmesi nedeniyle ESK sistemlerinin geliştirilmesi daha da önemli bir hale gelmektedir. ESK sistemleri ayrıca sağlık alanında ilgili kişi ve kurumların teknik ve aynı zamanda anlamsal düzeyde sınır ötesi birlikte çalışabilirlik olanağı sunmaktadır. Ancak bu hedeflere ulaşılabilmesi için ESK sistemlerinin belirli standartları desteklemesi ve belirli bir kalite seviyesinde hazırlanması gerekmektedir. Bu amaçla, Ulusal Sağlık Bilgi Altyapısı'nın (*National Health Information Infrastructure-NHII*) ve destekleyici veri standartlarının oluşturulmasına yönelik birçok çaba yürütülmektedir.[81] Bu veri

[80] Waegemann CP. Status Report 2002: Electronic Health Records. Medical Records Institute; 2002.
[81] Zerhouni EA. Keynote Presentation. Paper presented at: Proc AMIA Symp 2005: October 23, 2005; Washington, D.C.

standartları, gerek klinik araştırmaların yapılması gerekse dünya genelinde hastalıkların aynı dil ile izlenmesi ve tanımlanması konularında son derece önemlidir.

Veri standartları, farklı kaynaklardan veya biçimlerden gelen verilerin temsili için mutabakata dayalı özellikler olarak tanımlanmaktadır. Bu standartlar verilerin paylaşımı, taşınabilirliği ve yeniden kullanılabilirliği için gerekli ve önemlidir.[82] Standartlaştırılmış veri kavramı, bu alanlardaki verileri kodlayan hem veri alanları (üst veri) hem de değer kümeleri için belirtimleri içerir. Standartlar veri paylaşımı, taşınabilirliği ve yeniden kullanılabilirliği için son derece önemlidir.[83]

Uygulamalı kullanımları destekleyen klinik araştırma veri standartlarına doğru ilerlemek amacıyla Klinik Veri Standartları Değişim Konsorsiyumu (*Clinical Data Interchange Standards Consortium-CDISC*) ve Düzenlenmiş Klinik Araştırma Bilgi Yönetimi (Regulated Clinical Research Information Management-*RCRIM*) Yedinci Sağlık Seviyesi Teknik Komitesi'dir (*Health Level Seven-HL7*) gibi birçok grup tarafından çalışmalar yürütülmektedir. CDISC üyeliği, ağırlıklı olarak dünya çapındaki büyük ilaç şirketlerinden gelirken, FDA (*The Food and Drug Administration*) 'nın yanı sıra Ulusal Kanser Enstitüsü (*National Cancer Institute*- NCI) gibi devlet kurumlarının temsilcilerini de içerir. CDISC'nin öncelikli hedefi, düzenleyici sunumlar için standart veri modelleri oluşturmaktır.

HL7 ise, kendini tüm sağlık ortamlarında klinik ve idari veriler için standartlar üretmeye adamış, kâr amacı gütmeyen bir gönüllü kuruluştur ve bir Amerikan Ulusal Standartlar Enstitüsü (American National Standards Institute-ANSI), Akredite Standartlar Geliştirme Kuruluşu (Standards Development Organizations-SDO)'dur.[84] ANSI tarafından akredite edilmiş tüm SDO'lar gibi, HL7 de fikir birliği, açıklık ve çıkar dengesi sağlayan katı ve iyi tanımlanmış bir dizi işletim prosedürüne bağlıdır. RCRIM Teknik Komitesi, CDISC ile aynı hedeflerin bazılarını paylaşır, ancak aynı zamanda daha geniş klinik araştırma ve hasta güvenliği çıkarlarını da temsil eder. HL7 boyunca gelişen standartların resmi ve gerekli tartışması ve onayı, teknik komitelerde ve RCRIM gibi özel ilgi gruplarında tanımlanan standartların diğer sağlık

[82] Chalmers RJG. Editorial. Health care terminology for the electronic era. Mayo Clinic Proc 2006;81:619–624 5. Dudeck J. Aspects of implementing and harmonizing healthcare communication standards. Int J Med lnform 1998;48:163–71.
American Medical Informatics Association and American Health Information Management Association Terminology and Classification Policy Task Force. Healthcare Terminologies and Classifications: An Action Agenda for the United States: AMIA; 2006. Available at: http://www.amia.org/inside/initiatives/docs/terminologiesandclassifications.pdf.
IOM. To Err is Human: Building a Safer Health System. Washington, D.C.: Institute of Medicine; National Academy of Sciences; November 1999. Available at: http://www.iom.edu/ CMS/8089/5575.aspx.

[83] Chalmers RJG. Editorial. Health care terminology for the electronic era. Mayo Clinic Proc 2006;81:619–624
Dudeck J. Aspects of implementing and harmonizing healthcare communication standards. Int J Med lnform 1998;48:163–71.
American Medical Informatics Association and American Health Information Management Association Terminology and Classification Policy Task Force. Healthcare Terminologies and Classifications: An Action Agenda for the United States: AMIA; 2006. Available at: http://www.amia.org/inside/initiatives/docs/terminologiesandclassifications.pdf.
IOM. To Err is Human: Building a Safer Health System. Washington, D.C.: Institute of Medicine; National Academy of Sciences; November 1999. Available at: http://www.iom.edu/ CMS/8089/5575.aspx. Accessed October 12, 2007.

[84] Health Level Seven. Vol 2005: Health Level Seven, Inc.; 2005. Available at http://www.hl7.org/

hizmetleri alanlarında ortaya çıkan mesajlaşma standartlarıyla birlikte çalışabilir veya uyumlu olma olasılığını artırır. Ancak HL7'nin mevcut (2.x) sürümleri, klinik ortamlarda mesajlaşmayı desteklemek için nispeten basit modeller kullansa da, HL7 sürüm 3 halen yaygın olarak uygulanmamaktadır.

8.1.2 Genomik Veriler

30.000 ila 35.000 geni kapsayan insan genomunun dizileme maliyeti, yüksek verimli dizileme teknolojisinin gelişmesiyle birlikte hızla azalmaktadır.[85] Bu durum, mevcut halk sağlığı politikalarının iyileştirilmesi ve daha iyi bir hasta bakım servisinin sunulması amacıyla eylemlerin hayata geçirilmesi konularında genom ölçeğindeki verilerin analizini ön plana çıkartmaktadır.[86] Ancak bu tür önerilerin sunulması amacıyla düşük maliyetlerde ve hızlı klinik çözümlerin geliştirilmesi gerekmektedir. Bu karmaşık sorunu ele alan girişimler arasında, P4 tıp paradigması[87] (i) hastalık durumlarını belirlemek için genom ölçekli veri kümelerini analiz etmek, (ii) bir deneğin sürekli izlenmesi için kana dayalı teşhis araçlarına doğru ilerlemek, (iii) ilaç hedefi keşfine yönelik yeni yaklaşımlar keşfetmek, yakalama, doğrulama, depolama, madencilik, bütünleştirme ve son olarak (iv) her birey için veri modelleme gibi büyük veri zorluklarıyla başa çıkmak için araçlar geliştirilmesini destekleyici çalışmalar yürütmektedir. Ancak, klinik düzeyde eyleme geçirilebilir önerileri gerçekleştirmek, bu alan için büyük bir zorluk olmaya devam etmektedir.[88]

8.1.3 Görüntüye Dayalı Veriler

Tıbbi görüntüleme anatomi hakkında önemli bilgiler sunar ve organların fonksiyonlarını tespit etmenin yanı sıra hastalık tespiti ve tedavisi süreçlerini destekler. Yapılan çalışmalar, tıbbi görüntülerin çeşitli hastalıkların tanı, tedavi değerlendirmesi ve planlama aşamaları için önemli bir kaynak olduğunu göstermektedir.[89] Bu nedenle farklı tıbbi alanlarda Bilgisayarlı Tomografi-BT (Computed tomography-CT), Manyetik Rezonans Görüntüleme (MRG), X-ışını, moleküler görüntüleme, ultrason, fotoakustik görüntüleme, floroskopi, Pozitron Emisyonu Tomografi (Positron Emission Tomography (PET), Single-Photon Emission Computed Tomography (SPECT) ve Mamografi gibi birçok tıbbi görüntüle tekniği kullanılmaktadır. Günümüzde tüm bu

[85] E. S. Lander, L. M. Linton, B. Birren et al., “Initial sequencing and analysis of the human genome,” Nature, vol. 409, no. 6822, pp. 860–921, 2001.
R. Drmanac, A. B. Sparks, M. J. Callow et al., “Human genome sequencing using unchained base reads on self-assembling DNA nanoarrays,” Science, vol. 327, no. 5961, pp. 78–81, 2010.
[86] T. Caulfield, J. Evans, A.McGuire et al., “Reflections on the cost of ‘Low-Cost’ whole genome sequencing: framing the health policy debate,” PLoS Biology, vol. 11, no. 11, Article ID e1001699, 2013.
F. E. Dewey, M. E. Grove, C. Pan et al., “Clinical interpretation and implications of whole-genome sequencing,” JAMA, vol. 311, no. 10, pp. 1035–1045, 2014.
[87] L. Hood and S. H. Friend, “Predictive, personalized, preventive, participatory (P4) cancer medicine,” Nature Reviews Clinical Oncology, vol. 8, no. 3, pp. 184–187, 2011.
L. Hood and M. Flores, “A personal view on systems medicine and the emergence of proactive P4 medicine: predictive, preventive, personalized and participatory,” New Biotechnology, vol. 29, no. 6, pp. 613–624, 2012.
L. Hood and N. D. Price, “Demystifying disease, democratizing health care,” Science Translational Medicine, vol. 6, no. 225, Article ID 225ed5, 2014.
[88] G. H. Fernald, E. Capriotti, R. Daneshjou, K. J. Karczewski, and R. B. Altman, “Bioinformatics challenges for personalized medicine,” Bioinformatics, vol. 27, no. 13, Article ID btr295, pp. 1741–1748, 2011.
P. Khatri, M. Sirota, and A. J. Butte, “Ten years of pathway analysis: current approaches and outstanding challenges,” PLoS Computational Biology, vol. 8, no. 2, Article ID e1002375, 2012.
[89] F. Ritter, T. Blomkamp, A. Homeyer et al., “Medical image analysis,” IEEE Pulse, vol. 2, no. 6, pp. 60–70, 2011.

verilerin elektronik ortamda tanımlanması ve saklanması mümkün olmaktadır. Bu görüntüler üzerinde uygulanan görüntü işleme, makine öğrenmesi gibi yöntemleri ile alan uzmanlarının akciğer tümörleri, spiral deformasyon teşhisi, arter stenosu tespiti ve anevrizma tespiti gibi hastalıkların teşhis ve tedavi süreçlerinde desteklenmesi mümkün olur. Ayrıca, bu veriler kullanılarak 3B sayısal organ modellerinin oluşturulması sayesinde teşhis ve tedavi süreçlerinin desteklenmesi amacıyla detaylı verilerin sunulması, tıp fakültelerinin eğitim programları için teknoloji destekli simülasyona dayalı eğitim modellerinin sunulması, ameliyat öncesi planlama destek sistemlerinin hazırlanması gibi birçok destek sisteminin geliştirilmesi mümkün olur. Tüm bu farklı veri yapılarının bütünleşik olarak incelenmesinin önemi ve katkıları da yadsınamaz. Örneğin ESK ya da Genomik veriler gibi diğer veri türleri ile entegrasyonu analizlerin doğruluk seviyesini ayrıca artırmakta ve bir işlem için harcanan süreyi azaltmaktadır. Ancak bu tıbbi görüntü verileri tek bir veri için birkaç megabayttan çok daha büyük boyutlara kadar yer tutabilmektedir. Dolayısıyla bu tür verilerin, uzun süre saklanması büyük depolama kapasitelerini gerekli kılar. Ayrıca bu hedeflere ulaşabilmek için bu verinin uygun veri modelleri ile hazırlanması ve saklanması, uygun hesaplama yöntemleri ve modelleri ile analiz edilerek uygun platformlarda uygun ara-yüz modelleri ile alan uzmanlarına sunulması gerekmektedir. Dolayısıyla, bu süreçte verinin bilgisayar ortamında hazırlanması, modellenmesi, farklı veri yapıları ile eşleştirilmesi (entegrasyonu), analizi ve kullanıcıya sunulması aşamaları ciddi bir önem kazanmaktadır ve birçok zorluğu da içermektedir. Bu süreçte çözümlenmesi gereken birçok teknik problem ile karşılaşılır. Örneğin, büyük kapasitedeki bu tür veriler kullanılarak herhangi bir karara yardımcı otomasyon sistemlerinin geliştirilmesi için hızlı ve doğru algoritmaların kullanılması gerekmektedir. Ayrıca, bu sistemlerin başarı oranlarının artırılması için her hasta için elde edilen diğer veri kaynaklarından da yararlanılması gerekir ki, bu durumda uyumlu veri modelleri ile verilerin depolaması ve geniş veri yelpazesini kapsayabilen verimli yöntemlerin geliştirilmesi önemli bir sorun olarak karşımıza çıkmaktadır.

Özet olarak bilgisayar sistemleri, BT, MRG, SPECT, PET gibi karmaşık yöntemler kullanan görüntüleme cihazlarından elde edilen sağlık ile ilgili görüntülemeye dayalı bu veriler sadece depolamak veya görüntülemek için değil, aynı zamanda girdi dizilerinden görüntüler veya 3B modeller oluşturmak için de kullanılmaktadır. Dolayısıyla, tıbbi cihazlar arasında bağlantı ve bilgi alışverişinin sağlıklı bir şekilde yürütülmesi için bir standardın geliştirilmesi ve kullanılması da bu alanın önemli bir gereksinim olarak ortaya çıkmaktadır. Farklı yaklaşımlarla tıbbi görüntüleme ekipmanı yapan birçok üretici olması nedeniyle, kullanılan standartlar tıbbi görüntülerin ve verilerin alışverişini daha kolay hale getirmektedir. Bu kapsamda, DICOM (Digital Imaging and Communication in Medicine), tescilli olmayan bir veri değişim protokolünü belirten bir standarttır. Mevcut sürüm (3.0), Ulusal Elektrik Üreticileri Derneği (National Electrical Manufacturers Association- NEMA) tarafından 1993 yılında yayınlanmıştır. Bu standart, her yıl çalışma grupları tarafından hemen hemen her tıbbi branşı tatmin edecek şekilde geliştirilmektedir. Günümüzde DICOM, Tıbbi Görüntü Arşivleme ve İletişim Sistemleri (picture archiving and communication system-PACS) için bir temel oluşturarak, etkili tıbbi görüntüleme depolamasına ve farklı coğrafi alanlara aktarımına izin vermektedir.[90] DICOM

[90] Digital Imaging and Communications in Medicine (DICOM), NEMA Publications, "DICOM strategic document", Ver. 8.0, April 2008, available at: http://medical.nema.org/dicom/geninfo/Strategy.pdf
P. Mildenberger, M. Eichelberg, E. Martin "Introduction to the DICOM standard", European Radiology, Vol. 12, No. 4, April 2002, pp. 920-927

Standardı tıbbi verilerin nasıl görüntüleneceğini ya da bu verilerin nasıl açıklanacağı ile ilgili bilgileri tanımlamaz. Görüntü verilerinin yanı sıra DICOM, görüntü için önemli olan veri yapılarını da içerir. Bu yapılar, nesnenin tanımı, hasta verileri, kurum adı ve gerçekleştirilen işlemler veya raporlar gibi diğer bilgileri içeren bir başlığa yerleştirilir. DICOM, en iddialı tıbbi görüntü standartlarından biridir. Görüntü verilerini standart hale getirmek ve farklı üreticilerin ekipmanları arasında kolayca paylaşmak için geliştirilmiştir. Standardı geliştirmek için toplanan birçok çalışma grubu, her çalışma grubunun standardın yalnızca küçük bir uzmanlaşmış bölümünü geliştireceği şekilde bölünmüştür. Bu organizasyon yapısı çok verimlidir çünkü her çalışma grubu, aralarında mümkün olduğunca az örtüşme olacak şekilde farklı alanlardan sorumludur. DICOM Standardı, sürekli gelişen bazı parçaların daha fazla genişletilmesini ve kolayca yükseltilmesini mümkün kılmak için geliştirilmiştir, çünkü günümüzde tıbbi görüntüleme cihazları kadar görüntüleme standartları da çok hızlı gelişmektedir.

