



**SOSYAL MEDYA ORTAMLARINDA VERİ MAHREMİYETİ DUYARLI
FARKINDALIK MODELLERİ GELİŞTİRME**

Salih Erdem EROL

**DOKTORA TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI**

**GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ**

TEMMUZ 2022

Salih Erdem EROL tarafından hazırlanan “SOSYAL MEDYA ORTAMLARINDA VERİ MAHREMİYETİ DUYARLI FARKINDALIK MODELLERİ GELİŞTİRME” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Adli Bilişim Ana Bilim Dalında DOKTORA TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Şeref SAĞIROĞLU

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

İkinci Danışman: Dr. M. Umut DEMİREZEN

Elektrik Elektronik Mühendisliği Ana Bilim Dalı, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Başkan: Prof. Dr. Olgun DEĞİRMENCİ

Hukuk Ana Bilim Dalı, TOBB Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Prof. Dr. Mustafa ALKAN

Elektrik Elektronik Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Prof. Dr. Adem KALINLI

Bilgisayar Mühendisliği Ana Bilim Dalı, ODTÜ

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Doç. Dr. Murat DENER

Bilgi Güvenliği Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Dr. Öğr. Üyesi Çağrı ŞAHİN

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Tez Savunma Tarihi: 27/07/2022

Jüri tarafından kabul edilen bu tezin Doktora Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

Prof. Dr. Aslıhan TÜFEKÇİ
Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İmza

Salih Erdem EROL

27/07/2022

SOSYAL MEDYA ORTAMLARINDA VERİ MAHREMİYETİ DUYARLI FARKINDALIK MODELLERİ GELİŞTİRME

(Doktora Tezi)

Salih Erdem EROL

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Temmuz 2022

ÖZET

Veri boyutunun büyüdüğü, kişisel olarak üretilen veri çeşitlerinin hızla arttığı ve veriden değer üretmenin yaygınlaştığı günümüz dijital dünyasında en büyük veri üretim ortamları sosyal medya ve çevrimiçi internet uygulamalarıdır. Bahse konu ortamlarda kullanıcıların profil verileri ve paylaşımları başta olmak üzere çok farklı kişisel, hassas ve nitelikli veriler ifşa edilmektedir. Kişisel veri ifşalarının önüne geçilmesi ve kullanıcı gizliliğinin sağlanması için en etkili yöntem farkındalığın artırılmasıdır. Bu nedenle, öncelikle sosyal medya ve gizlilik kavramı detaylı şekilde ele alınmış, sosyal medyada gizlilik farkındalığının ölçülmesine yönelik literatürde yer alan yöntemler ile sosyal veri kullanılarak gerçekleştirilen uygulama çalışmaları detaylı olarak incelenmiştir. Kullanıcı mahremiyet ve gizlilik farkındalığını tespit etmek için Twitter ortamından açık veriler toplanarak etiketlenmiş, Zemberek kütüphanesi kullanılarak doğal dil işleme süreçlerinden geçirilmiş, fastText yaklaşımı kullanılarak oluşturulan dil modelleri ile %75-91 arasında, BERT transformer yaklaşımları ile oluşturulan dil modellerinde %90-95 arasında doğruluk değerleri ile kişisel veri ifşa riski barındıran paylaşımlar tespit edilmiştir. Kullanıcıların farkındalığının tespiti ve artırılması amacıyla, kişisel veri ifşa riski olan paylaşımların otomatik olarak tespiti ve renklendirilerek kullanıcıya bir arayüz üzerinden sunulması ile kişisel profil analizine imkân sağlayan T-PII Hunter adı verilen bir sistem geliştirilmiştir. Çalışmanın; kullanıcı gizlilik/mahremiyet farkındalığı ve Türkçe kişisel veri ifşalarının tespitine yönelik gerçekleştirilen ilk çalışma olması, veri toplama süreçlerine referans oluşturacak şekilde Türkçe arama kelimelerinin ilk kez hazırlanması, kişilerin kanunlarla güvence altına alınmaya çalışılan tüm verilerine yönelik bütüncül bir yaklaşım sunması, 40.000 civarı Türkçe tivit (tweet) etiketlenmesi ile oluşturulan kişisel bilgi veri kümesinin araştırmacılara açık olarak yayımlanması, kabul edilebilir başarımlar yüzdelere sahip dil modellerinin oluşturulması ve kullanıcı farkındalığının analiz edilebilmesi için gerçek zamanlı bir sistem önerilmesi gibi yönleriyle literatüre katkı sağlayacağı; kişisel veri ifşalarının azaltılmasının adli bilişim vakaları arasında yer alan kimlik hırsızlığı, dijital dolandırıcılık, kişilik haklarına saldırı, kişisel verilerin ifşası gibi olayların önceden belirlenmesine ve önlem alınmasına katkılar sağlayacağı değerlendirilmektedir.