8.1.4 Sinyale Dayalı Veriler

Günümüzde sağlık sistemleri, açık olaylar durumunda uyarı mekanizmaları sağlamak için tekil fizyolojik dalga biçimi verilerini veya ayrık hayati bilgileri kullanan çok sayıda farklı ve sürekli izleme cihazı kullanmaktadır. Tıbbi sinyaller özellikle her hastaya bağlı çok sayıda monitörden sürekli ve yüksek çözünürlüklü olarak elde edilmektedir. Bu durum tıbbi görüntülerde olduğu gibi verinin elde edilmesi ve depolanması aşamalarında hacim ve hız problemlerine neden olmaktadır. Bununla birlikte, bu yüksek yoğunluktaki verinin anlamlandırılması ve bu verilere dayalı alarm sistemlerinin geliştirilmesi bu tür bileşik bir yapıya sahip olmayan veri yapılarında verinin doğrulanması ve anlamlandırılması kapsamında ciddi problemlerin yaşanmasına neden olmaktadır. Bu tür verilerin insan gözü ile anlık analizi ve takibi de her zaman çok kolay olamamakta ve farklı sistemlerden gelen uyarılar bir alarm yoğunluğuna neden olmaktadır.[91] Fizyolojik sinyaller ayrıca uzay-zamansal nitelikte bir karmaşıklık içermektedir.

Bu veriler üzerinde geliştirilecek olan sistemlerin geniş ve kapsamlı bir bakış açısıyla hastaların gerçek fizyolojik koşulları bağlamında farklı bilgi kaynakları ile doğrulanmış verileri kullanması, daha doğru ve yüksek seviyeli destek sistemlerinin geliştirilmesi için gerekli bir koşuldur. Bu nedenle, multimodal klinik zaman serisi verileri arasındaki etkileşimleri ve korelasyonları incelemeye yönelik gelişmiş ve daha kapsamlı yaklaşımların geliştirilmesi gerekmektedir. Bu tür analizler, insan gözü ile ikiden fazla sinyali etkileyen verilerin analizlerinin zorluğu nedeniyle[92] tıbbi süreçlerin desteklenmesi açısından son derece önemlidir.

W.D. Bidgood, Jr., S.C. Horii, F.W. Prior, D.E. Van Syckle, "Understanding and Using DICOM, the Dana Interchange Standard for Biomedical Imaging", Journal of the American Medical Informatics Association, Vol. 4, No. 3, May 1997, pp. 199-212

[91] B. J. Drew, P. Harris, J. K. Z`egre-Hemsey et al., “Insights into the problem of alarm fatigue with physiologic monitor devices: a comprehensive observational study of consecutive intensive care unit patients,” PLoS ONE, vol. 9, no. 10, Article IDe110274, 2014.
K. C. GrahamandM. Cvach, “Monitor alarmfatigue: standardizing use of physiological monitors and decreasing nuisance alarms,”The American Journal of Critical Care, vol. 19, no. 1, pp. 28–34, 2010.
M. Cvach, “Monitor alarm fatigue: an integrative review,” Biomedical Instrumentation & Technology, vol. 46, no. 4, pp. 268–277, 2012.

[92] J. M. Rothschild, C. P. Landrigan, J. W. Cronin et al., “The Critical Care Safety Study: the incidence and nature of adverse events and serious medical errors in intensive care,” Critical Care Medicine, vol. 33, no. 8, pp. 1694–1700, 2005.

8.2 İşletim Ortamı ve Uygulama Modeli

Sağlık veri uzayının kendisine özgü veri yapıları, gereksinimleri ve standartları konusunda yapılan çalışmalar yukarıda genel olarak özetlendi. Halen birçok organizasyon tarafından çözülmeye çalışılan sağlık veri uzayı ve veri yapıları ile ilgili sorunlar, uygulama ortamları ve farklı uygulama modelleri kapsamında değerlendirildiğinde çözülmesi gereken yeni sorunları da gündeme getirmektedir. Bu sorunlar aşağıdaki başlıklar altında incelenebilir.

8.2.1 Veri Güvenliği

Sağlık verilerinin elektronik ortamda saklanması ve ilgili kişiler tarafından erişimin sağlanması genel olarak veri güvenliği[93], iletişim ve taşıma güvenliği[94] ve sistem güvenliği[95], veri depolama güvenliği[96] gibi farklı seviyelerde güvenlik gereksinimlerinin karşılanmasını gerekli kılmaktadır.

P. Carayon and A. P. G¨urses, “A human factors engineering conceptual framework of nursing workload and patient safety in intensive care units,” Intensive and Critical Care Nursing, vol. 21, no. 5, pp. 284–301, 2005.
P.Carayon, “Human factors of complex sociotechnical systems,” Applied Ergonomics, vol. 37, no. 4, pp. 525–535, 2006.

[93] Ball M, Smith C, Bakalar RS. Personal Health Records: Empowering Consumers. Journal of Healthcare Information Management 2006; 21 (1): 76–86.
Agrawal R, Johnson C. Securing electronic health records without impeding the flow of information. Int J Med Inform 2007; 76 (5–6): 471–479.
Beun JG. Electronic healthcare record; a way to empower the patient. Int J Med Inform 2003; 69 (2–3): 191.
Birkmann C, Dumitru RC, Prokosch H-U. Evaluation of Health-related Internet Use in Germany. Methods Inf Med 2006; 45 (4): 367–376.
Winkelman WJ, Leonard KJ. Overcoming Structural Constraints to Patient Utilization of Electronic Medical Records: A Critical Review and Proposal for an Evaluation Framework. J Am Med Inform Assoc 2004; 11 (2): 151–61.

[94] Blobel B. Comparing approaches for advanced e-health security infrastructures. Int J Med Inform 2007; 76 (5–6): 454–459.
Spidlen J, Hanzlicek P, Riha A, Zvarova J. Flexible information storage in MUDRII EHR. Int J Med Inform 2006; 75 (3–4): 201.
Wozak F, Schabetsberger T, Ammmenwerth E. End-to-end Security in Telemedical Networks – A Practical Guideline. Int J Med Inform 2007; 76 (5–6): 484–490.

[95] Iakovidis I. Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe. Int J Med Inform 1998; 52 (1–3): 105–115.
Ishikawa K, Ohmichi H, Umesato Y, Terasaki H, Tsukuma H, Iwata N, et al. The guideline of the personal health data structure to secure safety healthcare: The balance between use and protection to satisfy the patient’needs. Int J Med Inform 2007; 76 (5–6): 412–418.
Hammond WE. Making the boundaries clearer: revisiting information systems with fading boundaries. Int J Med Inform 2003; 69 (2–3): 99–104.
Hasselbring W, Reussner R. Toward trustworthy software systems. Computer 2006; 39 (4): 91–92.
Hanmer L. Criteria for the evaluation of district health information systems. Int J Med Inform 1999; 56 (1–3): 161.
Humphreys BL. Electronic Health Record Meets Digital Library: A New Environment for Achieving an Old Goal. J Am Med Inform Assoc 2000; 7 (5): 444–552.

[96] Ueckert F, Goerz M, Ataian M, Tessmann S, Prokosch H-U. Empowerment of patients and communication with health care professionals through an electronic health record. Int J Med Inform 2003; 70 (2–3): 99.
de Meyer F, Lundgren P-A, de Moor G, Fiers T. Determination of user requirements for the secure communication of electronic medical record information. Int J Med Inform 1998; 49 (1): 125.
Agrawal R, Grandison T, Johnson C, Kiernan J. Enabling the 21st Century Health Care Information Technology Revolution. Communications of the ACM 2007; 50 (2): 35–42.

Bu durum farklı güvenlik hizmetlerinin uygulanmasını[97] ve güvenlik politikalarının[98] tanımlanmasını gerektirmektedir. Dolayısıyla veriye kimin, ne zaman, hangi amaçla ve hangi koşullarda erişimin sağlandığı bilinmelidir.

Veri güvenliği noktasında sağlık verilerinin gerek Türk hukukunda gerekse uluslararası düzenlemelerde hassas ya da özel nitelikli kişisel veri olarak kabul edildikleri de eklenmelidir. Genelde, hassas/ özel nitelikli kişisel verilerin, özelde ise bunlar arasında yer alan sağlık alanındaki kişisel verilerin işlenmesi konusunda ise hukuken ortaya çıkan durum şöyledir:

GDPR "Özel Kategorilerdeki Kişisel Veriler"; KVKKn ise "Özel Nitelikli Kişisel Veriler" ibaresini tercih etmektedir.

Bununla ilgili GDPR md. 9 ve KVKKn md. 6 birlikte değerlendirildiğinde, kişisel veriler açısından, GDPR ve KVKKn hükümlerindeki özel nitelikli kişisel verilerin tek tek sayıldığı görülmektedir. Ancak iki düzenlemede birebir aynı tür veriler özel nitelikli kişisel veri olarak kabul edilmemiştir.

GDPR md. 9 ile sayılan özel kategorilerdeki kişisel veriler "*ırk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile biyometrik verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin veriler*"dir.

KVKKn md. 6 ile kabul edilenler "*kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri*"dir.

Ayrıca genetik veriler, biyometrik veriler, sağlık ile ilgili veriler veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin veriler için bunların "*bir gerçek kişinin kimlik teşhisinin yapılması amacıyla*" işlenmesi gerekmektedir. KVKKn md. 6'da ise böyle bir şart bulunmamaktadır.

Diğer yandan her iki düzenlemede de özel nitelikteki kişisel veriler için özel nitelikte olmayanlardan farklı işleme nedenleri ve koşulları öngörülmüştür. Bunların tümüne çalışma kapsamında girilmeyecek olmakla birlikte bilhassa kamu kurumları açısından önem taşıyabilecek olanlara değinilecektir.

[97] Blobel B. Comparing approaches for advanced e-health security infrastructures. Int J Med Inform 2007; 76 (5–6): 454–459.
Blobel B. Advanced EHR Architectures – Promises or Reality. Methods Inf Med 2006; 45: 95–101.
[98] Saastamoinen H. Exception-Based Approach for Information Systems Evaluation: The Method and its Benefits to Information Systems Management. The Electronic Journal of Information Systems Evaluation 2004; 8 (1): 51–60.
Kim MI, Johnson KB. Personal Health Records: Evaluation of Functionality and Utility. J Am Med Inform Assoc 2002; 9 (2): 171–180.
Egyhazy C, Mukherji R. Interoperability Architecture using RM-ODP. Communications of the ACM 2004; 47 (2): 93–97.
Hristidis V, Clarke PJ, Prabakar N, Deng Y, White JA, Burke RP. A Flexible Approach for Electronic Medical Records Exchange. International workshop on Healthcare information and knowledge management. Virginia 2006. pp 33–40.
Loane M, Wootton R. A review of guidelines and standards for telemedicine. Journal of Telemedicine and Telecare 2002; 8: 63–71.

KVKKn md. 6 ile özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu düzenlenmektedir. Ancak belirli kategoriler ve veri işleyecek kişiler için bir istisna öngörülmüştür. Bu hallerde, ilgilinin açık rızası olmasa da sayılan özel nitelikli kişisel verileri işlenebilecektir.

GDPR ise özel nitelikteki kişisel verilerin işlenmesi yasağını şu hallerde kaldırmaktadır (yukarıda da ifade edildiği üzere, aşağıda, kamu kurumları açısından ilgi kurulabilecek olan nedenlere yer verilmiştir):

1. Veri öznesinin açık rızası,
2. İstihdam ve sosyal güvenlik ve sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve spesifik haklarının kullanılması amacıyla işleme faaliyetinin gerekmesi,
3. Veri öznesinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde, veri öznesi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olması,
4. İşleme faaliyetinin bir vakıf, birlik veya kar amacı gütmeyen başka bir organ tarafından siyasi, felsefi, dini veya sendika amacıyla uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında işlemenin ve yalnızca organın üyeleri veya eski üyeleri ya da amaçlarıyla bağlantılı olarak kendisi ile düzenli olarak temas halinde bulunan kişilerle ilgili olması ve kişisel verilerin veri öznelerinin rızası olmaksızın söz konusu organ dışında açıklanmaması koşuluyla gerçekleştirilmesi,
5. İşleme faaliyetinin veri öznesi tarafından açık bir biçimde kamuya açıklanan kişisel verilerle ilgili olması,
6. Yargılama kapsamında iddiada bulunma ve savunma hakları bağlamında işlenmesi,
7. “Kayda değer ölçüde kamu yararı adına” denilecek nedenlerden ötürü işleme faaliyetinin gerekmesi,
8. Koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, Birlik ya da üye devlet hukukuna dayalı olarak veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca ve mesleki gizlilik kuralları veya yasa hükümlerinin sağladığı güvencelere tabi olarak çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi açısından işleme faaliyetinin gerekli olması,
9. Kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyetinin gerekmesi.

Veri güvenliğinin adımlarından olan, kişisel verilerin hukuka uygun işlenmesi, özellikle sağlık verileri söz konusu olduğunda, GDPR uyarınca yukarıda sayılan işleme nedenlerine dayalı olarak yapılmak durumundadır.

8.2.2 Veri Yapıları ve Veri Entegrasyonu

Yukarıda da anlatıldığı gibi, sağlık sistemleri farklı yoğunluklarda, farklı yapılarda ve farklı modellerde çeşitli verilerin toplanması, biçimlendirilmesi ve anlamlandırılmasını gerekli kılmaktadır. Bu veriler elektronik sağlık kayıtlarında olduğu gibi yapısal veri modelleri ile operasyonel sistemler içinde üretilen veriler olduğu gibi, genomik veriler, görüntüye dayalı veriler, sinyale dayalı veriler gibi zaman boyutunda yoğun veri yapıları ile ve birçok farklı standart ve biçimde farklı sağlık sistemleri tarafından üretilen ve saklanan verileri de içermektedir. Tüm bu verilerin bütünleşik bir bakış açısı ile analizinin sağlık sistemlerine muhtemel katkısı yadsınamaz. Bu şekilde süreçlere dayalı karşılaştırmalı olarak yapılan

analizler, zamana dayalı keşfedilen veri desenleri gibi analizler gerek gelecekte karşılaşılabilecek olası sağlık durumları ile ilgili öngörülerde bulunmayı kolaylaştırabilir, gerekse sağlık sistemlerindeki verimlilik ve performans artışlarına neden olabilir. Ancak sağlık verilerinin bu karmaşık, farklı ve dağınık veri yapıları, beraberinde birçok problemi de getirmektedir ve günümüzde tüm bu verilere bütünleşik olarak bakabilmeyi sağlayan standartlar ya da sistemler henüz geliştirilmemiştir. Dolayısıyla sağlık sistemi veri yapıları, kendisine özgü veri saklama, modelleme ve analiz yöntemlerine ihtiyaç duymaktadır. Bu alanda gerek araştırmacıların gerek bilişim uzmanlarının ve gerekse sağlık sistemlerine çözüm üreten donanım ve yazılım kuruluşlarının sağlık sistemlerine özgü çözümler üretmelerine ve birlikte çalışabilen çözümler geliştirmelerine ihtiyaç vardır.

8.2.3 Veri Analizi

Yukarıda da anlatıldığı üzere, sağlık sistemlerinin veri yapıları kendisine özgü birçok farklı özelliğe sahiptir. Bu verilerin gerek istatistiksel modeller ile gerekse yapay zeka ve büyük veri analizlerine yönelik geliştirilmiş olan algoritmalar kullanılarak analiz yöntemlerinde sağlık sistemlerine özgü yaklaşımlara ihtiyaç vardır. Halen bu verilerin analizinde önemli bir yol kat edilmiş olduğu bilinmektedir. Ancak bu verilere bütünleşik olarak bakabilen ve bütünleşik analiz modelleri geliştiren sistemlerin eksikliği, gelecekte sağlık sistemlerine özgü veri depolama, veri entegrasyonu, veriye ulaşım, veri analizi ve veri görselleme gibi birçok konuda yenilikçi çözümlerin üretileceği öngörülmektedir. Dolayısıyla, sağlık veri uzayının gebe olduğu bu yenilikçi yaklaşımların sağlık sistemlerine önemli kazanımların sağlanmasının mümkün olacağını söylemek yanlış olmayacaktır.

8.2.4 Kısa, Orta, Uzun Dönem Planlar

Sağlık veri uzayının kendisine özgü mevcut modelleri bulunmakla birlikte mevcut sistemlerde yaşanmakta olan ciddi problemleri de bulunmaktadır. Bu problemler içinde teknik problemler kapsamında farklı veri biçimleri, veri yapıları ve veri standartları verinin bütünleştirilmesi (entegrasyonu) ve bütünleşik, öngörüye dayalı veri analizi olanaklarının artırılması kapsamında birçok teknik problemi de beraberinde getirmektedir. Bununla birlikte verinin modelleme yöntemleri, veriye erişim yöntemleri, veri saklama alanı ihtiyaçları, verinin zaman içinde kaybedilmeden saklanması gereksinimleri gibi birçok teknik problem de sağlık sistemlerinde karşımıza çıkmaktadır. Sonuç olarak, tüm bu teknik problemlerin aşılması amacıyla, sağlık sistemlerine özgü daha bütünleşik, performansa dayalı ve yapısal çözümlerin üretilmesine ihtiyaç olduğu belirtilebilir.