Bilim Kodu : 92401

Anahtar Kelimeler : Kişisel veri, sosyal veri, mahremiyet, BERT, fastText, model, sistem

Sayfa Adedi : 133

Danışman : Prof. Dr. Şeref SAĞIROĞLU

İkinci Danışman : Dr. M. Umut DEMİREZEN

DEVELOPING DATA PRIVACY SENSITIVE AWARENESS MODELS IN SOCIAL MEDIA ENVIRONMENTS

(Ph. D. Thesis)

Salih Erdem EROL

GAZİ UNIVERSITY
INFORMATICS INSTITUTE

July 2022

ABSTRACT

Social media and online internet applications are the biggest data production environments in today's digital world where the size of data is growing, the types of personally produced data are increasing rapidly and generating value from data is becoming widespread. In these environments, various personal, sensitive and qualified data, especially profile data and sharing of users, are disclosed. For this reason, first of all, the concept of social media and privacy was discussed in detail, and the methods in the literature for measuring privacy awareness in social media and application studies using social data were investigated in depth. In order to detect user privacy and privacy awareness, open data was collected from the Twitter environment and labelled. The obtained data were preprocessed through Zemberek natural language processing library, and with the language models created using fastText approach, tweets that have the risk of personal data disclosure were detected with accuracy values between 75-91% and between 90-95% in the language models created with the BERT transformer approaches. In order to measure and increase the privacy awareness of the users, the system called as T-PHI Hunter, which allows personal profile analysis, was developed, and an interface was created to display the shares with the risk of personal data disclosure by coloring them. It is considered that this study will contribute to the literature in terms of being the first study in Turkish language to identify personal data disclosures, determining Turkish search words as a reference to data collection processes for personal data, applying a holistic approach to all data of individuals that are tried to be secured by law unlike the studies conducted on specific personal data frequently seen in the literature, publishing the personal information dataset created by tagging around 40 000 Turkish tweets, open to researchers, creating language models with acceptable success percentages, and proposing a real-time system to analyze user awareness. It is also thought that reduced disclosure of personal data can be used as a proactive measure to prevent many incidents such as identity theft, digital fraud, attack on personal rights, disclosure of personal data, which are among the forensic cases.

Science Code : 92401

Key Words : Personal data, social data, privacy, BERT, fastText, model, system

Page Number : 133

Supervisor : Prof. Dr. Şeref SAĞIROĞLU

Co-Supervisor : Dr. M. Umut DEMİREZEN

TEŞEKKÜR

Yüksek lisans eğitimine başladığım 2014 yılından bugüne kadar akademik, sosyal ve kültürel anlamda hayatıma yön veren, bilgisi, yaklaşımı ve pozitif enerjisi ile çalışma azmimi hep yüksekte tutan, özellikle doktora eğitimim süresince bu tezin belirlenmesi ve hazırlanması sürecinde değerli katkı ve yönlendirmeleriyle her zaman desteğini çok yakından hissettiğim, önerilerinden faydalandığım, danışman hocam Sayın Prof. Dr. Şeref SAĞIROĞLU'na, çalışmalarım boyunca zaman gözetmeksizin her türlü soruma anında cevap veren, bilgisi, tecrübesi ve yönlendirmeleri ile desteğini hep yanımda hissettiğim danışman hocam Sayın Dr. M.Umut DEMİREZEN'e, tez izleme komitemde yer alıp tüm çalışmalarım boyunca değerlendirme ve tavsiyeleriyle tezimin şekillenmesine katkı sağlayan değerli hocalarım Sayın Prof. Dr. Mustafa ALKAN ve Sayın Prof. Dr. Olgun DEĞİRMENCİ'ye, çalışmalarına ilişkin fikir alışverişi yaptığım ve veri etiketleme sürecinde yer alarak tezime katkıda bulunan arkadaşlarıma, doktora eğitimim süresince sabırla manevi desteğini esirgemeyen, zor günlerimde hep yanımda olan sevgili eşim Yasemin EROL'a, zaman zaman oyun ve park zamanlarını ertelemek zorunda kaldığım kızlarım Ece ve Begüm'e, maddi manevi her türlü destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli Anneme, Babama ve Kardeşime teşekkür ve şükranlarımı sunarım.