Sağlık sistemleri kişiye özgü son derece önemli ve mahremiyet içeren verilerin saklanmasını zorunlu kılmaktadır. Aynı zamanda bu verilerin diğer sistemlerle, uzmanlarla ve kişilerle paylaşımı da bazen son derece önemli ve kritik olabilmektedir. Dolayısıyla bu sistemlere özgü olarak geliştirilecek veri saklama ve paylaşım modelleri konusunda henüz yaygın olarak kullanılan standartların bulunmaması önemli bir hukuki açığı da beraberinde getirmektedir. Veri uzayı kapsamında farklı alanlarda uygulanan güvenlik protokollerinin ötesinde sağlık sistemlerine özgü olarak atılacak olan adımlara ihtiyaç olduğu değerlendirilmektedir.

9 Finans Alanında Veri Uzayı Uygulaması

Günümüzde finansal dünya, teknolojik yenilikler ve gelişmelerin etkisiyle büyük bir değişim ve dönüşüm yaşıyor. Bu değişimler, finans sektörünü daha önce hayal bile edilemeyecek bir hızda dönüştürüyor. Geleneksel finansın yerini artık daha hızlı, daha mobil, daha erişilebilir ve daha veri odaklı bir finans sistemi alıyor.

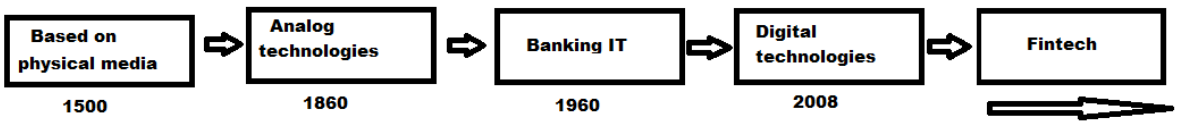
Finansal Veri Uzayı (Financial Data Space), finans dünyasında bulunan büyük miktardaki verilerin toplandığı, düzenlendiği ve paylaşıldığı bir dijital ekosistemdir. Geleneksel finans sistemi yerini, bu dijital veri alanına bırakmaya başladı. Bu uzay, birçok kaynaktan gelen farklı türde verileri içeriyor. Bu hisse senedi fiyatları, faiz oranları, döviz kurları, ekonomik göstergeler gibi finansal araç ve piyasalara ait pek çok veriyi içerir.

Bu veri uzayı, genellikle birçok farklı kaynaktan gelen verileri içerir. Finansal kurumlar, teknoloji şirketleri ve hatta bireyler bu veri uzayına katkı sağlarlar. Bu veriler, hisse senedi fiyatlarından tahvil faiz oranlarına, makroekonomik göstergelerden müşteri işlemlerine kadar geniş bir yelpazede olabilir.

Finansal piyasalarda verinin önemi gün geçtikçe daha da öneme sahip olmaktadır. Finansal piyasalarda doğru, güvenilir ve hızlı kararlar için verinin önemi büyüktür. Veri üretimin artması rekabet açısından düşünüldüğünde verinin önemi gün geçtikçe daha da artmaktadır. Elektronik iletişim noktalarının artması ile verinin çeşitliliği de artmaktadır. Böylece kullancılara daha fazla kişiselleştirilmiş ürün ve hizmetlerin sunulmasınına olanak sağlanmaktadır.

9.1 Finans Sektöründe Teknoloji

Finansal piyasaları fiziki medyadan Fintech'e geçişi çok hızlı oldu. Dijital teknolojilerin gelişimi ile finansal sektör teknolojiye en hızlı uyum sağlayan sektörlerin başında geldi.Digital teknolojilerin gelişimi ile de veriye ulaşım daha kısa zaman aldı.[99]



Şekil 12: Finans Sektöründe Teknoloji Adaptasyonunun Çizelgesi

9.2 Finansal Verinin Önemi

Finansal kurumların veriyi kullanım amaçları farklılık gösterebilir. Fakat, temelde finansal kurumlarının veriyi kullanma amaçları şöyle özetlenebilir.

- Karar Alma Süreçlerinin İyileştirilmesi: Finansal veri, finansal kurumların daha hızlı ve doğru kararlar almasını sağlar. Büyük veri analitiği ve yapay zeka, bu verileri hızlı bir şekilde analiz ederek, daha iyi yatırım ve risk yönetimi kararları alınmasını sağlar. Bu işlem maliyetlerini düşürdüğü gibi daha iyi kararlar alınmasına da yardımcı olur.

[99] HMM Fairooz ve CN Wickramasinghe , ''İnnovation and Development of Digital Finance : A Review on Digital Transformation in Banking & Financial Sector of Sri Lanka'', Asian Journal of Economics, Finance and Management 1, No 2 (2019),73

- Risk Yönetimi: Finansal kurumlar veri analitiği aracılığıyla riskleri daha iyi takip edebilir ve izleyebilir. Bu finansal krizlerin önlenmesine, Pazar eğilimlerinin tespitine ve müşteri varlıklarının korunmasına yardımcı olur.
- Müşteri Hizmetleri: Veri kurum müşterilerine daha iyi ve kişilleştirilmiş hizmetler sunmayı mümkün kılar. Kurumlar müşterilerinin tercihini anlamak ve daha iyi hizmet sunmak için bu verileri kullanırlar.
- Yatırım Fırsatları: Yatırımcılar, finansal verileri analiz ederek daha bilinçli yatırım fırsatları bulabilirler. Geçmiş verileri ve analizleri kullanarak gelecekteki fırsatları daha iyi tahmin edebilirler.

9.3 Dünyada Açık Bankacılık Uygulamaları Ve Regülasyonları

Finansal teknolojiler alanında mihenk taşı olarak kabul edilebilecek düzenlemelerden ilki, Avrupa Birliği tarafından 2007 yılında yayınlanan ve 2009 yılında tüm üye ülkelerde uygulanmaya başlanan Ödeme Hizmetleri Direktifidir. Payment Services Directive ("PSD") PSD'yi, 2015 yılında yayınlanan ve geçiş dönemi için iki senelik bir süre öngörülen ikinci Ödeme Hizmetleri Direktifi – Payment Services Directive 2 izledi. Açık bankacılık kavramını AB sınırları içinde kurumların bir inisiyatifi olmaktan çıkarıp çerçevesi kanunlar ile belirlenmiş mecburi bir statüye kavuşturmayı hedefleyen PSD2 ile birlikte, onayı alınan banka müşterilerinin finansal bilgilerinin banka dışı diğer hizmet sağlayıcılarının erişimine açılması zorunluluk haline gelmiştir.[100]

Finans sektörünün en gelişmiş olduğu ülkelerden biri olan Birleşik Krallık'ta ise, ülkenin AB üyesi olduğu dönemde uygulanmaya başlayan PSD ve PSD2'ye ek olarak Birleşik Krallık Rekabet ve Piyasalar Kurumu ("CMA") tarafından ülkedeki 9 büyük bankanın açık API yapılarına geçmesini ve Açık Bankacılık Uygulama Kurumu ("OBIE") isimli yapıyı kurmalarını mecburi kılınmıştır. OBIE, 2018 yılının Ocak ayında ilk açık bankacılık standardını yayınlamış olup, bu standardı aynı yılın Mart ayında ikinci standart izlemiştir. OBIE'nin verilerine göre şimdiye kadar 118 kuruluş açık bankacılık lisansı almış olup, 200 şirket de başvuru aşamasındadır. Tüm bu gelişmeler sonucunda, Birleşik Krallık'ta açık bankacılık API'leri üzerinden sağlanan işlem sayısı bir milyonu geçmiş durumdadır. Öte yandan Meksika, 10 Mart 2018'de kabul ettiği yasa ile kullanıcı verilerinin finansal kuruluşlar arasında açık API yapıları ile paylaşılmasını yasal hale getirmiştir. Yasanın imkân tanıdığı yapılar ilerleyen dönemlerde Merkez Bankası ve Meksika Ulusal Bankacılık ve Menkul Kıymetler Komisyonu tarafından detaylandırılarak geliştirilecektir. İsviçre'de ise ülkedeki tüm bankacılık sistemi için genel bir API standardı hazırlamak amacıyla çalışmalar sürdürülmektedir.[101]

Avustralya'da açık bankacılık tartışmaları, Avustralya Federal Hükümeti tarafından açıklanan ulusal bir Tüketici Veri Kanunu ("CDR") hazırlanmasıyla başlamış bulunmaktadır. Bankacılık sektörü, CDR'yi "açık bankacılık" adı altında benimseyen ilk sektör olacaktır. Asya'da ise, Temmuz 2018'de Hong Kong Para Otoritesi ("HKMA"), açık bankacılık için düzenleyici çerçeveyi belirleyen Açık API Çerçevesini yayınlamıştır. Aynı yönde, Singapur Para Otoritesi,

[100] https://kilinclaw.com.tr/turkiyede-ve-dunyada-acik-bankacilik/
[101] https://www.tcmb.gov.tr/wps/wcm/connect/d60cc679-ce04-4941-b310-b3788b6f3540/Odeme+Hizmetlerinde+Veri+Paylasim+Servislerine+Iliskin+Rehber.pdf?MOD=AJPERES

açık bankacılık düzenleme stratejilerinin bir parçası olarak tavsiye niteliğinde API Yönergeleri yayınlamış bulunmaktadır.[102]

9.4 Avrupa Birliği, 2022 Açık Finans Raporu

Açık finans, çok çeşitli finansal hizmetlerin kişisel ve kişisel olmayan verilerin paylaşılması, erişilmesi ve yeniden kullanılması anlamına gelir. Açık finansmanın amacı, tüketicilerin ve doğrudan dağıtıma gelişmiş finansal ürün ve hizmetlerin teşvik edilmesidir. Açık finans için kilitlenmiş, güçlü ailenin güveni ve inancıdır. Sektörler arasında ve sektörler içinde gelişmiş veri açıklığına yönelik daha ileri adımlar, veriye dayalı inovasyon fırsatlarını artıracak ve veriler için daha geniş bir tek pazar varyasyonunu kesintiye uğratmaktadır.

Finansal ürün ve hizmetlerin bozulması ve firmalara daha iyi hedeflenmiş daha doğru ihtiyati risk yönetimi dahil olmak üzere kişisel ve firmalar için hizmetler ve ürünler oluşturmak için Yapay Zeka / Makine Öğrenimi modellerinin geliştirilmesini desteklemek.

İnovasyon - açık finansta verilerin birlikte çalıştırılabilmesini sağlamak; birlikte Hizmetler. Bu şunları içerir: amacına ulaşmak için yalnızca güçlü müşterinin güvenine ve kayıtlı olan kişisel veriler uygulanacak siber güvenlik riskleri; Kişisel ve kişisel olmayan verilerin korunması, ticari sırlar, fikri mülkiyet hırsızlığı veya endüstriyel casusluk dahil. Açık finansmanın temel odak noktası tavsiyeleri ve kişiselleştirilmiş tavsiyeler almak için verimlilik yaratmak olmalıdır.

Finansal sistemin bileşenleri olarak finansal hizmetler kullanıcıları, sağlayıcıları, finansal altyapısı ve düzenleyici ve kurumsal ortamdan oluşur.

Fintech'in benimsenmesinin temel itici güçleri arasında geleneksel finansın yüksek maliyetleri, rekabetçi bir ortam, destekleyici düzenleme ve değişen demografi ile ilişkili karşılanmamış talep yer alıyor.

9.5 Türkiye'de Açık Bankacılık

Bankalarda son dönemde veri paylaşımın yapıldığı son uygulamalar olarak açık bankacılık görülmektedir.

Açık bankacılık, finansal sistemdeki verilerin belirlenen düzenlemelere uygun bir şekilde standart Uygulama Programlama Arayüzleri (Application Programming Interface, API) aracılığı ile müşterinin açık rızası dâhilinde üçüncü taraf hizmet sağlayıcıların erişimine açılmasıdır. Bu sayede üçüncü taraf hizmet sağlayıcılar rekabet ortamında geliştirdikleri yenilikçi finansal hizmetler ile kullanıcılara çok daha hızlı, düşük maliyet ve yüksek kullanıcı deneyimi ile işlem gerçekleştirme imkânı sunarken, finansal kuruluşlar da temel hizmetlerini kullanıcılara üçüncü taraf hizmet sağlayıcılar vasıtasıyla daha yaygın ve müşteri ihtiyaçlarına en uygun şekilde kullandırabilmektedir. Çok çeşitli bankacılık hizmetleri ve finansal hizmetleri içeren açık bankacılık uygulamalarının bir çeşidi olarak, 12 Kasım 2019 tarihli ve 7192 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile değiştirilen 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunun (Kanun) 12 nci maddesinin birinci fıkrasına

[102] https://kilinclaw.com.tr/turkiyede-ve-dunyada-acik-bankacilik/

TCMB'nin yetki ve sorumluluk alanında bulunan ödemeler alanı için tanımlanmış iki temel hizmet eklenmiştir:[103]

- Ödeme Emri Başlatma Hizmeti: Ödeme hizmeti kullanıcısının isteği üzerine başka bir ödeme hizmeti sağlayıcısında bulunan ödeme hesabıyla ilgili sunulan ödeme emri başlatma hizmeti [(f) bendi],
- Hesap Bilgisi Hizmeti: Ödeme hizmeti kullanıcısının onayının alınması koşuluyla, ödeme hizmeti kullanıcısının ödeme hizmeti sağlayıcıları nezdinde bulunan bir veya daha fazla ödeme hesabına ilişkin konsolide edilmiş bilgilerin çevrimiçi platformlarda sunulması hizmeti [(g) bendi].

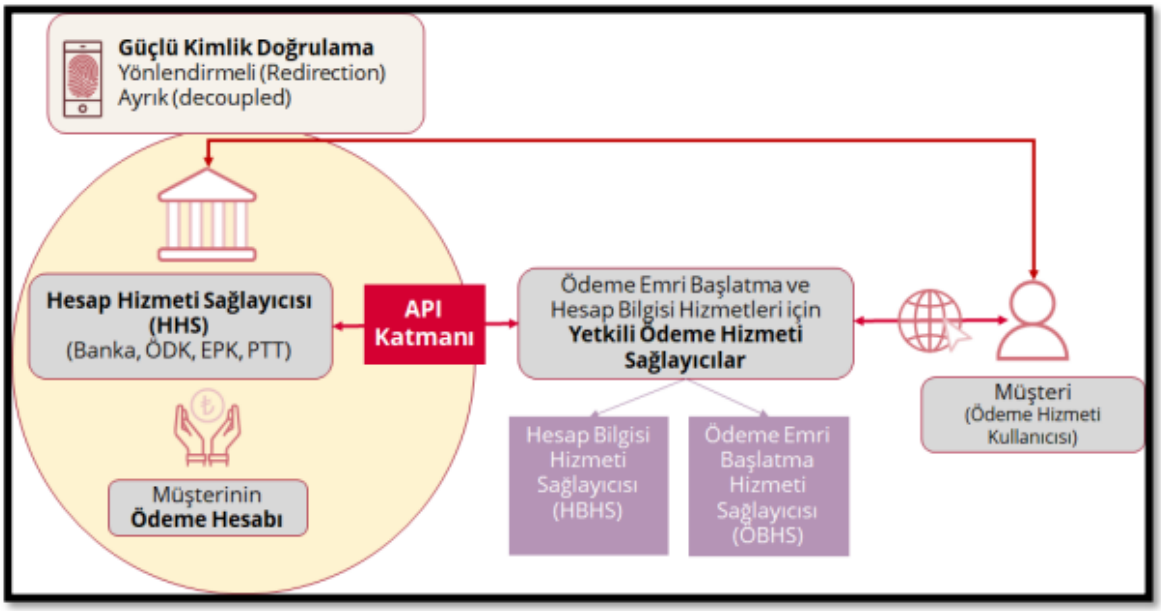
Ödeme Hesapları ve İşlem Türleri - ÖHVPS kapsamına giren ödeme hesabı olarak değerlendirilecek hesaplar Yönetmeliğin 59 uncu maddesinin sekizinci fıkrasında sayılmıştır:

- Vadesiz hesaplar,
- İşlem hesapları,
- Kredi kartı hesapları,
- Elektronik para hesapları,
- Müşteri adına açılan ve başka bir hesaba bağlı olmaksızın diğer kişilere fon aktarımı yapılabilen hesaplar (bu hesaplar belirlenirken geçici hareketlerin izlendiği nazım hesaplar benzeri hesaplar dışarıda bırakılmalıdır)
    - TCMB, bu hesaplar dışında kalan ancak ödeme hizmeti sağlayıcılarının sundukları ödeme hizmetlerinde kullanılan diğer hesap türlerinden uygun olanları da ödeme hesabı olarak değerlendirilmesine karar vermeye yetkilidir. Bir ödeme hesabının açık bankacılık kapsamında değerlendirilebilmesi için Yönetmeliğin 60 ıncı ve 61 inci maddeleri uyarınca çevrimiçi erişilebilir olması gerekmektedir. İşletilmekte olan çevrimiçi ödeme hesaplarına ilişkin ÖHVPS kapsamında değerlendirilen işlemin bulunduğu iş modelleri için TCMB'ye faaliyet izni başvurusunda bulunulması gerekmektedir.
    - Yürürlükteki ÖHVPS API Standartları belgesi (https://ohvps.github.io/);
        - Vadesiz TL, yabancı para hesapları (gerçek ve tüzel kişilere ait ödeme hesapları) ve kredili mevduat hesaplarını,
        - Ödeme Emri Başlatma Hizmeti için o Tekil ödeme (Virman/Havale/FAST/Müşterilerarası TL Aktarım Sistemi PÖS) işlemleri
        - Sadece Virman ve havale işlemleri kapsamında ek olarak yabancı para transferi o Aşağıdaki akış türlerini içeren TR Karekodlu ödemeler şöyledir:
        - Akış türü 01: Dinamik doğrulamalı işyeri ödemesi
        - Akış türü 02: Statik doğrulamalı işyeri ödemesi
        - Akış türü 03: Kişiden kişiye ödemeler.
        - Hesap Bilgisi Hizmeti için o Temel veya ayrıntılı hesap bilgisi sorgusu o Bakiye sorgusu o Gerçekleşen işlemler için hesap hareketleri sorgusu işlemlerini desteklemektedir.

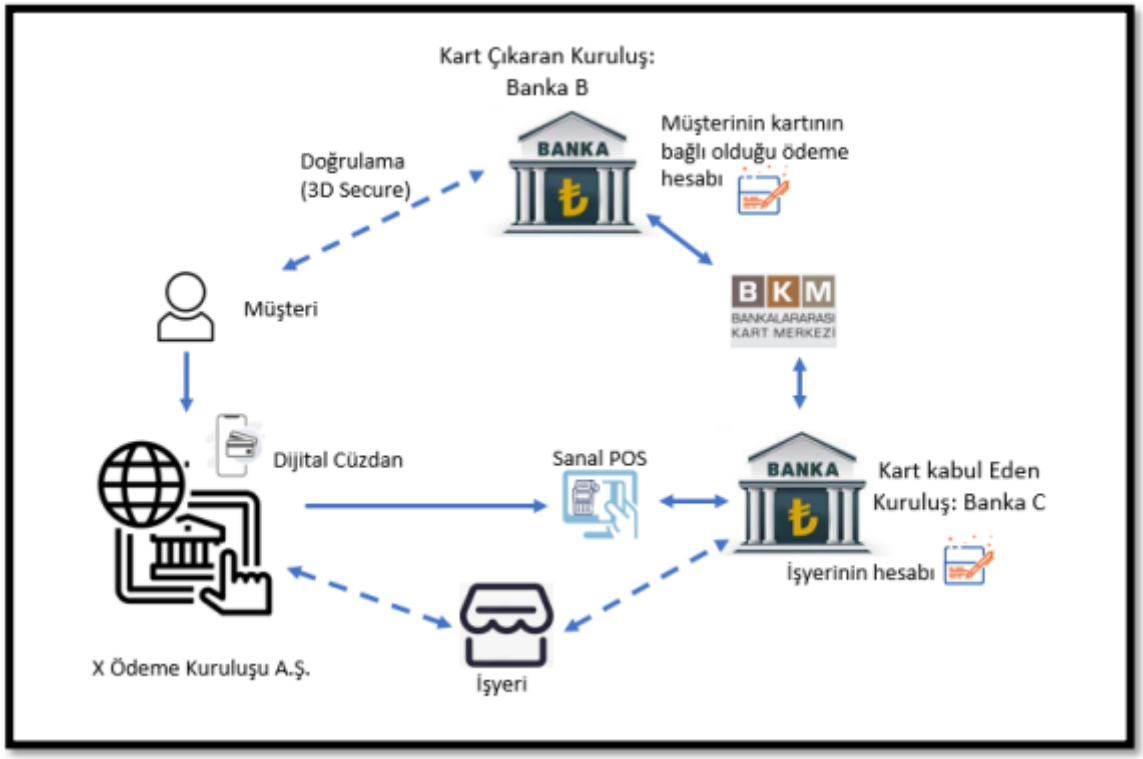
[103] https://www.tcmb.gov.tr/wps/wcm/connect/d60cc679-ce04-4941-b310-b3788b6f3540/Odeme+Hizmetlerinde+Veri+Paylasim+Servislerine+Iliskin+Rehber.pdf?MOD=AJPERES

- Bir HHS'nin gerçek veya tüzel kişi müşterilerine yalnızca kendi nezdinde bulunan ödeme hesaplarına ilişkin olarak verdiği hizmetler ÖHVPS kapsamı dışındadır. Ödeme hizmeti sağlayıcısının kendi nezdindeki hesaplarla ilgili olarak kendi müşterisine Kanun kapsamında sunduğu hizmet ödeme hesabının işletimi ile ilgili olup 6493 sayılı Kanun'un 12 nci maddesinin birinci fıkrasının (a) bendi kapsamındadır. HHS'lerin başka ödeme hizmet sağlayıcılar nezdindeki hesaplarla ilgili sunduğu hizmetler 6493 sayılı Kanun'un 12 nci maddesinin birinci fıkrasının (f) ve (g) bentleri kapsamındadır.

Ödeme Hizmetleri Veri Paylaşım Servisleri (ÖHVPS) olarak adlandırılan söz konusu iki hizmet ile ödemeler alanındaki açık bankacılık servisleri Avrupa Birliği Ödeme Hizmetleri Direktifi'nin ikinci sürümü (Payment Services Directive 2-PSD2) ile uyumlu şekilde tanımlanmıştır. Diğer taraftan, 7192 sayılı Kanun ile 6493 sayılı Kanun'da yapılan değişiklikler çerçevesinde TCMB tarafından hazırlanan "Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik" (Yönetmelik) ve "Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ" (Tebliğ) 1 Aralık 2021 tarihli ve 31676 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiş olup söz konusu düzenlemeler ile ÖHVPS'ye ilişkin temel hususlar ile ilgili çerçeve çizilmiştir.



Şekil 13: Ödeme Hizmetleri Veri Paylaşım Servisleri (ÖHVPS) Genel Gösterimi



Şekil 14: Ödeme Hizmetleri Veri Paylaşım Servisleri (ÖHVPS) Senaryosu

Bu senaryoda (a), (b) ve (c) bentlerinden faaliyet izni bulunan X Ödeme Kuruluşu A.Ş.'nin (X Ödeme) müşterileri kendilerine ait banka kartlarını X Ödeme'nin sunduğu dijital cüzdanda saklamaktadır. Müşteri, X Ödeme'nin uygulamasını kullanarak bu dijital cüzdandaki kartlarından (bağlı ödeme hesabından) X Ödeme'nin anlaşmalı işyerinin hesabına fon transferi yapmaktadır (Şekil 14).

9.6 Finansal Sektörde Veri Paylaşımı Yapan Kurumlar

Türkiye Cumhuriyeti Merkez Bankası (TCMB): Merkez bankası istatistikler başlığı altında çoğunlukla ulusal ve uluslararası verileri paylaşmaktadır. Enflasyon, faiz, döviz, reel Sektör, ödemeler dengesi, bankacılık ve piyasa verilerini sunmaktadır. Bu kapsamda Merkez Bankası Elektronik Veri Dağıtım Sistemini (https://evds2.tcmb.gov.tr/) kurarak finansal kurumlara bilgi akışı sağlamaktadır.

Bankacılık Düzenleme Ve Denetleme Kurumu (BDDK): Kamuoyunun ve ilgili tüm tarafların bilgilendirilmesi amacıyla BDDK tarafından bankacılık sektörüne ilişkin olarak çeşitli veriler yayımlanmaktadır. Bankacılık sektörüne Günlük Bülten, Haftalık Bülten, Aylık Bülten, Finansal Türkiye Haritası (FinTürk)-İllere Göre, Kredi Kartı Bilgileri ve Türk Bankacılık Sektörü (TBS) Temel Göstergeleri ve Banka Dışı Mali Kuruluşlar Verileri olarak Faktoring, Finansal Kiralama, Finansman, Varlık Yönetim Şirketi verisini paylaşmaktadır.

Türkiye Bankalar Birliği (TBB): Bankalara ait bünyesinde bulundurduğu veri sistemi ile (https://verisistemi.tbb.org.tr/) çeşitli raporlar sunulmaktadır.

Kredi Kayıt Bürosu (KKB): 31 Aralık 2022 tarihi itibarıyla 57 banka, 19 tüketici finansmanı, 49 faktoring, 21 finansal kiralama, 10 sigorta, 23 varlık yönetim şirketi, 7 diğer olmak üzere

toplam 186 üyeye sahiptir. 2022 yıl sonu itibarıyla 89 ürün ve hizmeti üyelerinin kullanımına sunmaktadır. Müşteriye ait kredili ürünlerin sayısı ve bankalarda bulunan varlıklar ile ilgili bilgiler de bulunur. KKB risk raporunda güvenilirlik durumu; kredi ürünlerinin kullanımı ve ödeme istikrarının ölçümü ile belirlenir.

KKB, risklerin tespiti ve değerlendirilmesi için bir veritabanı işlevi görür.

KKB, adalet yargı sistemi olan UYAP'tan kredi riskini oluşturacak konkordato ve iflas risklerinin paylaşılması son yıllarda sağlayarak diğer sektörlerden de veri paylaşımını sunmuştur.

KKB'nin sağlık sistemi ile entegrasyonu açısından bankalarca/finansal kurumlarca kredi kullandırımı yapılması esnasında hayat sigortası kapsamında müşterinin rızası dahilinde Sağlık Bakanlığı bünyesindeki veriye ulaşım sağlanarak müşterinin hastalık bilgileri sonucunda risk raporunun oluşturulması sonradan oluşacak yargı süreçlerini ortadan kaldırabilir. Ancak, Sağlık Bakanlığı nezdinde verilerin KKB ile paylaşılması husundaki KVK hukuki değerlendirmeler de önemlidir.

Bankalararası Kart Merkezi (BKM): BKM Veri Ambarı MIS ve Raporlama Hizmetleri ile üyelerine çeşitli veri sunmaktadır.BKM Veri Ambarı Türkiye içinde yurtiçi/yurtdışı kartlar kullanılmak suretiyle ve Türkiye dışında yurtiçi kartlar kullanılmak suretiyle gerçekleşen alışveriş ve nakit işlemlerine ait otorizasyon ve takas kayıtlarının, sahtekarlık bildirimlerinin ve işyeri kayıtlarının geriye dönük saklanmasını sağlayan hizmettir.

BKM Veri Ambarı ile söz konusu kayıtların, sahtekarlık tespiti, istatistik, pazar araştırma ve pazar geliştirme amaçlı olarak Üyeler ve BKM tarafından sorgulanması ve analiz edilmesi sağlanmaktadır.

10 Mobilite Alanında Veri Uzayı Uygulaması

Mobilite, bireylerin, nesnelerin veya verinin fiziksel ya da sanal ortamlar arasında serbestçe hareket edebilme yeteneğini ifade eder. Bu kavram, günümüzde özellikle teknolojinin sürekli gelişen dünyasında, taşınabilir cihazların yaygınlaşmasından otomotiv endüstrisindeki akıllı ulaşım sistemlerine kadar birçok alanda karşımıza çıkar. İnsanların günlük yaşamlarını daha verimli ve rahat hale getirebilmek adına teknolojinin sunduğu mobil çözümler, bireylerin zaman ve mekândan bağımsız bir şekilde bilgiye erişimini ve işlevselliğini artırır.

Veri uzayı, veri nesnelerinin ve bu nesneler arasındaki ilişkilerin geometrik bir temsilini ifade eder. Bu kavram, çok boyutlu veri setlerinin analiz edilmesi ve bu verilerin uygun bir şekilde görselleştirilmesi için kullanılır. Veri uzayında her bir nesne, bir vektör olarak temsil edilir ve bu vektörler arasındaki uzaklıklar, nesneler arasındaki benzerlikleri veya farklılıkları belirler. Mobilite ile birleştirildiğinde, veri uzayı kavramı, hareket halindeyken de veri analizi ve işleme yeteneklerinin önemini vurgular. Bu sayede, dinamik ve değişken ortamlarda bile bilgiye hızla ve etkin bir şekilde ulaşabiliriz.

Günümüzde mobil teknolojiler, modern yaşamın ayrılmaz bir parçası haline gelmiştir. Akıllı telefonlardan tablet bilgisayarlara, giyilebilir cihazlardan IoT (Nesnelerin İnterneti) cihazlarına kadar birçok teknolojik araç, bireylerin günlük yaşamlarını daha bağlantılı, erişilebilir ve rahat hale getirmektedir. Bu cihazların yaygınlaşmasıyla birlikte, bilgiye erişim, eğlence, iş, sosyal iletişim ve birçok diğer faaliyet, artık cepte taşınan bir cihaz aracılığıyla her an her yerde gerçekleştirilebilir hale gelmiştir. Bu durum, hem bireylerin yaşam tarzını hem de iş dünyasının işleyişini radikal bir şekilde dönüştürmüştür.

Bu teknolojik dönüşümün etkisi sadece bireysel kullanıcılarla sınırlı değildir. Şirketler, mobil teknolojilere yatırım yaparak iş süreçlerini optimize ediyor, müşteriyle etkileşimlerini artırıyor ve yeni pazar fırsatları yaratıyorlar. Eğitim, sağlık, finans ve birçok diğer sektör, mobil uygulamalar ve çözümler sayesinde daha erişilebilir ve kullanıcı dostu hizmetler sunmaktadır. Ayrıca, mobil teknolojilerin artan önemi, veri güvenliği, gizlilik ve etik konularında yeni tartışma ve sorunların ortaya çıkmasına da neden olmuştur. Bu nedenle, mobil teknolojilerin yükselişi, hem fırsatları hem de zorlukları beraberinde getiriyor.

Veri uzayında mobilite kavramı, günümüzde büyük bir öneme sahiptir. Bu kavram, veri nesnelerinin dinamik ve değişken ortamlarda sürekli olarak hareket ettiği ve bu hareketin veri analizi, yorumlama ve görselleştirme süreçlerine direkt etkisi olduğu anlamına gelir. Özellikle akıllı telefonlar, IoT cihazları ve diğer mobil teknolojiler sayesinde, bireyler ve kurumlar her an her yerde veri üretiyor, paylaşıyor ve tüketiyor. Bu mobil veri akışı, veri uzayının sürekli olarak genişlemesine ve evrilmesine neden olur. Bu durum, veri bilimcileri ve analistleri için hem yeni fırsatları hem de zorlukları beraberinde getirir; zira bu sürekli değişen veri uzayında doğru bilgiye hızlıca ulaşmak ve bu bilgiyi anlamlı bir şekilde yorumlamak kritik bir öneme sahip olmuştur.

Mobilitede, artan bağlantılılık ve teknolojik ilerlemelerle birlikte hem yeni zorluklar hem de fırsatlar ortaya çıkmaktadır. Güncel zorluklar arasında, artan veri hacmi nedeniyle gizlilik ve veri güvenliği konuları, cihazlar arası uyumluluk sorunları ve sürekli değişen teknolojiye adaptasyon bulunmaktadır. Öte yandan, bu evrimsel süreç, özelleştirilmiş kullanıcı deneyimleri, daha hızlı ve kesintisiz bağlantı seçenekleri ve genişleyen veri uzayından elde edilen derinlemesine analizler gibi fırsatları da beraberinde getiriyor. Bu dengede ilerlemek,

sektör oyuncuları için hem rekabetçi kalabilmek hem de kullanıcıların ihtiyaçlarına cevap verebilmek adına kritik bir öneme sahiptir.

Mobil teknolojiler, modern yaşantımızın merkezine yerleşerek hem bireysel hem de toplumsal anlamda derin değişikliklere yol açmıştır. Mobilite; veriye erişimi, sosyal iletişimi ve kültürel değişiklikleri hızlandırarak, bireylerin ve toplumların dünyayla etkileşim biçimlerini dönüştürmüştür. Özellikle sosyal medya ve diğer dijital platformların mobil cihazlarla bütünleşmesi, küresel etkileşimin ve bilgi alışverişinin hızını artırmış, farklı kültürlerin birbirleriyle daha derinlemesine etkileşimde bulunmasına olanak tanımıştır. Ancak bu sürekli bağlantılılık, bireyler için yeni zorlukları da beraberinde getirirken, veri güvenliği ve kişisel gizlilik konularını da ön plana çıkarmıştır.