İÇİNDEKİLER

	Sayfa
ÖZET	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
İÇİNDEKİLER	vii
ÇİZELGELERİN LİSTESİ.....	ix
ŞEKİLLERİN LİSTESİ.....	xi
SİMGELER VE KISALTMALAR.....	xiv
1. GİRİŞ.....	1
2. MEVCUT ÇALIŞMALARIN İNCELENMESİ	9
2.1. Gizlilik, Mahremiyet ve Sosyal Ağ Kullanımına Kavramsal Bakış	9
2.2. Sosyal Ağlarda Mahremiyet Farkındalığına Yönelik Yapılan Çalışmalar	11
2.2.1. Metodoloji.....	12
2.2.2. Mevcut çalışmaların incelenmesi.....	12
2.2.3. Değerlendirmeler	17
2.3. Sosyal Ağ Verileri ile Gerçekleştirilen Uygulama Çalışmaları.....	19
2.3.1. Metodoloji.....	20
2.3.2. Çalışmaların incelenmesi ve konularına göre sınıflandırılması	21
2.3.3. Çalışmaların incelenmesi ve amaçlarına göre sınıflandırılması	35
2.3.4. Çalışmalarda karşılaşılan saha problemleri.....	39
2.3.5. Değerlendirmeler.....	42
3. MATERYAL VE METOT	45
3.1. Materyal	45
3.2. Metot	47

4. SOSYAL VERİ, VERİ SETLERİ, HAZIRLANMASI VE ANALİZLERİ	49
4.1. Sosyal Veri Kavramı ve Platformun Belirlenmesi.....	49
4.2. Veri Sözlüklerinin Oluşturulması ve Verinin Elde Edilmesi	53
4.2.1. Temel bilgiler	56
4.2.2. Siyasi görüş/düşünce	58
4.2.3. Dini görüş/inanç	60
4.2.4. Irk köken bilgileri.....	62
4.2.5. Cinsel yönelim	63
4.2.6. Ceza/Mahkûmiyet bilgileri	65
4.2.7. Sağlık bilgileri.....	66
4.2.8. Tüm kişisel bilgiler	68
4.3. Verinin Etiketlenmesi.....	70
4.4. Veri Ön İşleme	72
4.5. Test ve Eğitim Veri Setlerinin Hazırlanması	75
5. MODELLERİN OLUŞTURULMASI VE TEST EDİLMESİ	77
5.1. fastText.....	77
5.2. BERT (Bidirectional Encoder Representation from Transformer).....	92
6. GELİŞTİRİLEN GERÇEK ZAMANLI T-PII HUNTER SİSTEMİ	99
7. SONUÇ VE ÖNERİLER	115
KAYNAKLAR	121
ÖZGEÇMİŞ	133

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 1.1. Büyük ölçekli kişisel veri sızıntıları	1
Çizelge 2.1. Anahtar kelimeler ve veri tabanları	12
Çizelge 2.2. Sosyal ağlarda gizlilik/mahremiyet farkındalığına yönelik gerçekleştirilen çalışmaların karşılaştırılması	16
Çizelge 2.3. Anahtar kelimeler ve veri tabanları	20
Çizelge 2.4. Sosyal ağ verisi ile gerçekleştirilen uygulama çalışmalarının karşılaştırılması	31
Çizelge 4.1. Temel Bilgiler sınıfı için kullanılan arama kelimeleri.....	57
Çizelge 4.2. Siyasi Görüş/Düşünce sınıfı için kullanılan arama kelimeleri	59
Çizelge 4.3. Dini Görüş/İnanç sınıfı için kullanılan arama kelimeleri	61
Çizelge 4.4. Irk Köken Bilgisi sınıfı için kullanılan arama kelimeleri.....	62
Çizelge 4.5. Cinsel Yönelim sınıfı için kullanılan arama kelimeleri.....	64
Çizelge 4.6. Ceza/Mahkûmiyet sınıfı için kullanılan arama kelimeleri	65
Çizelge 4.7. Sağlık Bilgileri sınıfı için kullanılan arama kelimeleri.....	67
Çizelge 4.8. Tüm sınıflar için etiketli veri sayıları	69
Çizelge 4.9. Örnek etiketlenmiş tivitler	71
Çizelge 4.10. Zemberek-NLP modülleri.....	72
Çizelge 4.11. Veri ön işleme adımları örnek gösterim	74
Çizelge 5.1. Model eğitimlerinde kullanılan parametreler	80
Çizelge 5.2. En sık kullanılan performans metrikleri	81
Çizelge 5.3. Temel Bilgiler sınıfı model performansı	82
Çizelge 5.4. Siyasi Görüş/Düşünce sınıfı model performansı	83
Çizelge 5.5. Dini Görüş/İnanç sınıfı model performansı.....	84