Sonuç olarak, mobilite, günümüzün globalleşen dünyasında bilgiye erişimi, sosyal etkileşimi ve kültürel adaptasyonu şekillendiriyor, ancak bu dönüşümün beraberinde getirdiği zorlukları da dikkate almak esastır.

10.1 Mobilite ve Veri Erişim Kolaylığı

Mobil cihazların evrimi, teknolojinin sadece iletişimi değil, aynı zamanda bilgi işlem kapasitesini ve işlevselliğini de nasıl değiştirdiğinin bir göstergesidir. İlk taşınabilir telefonların basit arama ve mesajlaşma işlevlerinden, bugünkü akıllı telefonların geniş uygulama yelpazesine ve çoklu görev kapasitesine doğru geçiş, yapay zeka (YZ) teknolojilerinin bu cihazlara entegrasyonuyla daha da hızlandı. Yapay zeka, mobil cihazlarda sesli asistanlardan, fotoğraf tanıma sistemlerine, öneri algoritmalarından, dil çeviricilere kadar bir dizi uygulamada yer buldu. Bu entegrasyon, kullanıcı deneyimini daha kişiselleştirilmiş ve etkileşimli hale getirdi. Akıllı telefonların yapay zeka ile birleşimi, teknolojinin bireylerin günlük yaşantılarına ne denli derinlemesine nüfuz edebileceğinin bir yansımasıdır.

Veriye anında erişim imkanının artışı, çağımızın en belirgin teknolojik ilerlemelerinden biridir. İnternetin yaygınlaşması, bulut depolamanın ortaya çıkışı ve mobil cihazların evrimi sayesinde, bireyler ve kurumlar, ihtiyaç duydukları bilgilere neredeyse her yerde ve her zaman ulaşabilir hale geldi. Bu durum, iş süreçlerinden eğitime, eğlenceden sosyal etkileşimlere kadar birçok alanda dinamiklerin değişmesine yol açtı. Özellikle büyük veri ve yapay zeka teknolojilerinin yükselmesiyle, bu anında erişim imkanı, sadece mevcut verilere ulaşmak değil, aynı zamanda bu veriyi derinlemesine analiz ederek anlamlandırmak ve öngörülerde bulunmak için de kritik bir öneme sahip oldu. Bu gelişmeler, bilgiye erişimin ve bu bilginin kullanılmasının önündeki engelleri asgariye indirerek, daha bağlantılı ve bilgi temelli bir toplumun oluşmasına katkıda bulundu.

10.1.1 İş Hayatında Mobil Erişimin Faydaları

Mobil erişim, iş dünyasında çalışma dinamiklerini kökten değiştirdi. Eskiden ofise bağlı kalmak zorunda olan profesyoneller, şimdi akıllı telefonlar ve tabletler sayesinde her yerden çalışabilme özgürlüğüne sahip. Bu, esnek çalışma saatleri ve uzaktan çalışma modellerinin yaygınlaşmasını teşvik etti, bu sayede iş verimliliği arttı ve çalışan memnuniyeti yükseldi. Ayrıca, iş seyahatleri sırasında, toplantılarda veya saha görevlerindeyken bile e-postalara erişebilmek, belge paylaşabilmek ve işle ilgili uygulamaları kullanabilmek, iş süreçlerini hızlandırdı ve daha dinamik hale getirdi.

10.1.2 Özel Yaşamda Mobil Erişimin Faydaları

Özel yaşamda mobil erişim, bireylerin sosyal etkileşimlerini, eğlencelerini ve hatta günlük rutinlerini daha da kolaylaştırdı. Arkadaşlar ve aile ile iletişim kurma, sosyal medya platformlarına erişim, online alışveriş, seyahat planlama, sağlık takibi ve daha birçok faaliyet, bir mobil cihaz aracılığıyla parmak uçlarına kadar geldi. Aynı zamanda, kişisel hobiler, öğrenme ve kişisel gelişim için kullanılan uygulamalar sayesinde bireyler, boş zamanlarını daha verimli ve eğlenceli bir şekilde değerlendirebilir hale geldi.

Bu kolaylıklara rağmen, mobil erişimin sürekli olarak aktif olma beklentisi yaratması, iş ve özel yaşam arasında sınırların belirsizleşmesine yol açtı. Bu durum, bireyler için zaman yönetimi zorluklarını ve bazen de aşırı bağlantılılık hissini beraberinde getirebilir. Bu nedenle, mobil erişimin avantajlarından tam anlamıyla yararlanırken, teknolojiyle sağlıklı bir denge kurma ihtiyacı da ön plana çıkmaktadır.

10.2 Kişiselleştirilmiş Kullanıcı Deneyimi

Kişiselleştirilmiş kullanıcı deneyimi, dijital çağın talep ettiği bir standart haline gelmiştir. Kullanıcılar artık standart ve genel uygulamalar yerine, tercihlerine, ilgi alanlarına ve geçmiş davranışlarına uygun olarak özelleştirilmiş bir deneyim bekliyor. Bu özelleştirme, alışveriş önerilerinden sosyal medya akışlarına, haber kaynaklarından uygulama arayüzüne kadar geniş bir yelpazede hissedilmekte. Ancak bu artan beklenti, markaları ve dijital servis sağlayıcılarına, hem kişiselleştirmeyi doğru bir şekilde sunma hem de kullanıcı gizliliğini ve veri güvenliğini koruma zorunluluğunu getiriyor. Bu dengeyi sağlamak, kullanıcı sadakatini ve güvenini kazanmanın anahtarıdır.

Mobil cihazlar, kullanıcı alışkanlıklarını derinden etkileyerek modern yaşamın merkezine oturmuştur. Akıllı telefonlar ve tabletler sayesinde anlık bilgiye erişim, sosyal medya etkileşimi, online alışveriş ve medya tüketimi artık parmaklarımızın ucunda. Bu durum, geleneksel iletişim yöntemlerinden uzaklaşmamıza ve tüketim alışkanlıklarımızda dönüşümlere neden olmuştur. Ancak, bu sürekli bağlantılılık hali, kullanıcıların zamanlarını nasıl geçirdikleri konusunda da yeniden düşünmelerini gerektiriyor; aşırı bilgi tüketimi ve dijital izolasyon gibi olumsuz yan etkileri de beraberinde getiriyor.

Dijital çağın pazarlama ve medya dünyasında devrim yaratmış bir yaklaşımda kişiselleştirilmiş reklam ve içerik sunumudur. . Kullanıcıların online davranışları, alışveriş alışkanlıkları, sosyal medya etkileşimleri ve diğer dijital izleri analiz edilerek, onlara özel olarak hazırlanmış içerikler ve reklamlar sunulmaktadır. Bu kişiselleştirme, kullanıcıların ilgileriyle daha uyumlu ve etkili reklam kampanyaları oluşturulmasını sağlar. Sonuç olarak, firmalar için dönüşüm oranlarını artırırken, kullanıcılar için de daha alakalı ve değerli içerik deneyimleri oluşturmaktadır.

10.3 Güvenlik ve Gizlilik Konularında Yenilikler

Mobil cihazların yaygınlaşması, veri güvenliği risklerini de beraberinde getirdi. Bu cihazlar, kullanıcının kişisel bilgilerinden bankacılık detaylarına, fotoğraflarından mesajlarına kadar birçok özel veriyi barındırıyor. Kötü niyetli yazılımlar, phishing saldırıları ve ransomware gibi tehditler, kullanıcının bilgilerini ele geçirebilir veya cihazı kilitleyebilir. Aynı zamanda, açık Wi-Fi ağlarına bağlanma veya güncellenmemiş işletim sistemleri de veri sızıntılarına neden olabilir. Bu riskler, kullanıcıları mobil güvenlik konusunda daha bilinçli olmaya ve cihazlarını koruma yöntemleri araştırmaya teşvik etmektedir.

Mobil cihazlar, kişisel ve kurumsal bilgilere sürekli erişim imkânı sunduğundan, bu bilgilerin korunması hayati öneme sahiptir. Uygulamaların güncel tutulması, iki faktörlü kimlik doğrulama, şifre yöneticileri kullanma gibi basit önlemler, mobil güvenliği artırabilir. Aynı zamanda, VPN kullanımı, mobil cihaz yönetimi (MDM) çözümleri ve güvenliği artırılmış iletişim protokolleri gibi gelişmiş yöntemler, özellikle kurumsal mobil kullanımda veri sızıntılarına karşı ekstra bir koruma katmanı sağlar. Mobil güvenlik, sadece cihaz veya yazılım odaklı değil, aynı zamanda bilinçli kullanıcı davranışlarıyla da tamamlanmalıdır.

GDPR (Genel Veri Koruma Yönetmeliği) ve KVKK (Kişisel Verileri Koruma Kanunu) gibi düzenlemeler, bireylerin kişisel verilerinin korunmasını ve gizliliğini sağlama amacı güder. Bu tür düzenlemeler, özellikle mobil platformlarda, veri toplama, saklama ve işleme yöntemlerine dair katı kurallar getirmiştir. Mobil uygulama geliştiricileri ve hizmet sağlayıcıları, kullanıcının onayı olmadan kişisel veri toplamak, bu verilere erişmek veya paylaşmak konusunda sınırlamalara tabidir. Aynı zamanda, kullanıcılara veri toplama ve kullanımı hakkında şeffaf bilgilendirme yapma zorunluluğu bulunmaktadır.

Bu düzenlemeler, mobil cihazlar üzerinden gerçekleştirilen işlemlerin artmasıyla birlikte daha da kritik hale gelmiştir. Uygulamaların kişisel bilgileri, konum bilgileri veya cihaz erişim izinleri üzerinden topladığı veri miktarının artması, kullanıcıların gizlilik endişelerini de beraberinde getirmiştir. GDPR, KVKK gibi düzenlemeler, kullanıcılara verileri üzerinde daha fazla kontrol imkânı sunarken, işletmelere de veri koruma ve gizlilik konularında daha sorumlu davranma yükümlülüğü getiriyor. Bu, hem mobil teknolojinin hem de kişisel veri koruma anlayışının evrimini şekillendiren kritik bir adımdır.

10.4 Yeni İş Modelleri ve Fırsatları

Mobil tabanlı iş modelleri, son yıllarda teknolojik gelişmelerin ve kullanıcı alışkanlıklarının değişimi ile büyük bir popülerlik kazanmıştır. Akıllı telefonlar ve tabletlerin yaygınlaşması, işletmelere, tüketicilere doğrudan, her an erişilebilen ve kişiselleştirilmiş hizmetler sunma fırsatı veriyor. Mobil ödeme sistemlerinden, e-ticaret platformlarına, taksi çağırma uygulamalarından yemek servislerine kadar birçok sektör, mobiliteyi iş modelinin merkezine alarak yenilikçi çözümler geliştirmiştir. Bu mobil odaklı yaklaşım, tüketicilere esneklik ve konfor sunarken, işletmeler için de yeni gelir kanalları ve müşteri tabanı genişletme potansiyeli oluşturuyor.

Paylaşım ekonomisi, bireylerin sahip oldukları kaynakları, hizmetleri veya yetenekleri diğerleriyle paylaşmasını temel alır ve bu ekonomik modelin yükselişi, büyük ölçüde mobil platformların etkisiyle gerçekleşmiştir. Akıllı telefonlar ve uygulamalar, kullanıcıların anında bir araba paylaşımı hizmetine, bir konaklama platformuna ya da yeteneklerini sunabileceği freelance platformlara erişim sağlamasına olanak tanır. Airbnb, Uber ve TaskRabbit gibi platformlar, mobil teknolojiler sayesinde kullanıcıların hizmetlere ve ürünlere hızlı, esnek ve özelleştirilmiş bir şekilde erişim sağlamasını kolaylaştırarak paylaşım ekonomisinin global bir fenomen haline gelmesine katkıda bulunmuştur.

Yapay zeka, artırılmış gerçeklik, nesnelerin interneti (IoT) gibi ileri teknolojilerin mobil uygulamalara entegrasyonu, kullanıcılara daha interaktif, özelleştirilmiş ve sürükleyici deneyimler sunma potansiyeli taşımaktadır. Ayrıca, bulut bilişim sayesinde uygulamaların daha hızlı, güvenli ve verimli çalışmasına olanak tanıyan serverless mimariler, geliştiricilere daha esnek ve ölçeklenebilir çözümler sunmaktadır. Bu yenilikler, start-up'ların ve mevcut

işletmelerin, kullanıcı ihtiyaçlarına daha dinamik ve yenilikçi çözümler üretme fırsatını yakalamalarına yardımcı olmaktadır.

Mobil uygulama pazarı, sürekli değişen teknolojik trendlerle birlikte dinamik bir büyüme ve evrim gösteriyor. Artırılmış gerçeklik (AR) ve sanal gerçeklik (VR) teknolojilerinin mobil platformlara adaptasyonu, kullanıcılara daha sürükleyici deneyimler sunma potansiyelini artırıyor. Yapay zeka ve makine öğrenimi, uygulamaların kullanıcı alışkanlıklarını daha iyi anlamasına ve buna göre özelleştirilmiş içerik sunmasına olanak tanırken, 5G gibi gelişmiş ağ teknolojileri, mobil uygulamaların performansını ve hızını artırarak kullanıcı memnuniyetini yükseltiyor. Bu yenilikçi trendler, geliştiricilere ve işletmelere, sektörde fark yaratma ve rekabette öne çıkma fırsatı sunuyor.

10.5 Sosyal ve Kültürel Etkiler

Mobil cihazlar, sosyal iletişimin dinamiklerini kökten değiştirerek, bireylerin her an, her yerden birbirleriyle bağlantı kurmasını mümkün kılmıştır. Sosyal medya platformları, anlık mesajlaşma uygulamaları ve video konferans hizmetleri sayesinde, kullanıcılar sadece yazılı metinlerle değil, fotoğraf, video ve sesli mesajlarla da duygularını, düşüncelerini ve deneyimlerini paylaşabiliyor. Bu sürekli ve anında iletişim, global bir topluluk oluşturma, fikir alışverişi yapma ve olaylara anında tepki verme yeteneği sağlıyor. Ancak, mobil cihazların sunduğu bu sürekli erişilebilirlik, aynı zamanda bireylerin sürekli çevrimiçi olma baskısı ve dijital dünyada sosyal izolasyon hissi gibi zorlukları da beraberinde getiriyor.

Mobilitenin yaygınlaşması, kültürel değişikliklerin hızını ve kapsamını büyük ölçüde etkilemiştir. Akıllı telefonlar ve mobil internet sayesinde, bireyler dünyanın dört bir yanındaki kültürlerle anında bağlantı kurabilir, bilgi alışverişinde bulunabilir ve farklı yaşam tarzlarını keşfedebilir. Bu sürekli erişilebilirlik ve etkileşim, değerlerin, normların ve trendlerin hızla sınırlar ötesi yayılmasına yol açar. Örneğin, bir ülkede popüler olan bir müzik türü, mobil platformlar aracılığıyla kısa sürede global bir fenomen haline gelebilir. Bu da farklı kültürlerin birbirlerini daha derinlemesine anlamasına ve küresel bir topluluk bilincinin oluşmasına katkıda bulunur. Ancak, bu sürekli etkileşim aynı zamanda yerel kültürlerin erozyonuna ve küresel bir homojenleşmeye de yol açabilir.

Mobilite, sosyal ağların kullanımını ve etkisini radikal bir şekilde dönüştürmüştür. Akıllı telefonlar ve tabletler sayesinde, kullanıcılar günün her saatinde ve her yerden sosyal ağlara erişebilir, güncellemelerde bulunabilir, fotoğraf ve video paylaşabilirler. Bu sürekli bağlantı, anlık haber akışı ve olaylara gerçek zamanlı tepkilerin yanı sıra, dünya genelindeki olaylara anında erişim olanağı sağlar. Sosyal medya platformları, mobil özellikler sayesinde daha interaktif, görsel ve kullanıcı odaklı hale gelmiştir. Fakat bu durum, kullanıcıların sürekli çevrimiçi olma baskısı, dijital izolasyon hissi ve gizlilik konularında endişeler gibi yeni zorlukları da beraberinde getirir.

11 Enerji Alanında Veri Uzayı Uygulaması

Türkiye'de enerji sektöründe kamu kuruluşları olarak Enerji Bakanlığı ve bağlı ilgili kuruluşlar arasında veri uzayı çalışmaları ile ilgili ; verinin toplanması,iletilmesi hakkında münferit çabalar mevcuttur.Fakat bu çabalar belli kurumlar arasında kısıtlı bir çerçevede yapıldığı için yeterli değildir.

Enerji sektörü için veri uzayı çalışmasının yapılması sektörün geleceği ve özellikle yapay zeka gibi teknolojilerin kamu sektöründe kullanılması açısından önemli veri altyapısı oluşturacağı için gerekliliği açıktır.

Türkiye'de enerji sektörü için veri uzayı çalışmaları yapılırken Enershare Project - The Energy Data Space for Europe (Avrupa Enerji Veri Uzayı Çalışması) en iyi uygulama örneği olarak değerlendirilebilir.

Avrupa'da enerji sektöründe veri uzayı çalışmalarının oluşturulması amaçlı başlatılan Enershare projesi, yakın zamanda Avrupa'da oluşturulan Enerjinin Sayısallaştırılması Eylem Planı'nın (DOEaP-Digitization of Energy Action Plan) uygulanmasının önünü açmaktadır.

Avrupa için; yeni veri odaklı kavramlar, mimariler,çözümler, araçlar, hizmetler yönetişim ve iş modellerini daha fazla dağıtmak için entegre ve karbondan arındırılmış tüketici merkezli enerji sisteminin tasarlanması amaçlanmaktadır.

Genel enerji değer zincirleri boyunca paylaşılan enerji verilerini, entegre bir ortamda saklamak, paylaşılabilir bir formatta sunmak, bugüne kadar dijitalleşmenin sağlanamadığı ortamda tam bir dijitalleşme olanağı sağlamak projenin odağındadır.

Enershare'in amacı, Avrupa'da Avrupa Ortak Eylem Planının enerji alanı için öngördüğü daha akıllı, sektörlerle bütünleşmiş bir yapıda, karbondan arındırılmış bir çevre sağlayan ve katılımcı bir yönetişim yapısıyla desteklenen bir enerji sektörü oluşturmaktır.

Enershare konsepti enerji verileri için güvenilirlik, emniyet ve güvenlik konuları etrafında şekillenir.

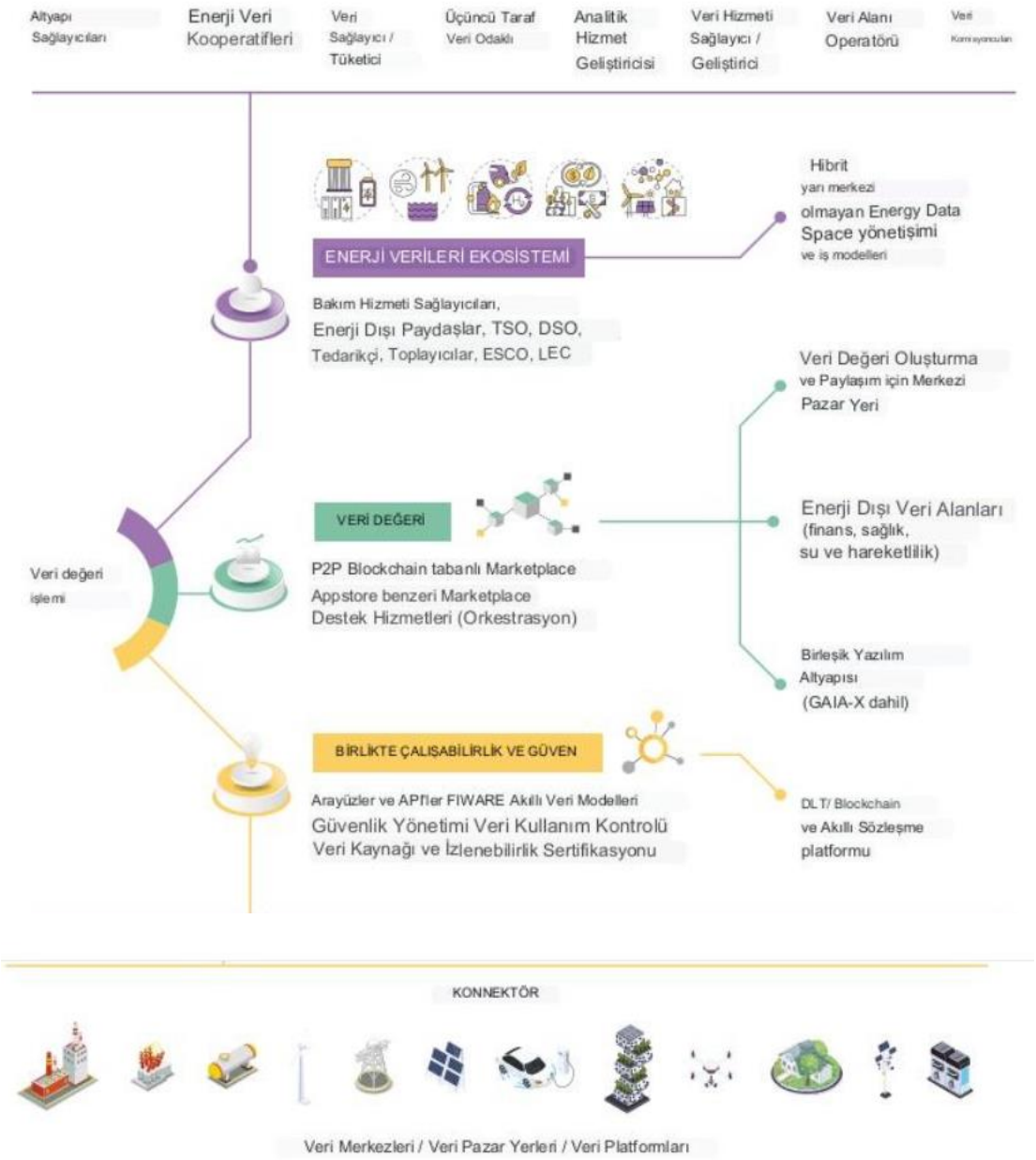
Paydaşlar arasında veri odaklı hizmetler için enerji verilerinin paylaşım ve değişimi üzerine inşa edilecektir. Sektörler arası enerji kullanıcı senaryoları ile enerji ve enerji dışı veriyi birleştirecektir. Enershare, önde gelen projeler, girişimler ve teknolojilerden yararlanır ve bunlara uyum sağlar IDSA, FIWARE ve GAIA-X uyumlu açık ve standartlaştırılabilir teknolojik bloklar oluşturmak amaçlanmaktadır.

EnerShare projesinin vizyonu ile ilgili görselde olduğu gibi enerji sektörü kendi içinde ve enerji sektörünün diğer sektörlerle olan veri paylaşımı çok katmanlı bir mimaride gerçekleşecektir. Her katmanda veriler kendi içinde paylaşılırken, diğer katmanların ihtiyacı olan veri gizlilik unsuru taşımıyorsa paylaşılacaktır. Aynı zamanda enerji verileri diğer sektörlerle Ortak Federasyon Veri Uzayı'nda tüm sektörlerin verileriyle birleştirilip, maksimum fayda elde edilmeye çalışılacaktır.[104]

[104] Enershare -The Energy Data Space for Europe

Şekil 15: EnerShare Vizyon Görseli

EnerShare konseptinde enerji verileri hibrit bir yönetişim modeli ile yönetilirken blokzincir teknolojisinin getirdiği özelliklerden, veriler için birlikte çalışabilirlik, güven ve izlenebilirlik özellikleri ile enerji sektörü paydaşları ve diğer sektörlerle iletişim olanağı sağlanacak, konseptin tamamlanması için kurulacak blokzincir tabanlı bir pazaryeri aracılığıyla güvenli veri transferi sağlanacaktır (Şekil 16).



Şekil 16: EnerShare Konsept Görseli

12 Savunma Alanında Veri Uzayı Uygulaması

Tüm diğer sektörlerde olduğu gibi; verinin stratejik, operasyonel ve taktiksel seviyelerdeki kullanımının optimize edilmesi, savunma alanında da doğru zamanda doğru bilgiye erişimi sağlayacak ve karar alma faaliyetlerinde yüksek öneme sahip bir destek unsuru olacaktır. Her türlü savunma faaliyetine ilişkin olarak güvenlik önlemlerinin tahsis edilmesinin, ülke kaynaklarının korunmasına ve refahının muhafaza edilmesine yönelik kritik bir unsur olduğu göz önünde bulundurulduğunda, verinin etkin kullanımına ilişkin çalışmaların hızlı bir şekilde planlanması ve tamamlanması daha da önemli bir hal almaktadır. Veri her ne kadar Mısır'lı tüccarların ve çiftçilerin yıllık satış ve mahsul miktarlarının kayıtlarını tuttukları parşömenler ve tabletlerden beridir tarihin her döneminde hayatımızda önemli bir karar alma aracı görevi görmüş olsa bile, gelişmeye devam eden ve günümüzde etkisini her zamankinden daha sert tecrübe ettiğimiz bilişim sistemlerinin varlığıyla; hacmi giderek artan, kullanımı hızlanan ve günden güne daha kritik bir rol üstlenen verinin geleneksel yöntemlerle yönetilmesi imkansız bir hale gelmiştir.

Verinin savunma alanındaki kullanımı da şüphesiz tarihin her alanında önemli görülmüştür. Özellikle I. Dünya Savaşı sonrasında zayıf düşen devletler, bu zorlu dönemin arkasından alevlenmiş olan II. Dünya Savaşı'nda, sahip oldukları kıt kaynakların muharebeye ilişkin operasyonel süreçlerdeki kullanım kararlarını doğru alabilmek için; bu karar alımları asker ve teçhizat sayıları, üretim hacimleri, ekonomik unsurlar, lojistik parametreleri gibi çeşitli verilerle kurgulanan matematiksel modellere dayandırmışlardır. Yöneylem Araştırması (Operations Research) alanının temelini atan bu matematiksel modeller, günümüzde artık işlem hacmi artmış olan modern bilgisayarlar tarafından çok daha etkin bir şekilde oluşturulmakta ve kullanılmaktadır.

Günümüzde ise artık askeri operasyonlardan sorumlu karar mercileri, gerekli bilgileri bilgisayar tabanlı gelişmiş sistemler vasıtasıyla elde etmektedirler. Artan, çeşitlenen, farklı yapılara bürünen, hızlanan ve giderek daha bileşik süreçlerle kullanılmak zorunda kalınan verilerin işlenebilmesi ve anlamlandırılabilmesi için elimizde daha güçlü, daha gelişmiş donanımlar; verinin analitiğini daha etkin ve hatasız gerçekleştirebilmek ve daha anlamlı bilgiler çıkarabilmek için daha kompleks algoritmalar ve insanın hata payını süreç denklemlerinden kaldırabilmek ve verimliliği artırabilmek için ortaya konan otomasyon sistemlerimiz bulunmaktadır. Yapay Zeka kavramıyla artık bilgisayar sistemleri yalnızca cevap veren (responsible) yapıdan sıyrılarak; Makine Öğrenmesi, Yapay Sinir Ağları, Derin Öğrenme gibi kavramlarla kendi girdisini kendi oluşturabilen, yani daha derin katmanlarla tekrar kullanılabilir anlamlar üretebilen yapılar olmaya yönelmektedir.

Halihazırda bir değişim içerisinde bulunan savunma unsurları, veriye ilişkin tüm bu unsurların çatısı konumunda bulunan veri uzayı kavramına ilişkin her türlü değişiklikten de etkilenmektedir. Devletlerin savunma ve muharebe stratejileri, yenilikçi tüm dijital unsurları içermek zorunda olunan bir yapıya bürünmektedir. Artık gelişmiş veri işleme teknolojilerinin hayatımıza getirdiği tüm etkiler; modern askeri harekat planlamalarından ordu modernizasyon stratejilerine, siber savaş tekniklerinden insansız hava araçlarının kullanımına kadar birçok gelişmeyi de tetiklemiştir. Savaşların hızları giderek artan bir yapıya bürünmektedir ve insan beyni bu duruma bağlı olarak giderek artmaya devam eden bunca veri hacmini işlemeye muktedir değildir. Bu sebepten ötürü bu veri hacmini doğru şekilde işleyebilecek ve karar verme aşamalarını otomatize edecek sistemleri geliştirmek çok önemlidir. Bu kompleks ve korkutucu derecede hızlı değişim fırtınasının içerisinde, yolunu bulabilmek için uygun bir

kılavuz ve stratejiyi oluşturamayan devletler, yaşanan gelişmelerin içerisinde kaybolarak kendilerini savunma ve muharebe alanlarında kaçınılmaz bir şekilde yenilgiyi kabullenmiş bir pozisyon içerisine sokacaklardır.

12.1 Savunma Alanında Verinin Önemi Ve Temel Veri Kategorileri

Verinin her şeyden önce, yeni bir anlayışın eseri olarak, bir değer (kıymet) olarak algılanması ve sorumluluğunun alınması önemli bir girdi noktasıdır. Bu anlayışın getirisi; verinin yönetimine ilişkin usul ve esasların doğru şekilde tahsis edilmesi ve karar alma faaliyetlerinin ve ortaya konacak her türlü eylemin, kullanışlı bilgiye dönüştürülen verinin sağladığı iç görülere dayanarak gerçekleştirilmesinin sağlanmasıdır. Bu anlayış, savunma alanına ilişkin olarak da rekabetçi ortamda stratejik karar alımların isabet seviyesini artıracak ve avantaj kazanılmasını sağlayacaktır. Ortaya konacak olan bu denli stratejik bir bakış açısı, savunma alanına ilişkin olarak liderliği, yönetişimi (governance) ve hesap verilebilirliği de ihtiva etmektedir. Bu bakış açısının işletilebilmesi için her şeyden önce uygun usul ve esasların belirlenmesi, yani verinin yönetimine ilişkin gerekli politikaların oluşturulması ve bu çerçeve dahilinde gerekli geliştirme adımlarının uygulanması gerekmektedir. Halihazırda verinin yönetimine ilişkin olarak ortaya konan, dünya çapında ve ülkemizde de ortaya konmuş bir takım politika ve strateji belgeleri, savunma alanına spesifik olarak odaklansın veya odaklanmasın, bu alanda da büyük oranda geçerli olabilecek içerikler ihtiva edecektir. Savunma politikalarına endeksli olarak alan bazlı gerçekleştirilecek birtakım uygulamalar, verinin yönetiminin savunma alanı için özelleştirilmiş bir yapı halini almasını sağlayacaktır.

Savunma alanında, verinin kategorize edilmesi, bilgi yönetiminin optimize edilmesi ve doğru kararların alınması için kritik bir rol oynar. Savunma verisi genellikle aşağıdaki gibi kategorilere ayrılabilir:

- **İstihbarat Verisi:** Bu, tehditler, düşman kabiliyetleri ve hareketleri hakkında toplanan veridir. Elektronik istihbarat (ELINT), sinyal istihbaratı (SIGINT) ve görüntü istihbaratı (IMINT) gibi alt kategorilere sahip olabilir.
- **Operasyonel Veri:** Operasyonların yürütülmesi için gerekli olan bilgileri içerir. Bu, kuvvet konumları, hareket rotaları, lojistik bilgisi gibi bilgileri içerir.
- **Taktik Veri:** Belirli bir görev veya operasyon sırasında kullanılan veri türüdür. Bu, düşmanın olası hareketleri, hava durumu veya arazinin topoğrafik bilgileri gibi bilgileri içerebilir.
- **Eğitim ve Simülasyon Verisi:** Askeri eğitim ve simülasyonlar için kullanılan veridir. Bu, gerçekçi senaryolar oluşturmak için gereklidir.
- **Platform ve Sistem Verisi:** Bu kategori, askeri hava araçları, deniz araçları, kara araçları, silah sistemleri, siber sistemler, sensörler, radarlar ve diğer teknolojik ekipmanlarla ilgili veriyi içerir. Sistemin durumu, performansı, kullanılabilirliği ve diğer özellikleri bu kategoride değerlendirilir.
- **Lojistik ve Bakım Verisi:** Askeri ekipmanın bakımı, tamiri ve tedarikiyle ilgili veridir. Bu kategori, ekipmanın durumu, yedek parça envanteri ve tedarik zinciri bilgisi gibi bilgileri içerir.
- **Araştırma ve Geliştirme Verisi:** Savunma sektöründe yeni teknolojilerin ve sistemlerin araştırılması ve geliştirilmesi için kullanılır.
- **İnsan Kaynakları Verisi:** Askeri personel hakkında bilgileri içerir, bu eğitim, deneyim, uzmanlık alanları gibi bilgileri kapsar.

- **Harekât Sonrası Değerlendirme Verisi:** Bir operasyon veya görevin tamamlanmasının ardından yapılan analizler için toplanan veridir.
- **İletişim ve Ağ Verisi:** Savunma iletişim ağlarının performansı ve güvenliği hakkında bilgi sağlar.
- **Güvenlik ve Tehdit Verisi:** Askeri sistemlerin ve ağların güvenliği hakkında bilgi içerir. Bu, siber tehditler veya fiziksel güvenlik ihlalleri hakkında bilgileri kapsayabilir.
- **Çevresel Veri:** Operasyon alanlarındaki doğal faktörlere ilişkin bilgileri içerir. Bu, hava durumu, arazi bilgisi veya deniz durumu gibi bilgileri içerebilir.

12.2 Savunma Veri Uzayı Çalışmalarındaki Temel İlkeler (ABD Örneği)

Savunma verileririnin güvenliği, gerek ulusal güvenliğin korunması, gerekse askeri operasyonların hassasiyeti açısından hayati bir rol oynamaktadır. Verinin doğru, hızlı ve güvenilir bir şekilde paylaşılması, stratejik avantajın yanı sıra askeri personelin güvenliği için de kritik öneme sahiptir. Veri paylaşımı diğer sektörlerden daha karmaşık ve hassas bir şekilde ele alınmalıdır. Bu bağlamda, Savunma Veri Uzayı çalışmalarında, veri paylaşımının hem stratejik avantajlarını optimize etmek hem de güvenlik risklerini minimize etmek için izlenmesi gereken temel ilkeler şu şekilde tanımlanabilir (US DoD Data Strategy Document, 2020):

- **Veri Stratejik Bir Varlıktır** – Savunma verileri yüksek ilgi gören bir veri grubudur, hem hızlı hem de kalıcı askeri avantaj sağlayacak şekilde kullanılmalıdır.
- **Veri Yönetişimi** – Verinin tüm yaşam döngüsü boyunca yönetilebilmesini sağlamak amacıyla, veri sorumluları, veri muhafızları ve veri yöneticileri gibi paydaşlar belirlenmelidir.
- **Veri Etiği** – Etik kurallar tanımlanmalıdır. Verinin nasıl toplandığı, kullanıldığı ve saklandığı ile ilgili olarak tüm düşünce ve eylemlerin ön saflarına etik konmalıdır.
- **Veri Toplama** – Verinin elektronik olarak toplanmasını oluşturma noktasında etkinleştirmeli ve bu verilerin soy ağacını her zaman korumalıdır.
- **Veri Erişimi ve Uygunluk** – Savunma verileri, uygun mekanizmalar aracılığıyla tüm yetkili kişi ve kuruluşların kullanımına sunulmalıdır.
- **Yapay Zeka Eğitimi için Veriler** – Yapay Zeka eğitimi ve algoritmik modeller için veri kümeleri giderek en değerli dijital varlıklar haline geliyor. Bu tür verileri yaşam döngüsü boyunca yönetmek için korumalı görünürlük ve veri egemenliğini önceleyen bir çerçeve oluşturmalıdır.
- **Amaca Uygun Veriler** – Veri toplama, paylaşma, kullanma, ve diğer sistemlerle engtegre olma noktasında her türlü ahlaki kaygı dikkatle değerlendirilmeli ve yanlış kullnım olasılığı ortadan kaldırılmaya çalışılmalıdır.
- **Yasa ve Yönetmeliklere Uyumun izlenebilmesi** – Bilgi yönetimi yaşam döngüsünü tasarlarken, verileri uygun şekilde güvence altına alan ve her türlü işlemin denetlenebilir şekilde kayıt altına alındığı çözümler uygulanmalıdır.

12.3 Savunma Veri Yönetimi ile ilişkili Hedefler

Savunma Bakanlığı Veri Stratejisinin temel ilkelerinden biri, verilerin bir BT varlığı değil, görevin kendisinin temel ve ayrılmaz bir parçası olduğunun anlaşılmasıdır. Veri her yerde bulunabilir. Silah platformları, bağlı (connected) cihazlar, sensörler, eğitim tesisleri, füze atış rampaları ve iş yazılımları gibi pek çok kaynaktan muazzam miktarda veri üretilmektedir. Bu verilerin toplanıp, yüksek kalitede, doğru, eksiksiz, zamanında, korumalı ve güvenilir olarak

kullanıma açılması kritik öneme sahiptir. Bu nedenle ABD Savunma Bakalığı aşağıdaki hedefleri belirlemiştir:

- **Görünürlük**: Kullanıcılar gerekli verileri bulabilmeli.
- **Erişilebilirlik:** Kullanıcılar verilere kullanım amacıyla ulaşabilmeli.
- **Anlaşılabilirlik:** Kullanıcılar, içeriği, bağlamı ve uygulanabilirliği tanımak için veriler ile ilişkili açıklamalara ulaşabilmeli.
- **Bağlantılılık:** Kullanıcılar, ulaştıkları veriyi tamamlayıcı diğer veri öğelerinden yaralanabilmeli.
- **Güvenilirlik**: Kullanıcılar, verilere tam anlamıyla güvenebilmeli.
- **Birlikte Çalışabilirlik**: Kullanıcılar ve veri sahipleri veriyi aynı anlam ve sunum dahilinde ele almalı.
- **Güvenlik:** Kullanıcılar, verilerin yetkisiz kullanım ve manipülasyona karşı korunduğunundan emin olmalı.

13 Sonuç

Kamu kurumlarında oldukça fazla miktarda veri üretilmektedir. Fakat kamuda üretilen bu verilerin analiz edilerek üretilen katma değer yeterli seviyede değildir. Kamu politikaları oluşturma sürecinde veri analizinden faydalanılması, kaynakların etkin ve verimli kullanılmasını sağlayacağı gibi vatandaş memnuniyetini de üst seviyeye çıkaracaktır.[105] Veri uzayı çalışmasının önemi bu noktada ortaya çıkmaktadır.

Veri uzayı çalışması sonucunda akan verilerden analizler yapılabilecek ve kamu yararına sonuçlar çıkarılabilecektir. Verinin analizinin faydası açıktır, fakat veri uzayını tek bir platformda toplayan, veri uzayı için geliştirilmiş özel bir yazılım henüz bulunmamaktadır. Avrupa Birliğinin bu yönde çabaları vardır ve geliştirilecek yazılım için bazı kriterler önerilmiştir.

AB tarafından önerilen veri uzayı yazılımı kriterleri aşağıdaki gibidir.[106]

- Uluslararası standartların desteklenmesi.
- Özel bir yazılım topluluğunun varlığı ve canlılığı. Bu dolaylı olarak bir yazılımın olgunluğunu gösterir ve örneğin şu şekilde ölçülebilir: teknik dokümantasyonun varlığı ve açıklığı, taahhüt sayısı, GitHub gibi sosyal kodlama platformlarında sorunlar ve hata düzeltmeleri, topluluk etkinliğinin organizasyonu, vb.
- Net katkı yönergelerinin, davranış kurallarının ve yazılım kod tabanının kalite kontrolü için mekanizmalar.
- Bakım kolaylığı ve teknik gelişme potansiyeli

Veri uzayının platformlarının gelişmesi sayesinde kamu yönetimi ile ilgilenen profesyoneller, siyasetçiler ve araştırmacılar; veri analizi, yapay zeka uygulamarından faydalanabilir hale gelecek ve bu verilerden sağlanan toplumsal fayda artacaktır. Türkiye'de de henüz, AB'de kurulmaya çalışılan veri uzayı yazılımı gibi bir yazılım geliştirilmemiştir. Türk Kamu Kurumlarının ihtiyaçlarına özel verilerin iş akışına, yetki seviyelerinde paylaşımına uygun bir veri uzayı yazılımı geliştirilmelidir. Bu yazılım veri analizi araçları ve makine öğrenmesi algoritmalarıyla desteklenmeli, oluşturulacak yapay zeka uygulamalarına sürekli veri sağlayabilen bir yapıda olmalıdır.

13.1 Hukuki Durum

Rekabet üstünlüğünün yönetilmesi noktasında verinin değerlendirilmesi bugünün dünyasında en etkin araç haline dönüştüğünden ülkesel, bölgesel ve küresel düzeyde rekabet unsurları açısından verinin öneminin dikkate alınması gerekmektedir. Veri yönetimi mevcut perspektiften daha geniş ele alınmalıdır. Veri yönetiminin bugün yalnızca bilişimsel ve ülke içi kamu hizmeti sunumu noktasında kapsamlandırıldığı görülmektedir. Ancak veri yönetişimi dünyada özellikle piyasa rekabeti ve uluslararası ticaretin düzenlenmesi açısından etkin bir araç olarak kullanılmaktadır. Uluslararası ticarette piyasalarda, veri üzerinden (big data, veri transferi gibi) gelişen politikalar yine veri üzerinden getirilen yasaklamalar ve yaptırımlar ile dengelenmeye çalışılmaktadır. Bu nedenle veri yönetimi ulusal ve uluslararası düzeyde bilişim alanından çok daha geniş bir strateji geliştirme yoluyla yapılmalıdır.

[105] "Veri Madenciliği Teknikleri İle Türkiye'de Yaşam Memnuniyeti Düzeyleri Üzerine Bir Uygulama" Doktora Tezi
[106] JRC Scıence For Polıcy Report - European Data Spaces

Veri taşınabilirliğini gerek kişisel veri, gerek veri güvenliği, gerekse rekabet koşulları açısından daha detaylı ele alınmalı ve ilgili düzenlemeler, farklı sektörlerde de geliştirilmelidir. GDPR ile KVKK arasındaki "rıza", "açık rıza" ve "aydınlatma yükümlülüğü" tanımları arasındaki teorik ve pratik farklılıklar giderilmelidir. Veri sorumlusuna, "açık rıza"nın alınması noktasında, ilgili kişiden her seferinde aydınlatma yapma yükümlülüğü ve bunun ispatının yüklenmesi yönündeki pratik sorunların çözümlenmesi yerinde olacaktır. Rızanın geri alınması hallerine ilişkin net bir düzenleme yapılmalıdır.

KVKK ile düzenlenen, kişisel verilerin yurtdışına aktarımına ilişkin düzenlemenin teorik ve pratik olarak işlevsel hale getirilmesi zorunludur. KVKK ile öngörülen kademeli düzenleme işlememekte; kişisel veriler, ilgili kişinin ancak açık rızası ile yurt dışına aktarılabilmekte, açık rızası yok ise aktarılamamaktadır. Halihazırda KVKK tarafından "yeterli korumanın bulunduğu ülkeler" belirlenmemiştir. Konu GDPR açısından ele alındığında önceliğin yeterlilik kararı, taahhüt, bağlayıcı kurallar gibi mekanizmalara verildiği görülmektedir. GDPR, bu hallerin olmaması durumunda diğer aktarım nedenlerine yüzünü dönmektedir. Bu noktada Türkiye'de de ya bu kademelendirme artırılarak ağırlık kanun ve diğer yasal düzenlemelerin GDPR'a uyumlanmasına verilmelidir, ya da Kurul tarafından halihazırdaki kanun ile kendilerine verilen yetki uyarınca ülke belirlemesinden başlamak üzere işlem yapılmalı ve veri aktarım sorununun çözülmesi açısından adımlar atılmalıdır.

Taahhütname ile aktarıma izin verilen vaka sayısı başvurulara nispeten oldukça düşük orandadır. Bunun da etkisi ile halihazırda Türk hukukunda taahhütname seçeneği ile de yurt dışına kişisel veri aktarımının gerçekleşmesi çok mümkün görünmemektedir. Veri aktarımının yarattığı sorunlar ise şu sonuçları doğurmaktadır:

- Öncelikle, "yeterli korumanın bulunduğu ülkeler" belirlemesi ve taahhütleşme yapılmadığında, Türk hukuku açısından yurtdışına kişisel veri aktarımının tek yolu olarak ilgili kişinin açık rızası yolu kalmaktadır. Yalnızca açık rızaya dayalı bir süreç ise ilk olarak pratik açıdan sorun, iş yükü olarak ise özel sektöre yüklenmektedir.
- Rızaya dayalı işlemeden söz edildiği noktada, rızanın geri alınması ("withdrawal of consent") sorunu doğmaktadır. Örneğin açık rıza ile kişisel verileri yurtdışına aktaran bir veri sorumlusu, ilgili kişi, hiçbir gerekçe göstermesine gerek olmaksızın rızasını geri aldığını bildirirse ne olacaktır? Bunun takibi ve vakitlice gereğinin yapılması, açık rıza alınması yükümlülüklerinin doğrudan bir sonucu olarak yine işletmenin üzerine bir yük ve sorumluluk olarak gelmektedir.
- Bu noktada, Kurul, yeterli korumanın bulunduğu ülkeleri belirlememişken ve ne zaman belirleneceği konusunda da bir muğlaklık söz konusu iken ve aynı zamanda rıza ile aktarımın getirdiği pratik ve hukuki sorunlar halihazırda mevcut iken tek ara çözüm, en azından sektörel piyasaların büyük aktörlerinin taahhütname yoluyla veri aktarımını sağlamaları olmalıdır, demek yanlış olmayacaktır.
- Ayrıca bu süreçleri zorlaştırmak, bilhassa başat sektörlerde, fiilen tekel yaratılması sonucunu doğurma potansiyelini de içermektedir. Dolayısıyla taahhüt ve izinlerle ara süreçler yaratılması orta ve küçük düzey aktörlerin de uluslararası ticarete dahilini kolaylaştıracaktır.
- Ayrıca veri aktarımının zorlaşması, pek çok veri sorumlusunun, ihlal gerçekleşene veyahut rızayı dikkate almadan "yakalanana" kadar usulsüzce işlemi sürdürmesi sonucunu da uygulamada doğurmakta, kuralları ve kararları etkisiz kılmaktadır ki, burada mutlaka uluslararası çok büyük hacimli bir ticaretin söz konusu olmasına da

gerek yoktur. Özellikle herkesin kullandığı uluslararası e-posta sunucularının, web sitesi alt yapılarının, mesajlaşma sistemlerinin, web servislerinin veri merkezlerinin yurtdışında olduğu ve bunlar üzerinden yapılan her türlü iş ve işlemlerin de yurtdışı aktarıma girdiği düşünüldüğünde sürecin zorlaştırmasının sistemi durmaya veya sorumlular ve ilgililerce "gittiği yere kadar" (ihlal ederek) kullanıma zorlayacağı da açıktır.

Verilerin silinmesi, imha edilmesi, yok edilmesi, anonim hale getirilmesi kavramları ile ilgili terimsel karmaşaların KVKK ve Türk Ceza Kanunu gibi diğer kanunlar ile bağlantılı olacak biçimde giderilmesi gerekmektedir.

KVKK'nin istisna kapsamı da md. 28 ile düzenlenmiştir. Burada da pek çok kamu hizmetinin ve kamu kuruluşunun KVKK kapsamı dışında tutulduğu, yani kişisel verilerin korunması ile ilgili düzenlemelere tabi olmadıkları görülmektedir. Bunun sonuçlarından biri özel sektörün zamanla, kamuyla verisini paylaşmak istememeye doğru yönelecek olmasıdır. Kendisine yüklenen her türlü hukuki, mail, idari, cezai ve ticari sorumluluğa karşılık sorumluluğu olmayan bir kamuyla veri paylaşımına girmek, kişiler arasında bir eşitsizlik ve dengesizlik duygusu yaratacaktır. GDPR kural ve uygulamalarında ise kamu kurumlarının sorumluluk kapsamında oldukları ve ihlale sebep olmaları halinde kurumlarca yaptırıma tabi tutuldukları görülmektedir.

Özel nitelikli kişisel verilere ilişkin sınıflandırmalar hem Türk kanunlarının kendi içinde, hem de GDPR tanımları ile uyumlandırılmalıdır.

Verilerin kamu kurumlarınca (birbirleri ile paylaşılırken) yeniden kullanımı (re-use) konusunda Avrupa Birliği Veri Yönetişim Yasası (EU Data Governance Act) hükümlerine sağlanabilecek uyumlar üzerine çalışılması yerinde olacaktır.

Privacy by Design (Tasarım Gereği Gizlilik) ve Privacy by Default (Varsayılan Olarak Gizlilik) sayesinde daha işin başında en sıkı "önce gizlilik" prensibiyle hareket etmenin ve gizlilik ve veri güvenliği ayarlarını en baştan sıkı biçimde yapmanın sağlanması; hem privacy by design'ın hem de privacy by default'un potansiyel risk değerlendirmesi ve potansiyel risklerin en aza indirilmesi açısından dikkate alınması, temel bir politika haline gelmelidir.

Veri alanının genişlemesi ve karmaşıklaşması, KVKK (Kişisel Verilerin Korunması Kanunu) ve GDPR (Genel Veri Koruma Yönetmeliği) gibi veri koruma yasalarının uygulanmasını daha da zorlaştırmaktadır. Bu durum hem bireylerin gizliliğinin koruması hem de işletmelerin yasalara uyumunun sağlanması açısından önemli sorunlara yol açabilir. Bu nedenle, veri uzayının KVKK ve GDPR hükümlerine uygun hale getirilmesi için etkin stratejilere ihtiyaç duyulmaktadır. Bu hususta izlenilebilecek yolları 7 kısımda toplamamız mümkün olacaktır:

- **Bilinçlendirme ve Eğitim**: Veri koruma yasalarının uygulanması, tüm organizasyonda bilinçlendirme ve eğitim gerektirir. İlgililer, KVKK ve GDPR hükümlerinin ne olduğunu, bu hükümlerin işlerine nasıl etki ettiğini ve hangi adımları atmaları gerektiğini anlamalıdır.
- **Veri Haritalandırması**: Veri uzayının genişlemesi, veri haritalandırmasını zorunlu hale getirir. Hangi verilerin toplandığını, nerede saklandığını, kimlerin erişim hakkına sahip olduğunu ve bu verilerin nasıl kullanıldığını bilmek, KVKK ve GDPR hükümlerine uyum sağlamada hayati öneme sahiptir.

- **Risk Değerlendirmesi**: Veri koruma yasalarına uyum, potansiyel risklerin değerlendirilmesini ve yönetilmesini gerektirir. Bu, hangi veri işleme faaliyetlerinin yüksek risk taşıdığını belirlemeyi ve bu riskleri nasıl azaltacağınızı belirlemeyi içerir.
- **Veri Minimizasyonu**: KVKK ve GDPR, gereksiz veri toplamayı ve saklamayı sınırlar. Bu nedenle, sadece gerçekten ihtiyaç duyulan verilerin toplanması ve işlenmesi, veri minimizasyonu ilkesine uyum sağlar.
- **Bireylerin Haklarının Korunması**: KVKK ve GDPR, bireylere verileri üzerinde belirli haklar vermektedir. Erişim hakkı, düzeltme hakkı, unutulma hakkı vb. bunlara örnek teşkil etmektedir. Bu hakların korunması ve bireylerin bu hakları etkin bir şekilde kullanabilmesi için birtakım mekanizmaların oluşturulması gerekmektedir.
- **Veri Koruma Görevlisi Atanması**: Büyük ve karmaşık veri uzayları olan organizasyonlar, bir Veri Koruma Görevlisi (Data Protection Officer, DPO) atamalıdır. Veri Koruma Görevlisi'nin görevi, veri koruma yasalarına uyumun sürekli olarak sağlanmasını denetlemek ve gerekli uygulamaları yönetmektir.
- **Veri İhlallerine Hazırlıklı Olma**: Veri ihlalleri hem KVKK hem de GDPR açısından ciddi sonuçlara yol açabilmektedir. Bu nedenle, veri ihlallerine karşı önleyici önlemler alınması ve bir veri ihlali durumunda ne yapılacağını belirleyen bir planın bulunması büyük önem arz etmektedir.

13.2 Yönetişim

Günümüzün dijital çağında, veri yönetimi ve paylaşımı, kurumlar için büyük bir önem arz ediyor. Bu alanlarda belirlenen politika ve standartlar, iş süreçlerinin etkinliğini artırırken, aynı zamanda veri güvenliği ve uyumluluk açısından da kritik bir rol oynamaktadır. Veri yönetişim politikasının tanımlanması, bu sürecin temel adımıdır. Bu politika, bir organizasyonun veri varlıklarını nasıl yöneteceğini ve koruyacağını belirler. Veri toplama, depolama, erişim ve kullanım süreçleri bu politika çerçevesinde düzenlenir. Ayrıca, bu politika kapsamında, veri yönetiminden sorumlu kurumlar da belirlenir. Örneğin, IT departmanı veri altyapısını yönetirken, finans departmanı mali verilerin korunmasından sorumlu olabilir. Bu şekilde, süreçlerin belirli bir düzene oturması sağlanır.

Bununla birlikte, belirlenen politikanın etkin bir şekilde uygulanabilmesi için standartların oluşturulması şarttır. Bu standartlar, veri yönetimi sürecinin nasıl işleyeceğini belirler. Veri düzenlemeleri, saklama politikaları ve güvenlik standartları gibi unsurlar bu standartların içinde yer alır. Bu sayede, veri bütünlüğü ve güvenliği sağlanmış olur. Ayrıca, veri paylaşımlarında mümkün olduğu sürece, ortak veri paylaşım lisansları kullanılmalıdır. Ulusal Standart Lisans Modelleri oluşturularak, paylaşılan verilerin kullanımı ve korunması standartlaştırılmalıdır. Bunu sağlamanın bir diğer önemli unsuru da Veri Sözlüğüdür. Organizasyonların kullandığı terimlerin, tanımların ve kısaltmaların bir araya getirildiği bu kaynak ile özellikle kurumlar arasında veri paylaşımı standartlaştırılmış olacaktır.

Veri yönetişimine ilişkin hedefler ve kurumların bu süreçte elde etmek istediği sonuçları tanımlanmalıdır. Örneğin, veri analiz süreçlerinin hızlandırılması veya veri tabanlı karar almanın geliştirilmesi gibi hedefler belirlenebilir. Bu hedefler, organizasyonun veri yönetimi sürecindeki başarı ölçütlerini belirler.

Kamu kurumları, veri uzayı bilincini artırmak ve uzman insan kaynağını artırmak için çeşitli eğitim programlarına yatırım yapmalıdır. Kamu kurumlarında görevli yönetici ve çalışanların veri uzayı yönetimine ilişkin standartları bilmesi ve uygulaması, veri güvenliği ve bütünlüğünün sağlanması için kritik önemdedir. Bu alanda uzman insan kaynağını artırılmalıdır. Orta ve

yükseköğretim ile mesleki eğitimin veri yönetimi odaklı derslerle zenginleştirilmesi, gelecekteki uzmanların bu alanda daha donanımlı olmasını sağlayacaktır. Ayrıca, mesleki eğitim programları ve sertifikasyonlar, çalışanların veri uzayı konusundaki bilgi ve becerilerini artırmalarına yardımcı olur.

Son olarak, veri paylaşımı ve iş birliğini kolaylaştırarak dijital dönüşümü desteklemek, kurumların veri yönetimi süreçlerini uluslararası standartlara taşımak için GAIA-X oluşumuna üye olunmalıdır. GAIA-X, kurumların veri yönetimi süreçlerini uluslararası standartlara taşımalarını sağlayarak bir dizi avantaj sunar. GAIA-X tarafından sunulan veri paylaşımı çerçevesi ile farklı organizasyonlar arasında veri paylaşımı halinde verilerin gizliliği ve güvenliği, uluslararası standartlara uygun olarak korunması sağlanmaktadır. Üstelik, GAIA-X'in uluslararası bir oluşum olması, kurumların uluslararası düzeyde rekabetçi olmalarını sağlar. Komşumuz olan Avrupa Birliği ülkeleriyle yürütülen ticari faaliyetlerde bu çerçeve önem arz ettiğinden, GAIA-X'e üye olmak, ayrıca GAIA-X çerçevesinin ön şartlarından biri olan GDPR ile tam uyumlu olmak koşulları sağlanmış olmalıdır. Halihazırda KVKK ile GDPR arasında tam uyum sağlanmamış olması, uluslararası ticarette Dijital Pazarda rekabet etmenin önünde engel teşkil etmektedir.

13.3 Etkileşim

Veri yönetimi ve paylaşımı, toplumun hızlı ve sürdürülebilir kalkınması için vazgeçilmez bir hale gelmiştir. Bu süreçte, kamu, özel sektör ve akademi arasındaki işbirliği, veri uzayının etkili bir şekilde yönetilmesi için temel bir mekanizma olarak öne çıkmaktadır. Ayrıca, birçok kurumun sunmuş olduğu açık verilerin bir araya getirilmesi için bir portal oluşturulmalıdır. Bu portal sayesinde, farklı kurumların sunduğu veriler tek bir çatı altında toplanabilecektir.

Açık verinin sunulması, sadece verinin yayımlanması anlamına gelmez; aynı zamanda bu verilerin çerçevesi ve standartları da belirlenmelidir. Bu standartlar, verilerin tutarlılığını ve anlaşılırlığını artırarak, veri kullanımını kolaylaştırır. Ayrıca, veri uyumluluğunu sağlamak için belirlenen standartların sıkı bir şekilde takip edilmesi gerekir. Verilerin erişilebilirliğini artırmak için bir açık veri sözlüğü oluşturulmalıdır. Veri sözlüğü ile kullanıcıların ihtiyaçlarına göre verilere hızlı ve etkili bir şekilde erişim sağlaması garanti edilecektir.

Verinin birleştirilerek yapay zeka algoritmalarıyla işlenmesi, veri uzayının gerçek potansiyelini ortaya çıkaracaktır. Bu süreç, verinin değerini artırarak, toplumun faydasına sunar. Örneğin, sağlık verilerinin birleştirilerek analiz edilmesi, hastalıkların erken teşhisi ve tedavi yöntemlerinin geliştirilmesine olanak sağlayabilir.

Veri uzayı alt yapıları oluşturulurken, yenilikçi teknolojilerden faydalanılması da kritik bir öneme sahiptir. Özellikle blokzincir gibi güvenli ve şeffaf teknolojiler, veri güvenliğini sağlamak adına önemli bir rol oynar. Bu teknolojiler, veri manipülasyonunu engeller ve güvenilir bir ortam sağlar.

Diğer taraftan Türkiye'de devlet eliyle işlenen verilerimiz bir çok kurumda tekrar kayıt altına alınmaktadır. Bu verilerin ilgili tek bir kurum tarafından yönetilmesi, verinin tekilleştirilmesi, veri bütünlüğünün ve güvenliğinin sağlaması için önemli bir adım olacaktır. Bu yaklaşım ile veri akışlarının merkezileştirilmesi ve koordinasyonun artırılması gereklidir. Böylece, veri depolama, erişim ve güncelleme süreçleri daha etkili bir şekilde izlenebilir. Ayrıca, veri yönetimi politikalarının uygulanması ve denetlenmesi daha kolay hale gelir. Tek bir kurumun sorumluluğunda olan veri yönetimi, veri tabanlı karar alma süreçlerini de hızlandırarak

organizasyonun daha hızlı ve akılcı adımlar atmasını sağlar. Bu yaklaşım, veri güvenliği açısından da kritik bir rol oynar, çünkü veriye erişim ve güncelleme kontrolleri daha sıkı bir şekilde sağlanabilir.

13.4 Sektörel Değerlendirmeler

Finans: Finansal verilerin sağlıklı toplanması, kapsamı ve ilgili kesimlerle paylaşılması bir ülkenin rekabet seviyesini doğrudan etkiler. Bunun nedeni finansal piyasalar üzerinden mali kaynak ve kredi yaratılmasıdır: üretim ve tüketim faaliyetlerinin finansmanı sağlanarak ekonomik büyüme, istihdam ve kalkınmaya önemli katkıda bulunur. Veriler aracılığıyla değer yaratma yolları geliştirilmeli, bu alanda yatırım teşvik yatırım yapma teşvik edilmeli, tüketicilerin ve işletmelerin bu verilere erişiminin ve bunları kullanmasınının kolaylaştırılması amaçlanmalıdır.

Finansal veri teknolojinin başdöndürücü bir hızlı gelişimi devam ediyor. Bulut bilişim, yapay zeka, büyük veri analitiği ve blok zinciri gibi teknolojiler, finansal verilerin daha güvenli ve etkili bir şekilde yönetilmesine olanak tanıyacaktır.

Ayrıca, regülasyonlar da finansal veri uzayının gelişimini etkiliyor. Veri gizliliği ve güvenliği odak noktası haline geldiğinden piyasa düzenleyiciler, kamu kurumları ile finansal sektörde faaliyet gösteren şirketlerin bu konulara daha fazla önem vermesi yaşamsal bir zorunluluktur.

Finansal Veri finans dünyasının geleceğini şekillendiren bir kavram olduğundan,daha fazla veri, daha fazla analiz ve daha fazla dijitalleşme, finansın daha sürdürülebilir, hızlı ve daha akıllı hale gelmesine yol açacaktır. Bu nedenle, finansal kurumlar ve yatırımcılar için finansal verinin önemini anlamak ve bu dönüşümün bir parçası olmak kritik bir öneme sahiptir.

Dünyada olduğu gibi ülkemizde de Açık Bankacılık işlemleri ile müşterilerin bankacılık hizmetleri ile olan ilişkisini kökünden değiştiren ve hatta finansal hizmetlere erişimi kısıtlı olan insanları bu hizmetlerle buluşturan uygulamalarının sektörde büyük bir değişim yarattığı görülüyor. Gittikçe gelişen ve ivmelenen açık bankacılık endüstrisinin önümüzdeki dönemde daha da etkisini artıracağı görülmektedir.

Bu bağlamda, finansal kurumlara ait verilerin tek bir noktadan sunulmasının finansal piyasalara olumlu yönde katkı sağlayacaktır. Türkiye İstatistik Kurumu (TÜİK)'in işletimindeki İstatistik Veri Portali (https://data.tuik.gov.tr/) bu konuda iyi bir örnektir. Benzer şekilde, sektörler arası veri paylaşımı önem arz etmektedir.

Mobilite: Mobilite alanında veri uzayı, modern dünyanın iki anahtar kavramı olarak ön plana çıkarken, bu iki olgu arasındaki etkileşim, teknolojik ilerlemenin hızla devam ettiği gelecekte de derinleşecek gibi görünüyor. İlk olarak, veri uzayının sürekli genişlemesiyle birlikte mobil cihazlar, bireylerin ve kuruluşların bu veriye erişimini ve onunla etkileşimini daha anlamlı hale getirecek şekilde evrilecektir. 5G ve ilerleyen ağ teknolojileri, büyük veri setlerinin neredeyse gerçek zamanlı olarak işlenmesini ve analiz edilmesini sağlayarak, bireylerin ve işletmelerin daha bilinçli kararlar almasına olanak tanıyacaktır. Bu, özellikle akıllı şehirler, sağlık ve eğitim gibi sektörlerde mobilite ve veri uzayının entegrasyonunun önemini artıracaktır.

İkincil olarak, yapay zeka ve makine öğrenimi teknolojilerinin yükselmesi, mobil cihazların veri uzayında toplanan bilgileri daha etkin bir şekilde kullanmasına yardımcı olacaktır. Bu, kişiselleştirilmiş deneyimlerin, otomatik öğrenmenin ve tahminsel analizlerin ötesine geçerek, kullanıcılara tamamen bireysel ve dinamik deneyimler sunma potansiyeli taşımaktadır. Özetle,

mobilite ve veri uzayı arasındaki bu yakınlaşma, hem bireysel kullanıcılar için hem de geniş ölçekli kuruluşlar için daha önce eşi görülmemiş fırsatlar ve kapasiteler yaratacaktır.

Savunma: Dünyada savunma alanında verinin kullanımına ilişkin hazırlanmış olan, yönlendirici nitelikteki belgelerin sayısı pek de fazla değildir. Amerika Birleşik Devletleri Savunma Bakanlığı, İngiltere Savunma Bakanlığı ve Avustralya Savunma Bakanlığı; savunma alanında kamuya ilişkin veri yönetimi yol haritasının ne şekilde olması gerektiğine dair strateji belgeleri yayınlayan kısıtlı sayıdaki ülkelerdir. Son dönemlerde özellikle otonom askeri sistemlerle, dünyada ciddi bir farkındalık edinen ülkemizde de her ne kadar Ulusal Yapay Zeka Stratejisi, Bulut Bilişim Stratejisi (Mevcut Durum Analizi Raporu ve Ülkesel İnceleme Raporu) gibi veriye ilişkin stratejik belgeler hazırlanmış olsa da savunma odaklı bir çalışma henüz gerçekleştirilmemiştir.

Bunun da ötesinde ülke çapında farklı alanlarda veriye ilişkin genel bir farkındalık düzeyini oluşturabilmek, mevcut durumu değerlendirebilmek ve ülke çıkarları doğrultusunda gerekli aksiyonları alabilmek adına bir Ulusal Veri Stratejisi'nin oluşturulması, diğer spesifik odaklı belgelerin oluşturulması için de bir referans nokta ve çerçeve pozisyonu teşkil edecektir.

Ülkemizde, Milli Savunma Bakanlığı bünyesinde, bu tip bir stratejinin oluşturulması için çalışma gruplarının oluşturulması; kamu kurumlarından, özel sektörden, kar amacı gütmeyen organizasyonlardan ve akademik camiadan paydaşların belirlenerek bu çalışma gruplarına dahil edilmesi ve gerekli çalışmaların tahsis edilmesi gerekli görülmektedir. Bu atılımın gerçekleştirilebilmesi için her şeyden önce; tüm kurumlar için önerdiğimiz üzere Milli Savunma Bakanlığı bünyesinde, veri yönetimine ilişkin faaliyetlerin yürütüleceği bir başkanlığın kurulması uygun olacaktır. Bu başkanlık bilgi teknolojileri ve siber güvenlik alanında faaliyette olan diğer başkanlıklarla yakın temasta çalışmalı, bu yeni başkanlık çalışmaları ile oluşturulacak veriye dayalı stratejik usul ve esaslar çerçevesinde faaliyetlerin yürütülmesi sağlanmalıdır.