Çizelge	Sayfa
Çizelge 5.6. Irk Köken Bilgileri sınıfı model performansı	85
Çizelge 5.7. Cinsel Yönelim sınıfı model performansı.....	86
Çizelge 5.8. Ceza/Mahkûmiyet Bilgileri sınıfı model performansı.....	87
Çizelge 5.9. Sağlık Bilgileri sınıfı model performansı	88
Çizelge 5.10. Tüm Bilgiler sınıfı model performansı	89
Çizelge 5.11. Modeller sıkıştırıldıktan sonra elde edilen sonuçlar	90
Çizelge 5.12. Tüm Bilgiler modeli ile elde edilen sonuçların kelime sayısı analizi	91
Çizelge 5.13. Model eğitimlerinde kullanılan parametreler	95
Çizelge 5.14. Tüm Bilgiler sınıfı model performansı (BERT)	96
Çizelge 6.1. Genel mod ile Tüm Bilgiler modeli için gerçek veri ile gerçekleştirilen örnek sınıflandırma sonuçları	106
Çizelge 6.2. fastText ve BERT modelleri performans metrikleri.....	111
Çizelge 6.3. İyelik modu ile yapılan sınıflandırmada düzeltilen hatalı tespitler	112
Çizelge 6.4. İyelik modu performans metrikleri	113

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 2.1. Metodoloji.....	20
Şekil 2.2. Çalışmaların konularına göre dağılımı	21
Şekil 2.3. Çalışmaların amaçlarına göre dağılımı.....	36
Şekil 2.4. Amaç tabanlı zaman skalası.....	36
Şekil 3.1. Çalışmada kullanılan materyal bilgileri.....	45
Şekil 3.2. Tez çalışma metodolojisi	47
Şekil 4.1. Sosyal veri kavramsal modeli.....	49
Şekil 4.2. Büyük veri yaşam döngüsü.....	51
Şekil 4.3. Mahremiyet çemberi.....	54
Şekil 4.4. Temel bilgiler veri seti kelime bulutu.....	58
Şekil 4.5. Siyasi görüş/düşünce veri seti kelime bulutu.....	60
Şekil 4.6. Dini görüş/inanç veri seti kelime bulutu.....	62
Şekil 4.7. Irk köken bilgisi veri seti kelime bulutu	63
Şekil 4.8. Cinsel yönelim veri seti kelime bulutu	64
Şekil 4.9. Ceza/Mahkûmiyet bilgileri veri seti kelime bulutu	66
Şekil 4.10. Sağlık bilgileri veri seti kelime bulutu.....	68
Şekil 4.11. Tüm verilerden elde edilen veri seti kelime bulutu	69
Şekil 4.12. Stratified Sampling yöntemi örnek gösterim.....	76
Şekil 5.1. CBOW ve Skip-gram model mimarisi	78
Şekil 5.2. Yapay sinir ağı temelli word2vec mimarisi.....	78
Şekil 5.3. CBOW ve Skip-gram modelleri örneği	79
Şekil 5.4. Temel bilgiler sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları	82

Şekil	Sayfa
Şekil 5.5. Siyasi görüş/düşünce sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları.....	83
Şekil 5.6. Dini görüş/inanç sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları ..	84
Şekil 5.7. Irk köken bilgisi sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları...	85
Şekil 5.8. Cinsel yönelim sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları.....	86
Şekil 5.9. Ceza/Mahkûmiyet sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları	87
Şekil 5.10. Sağlık bilgileri sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları ...	88
Şekil 5.11. Tüm kişisel bilgiler sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları.....	89
Şekil 5.12. Kelime sayılarına göre doğru ve hatalı tespit grafiği.....	92
Şekil 5.13. BERT için genel ön eğitim ve ince ayar işlemleri	93
Şekil 5.14. Transformer model mimarisi	94
Şekil 5.15. Karakter temizleme, karakter temizleme+durak kelime silme, karakter temizleme+normalizasyon, karakter temizleme+normalizasyon+durak kelime silme uygulanan setlerle elde edilen karmaşıklık matrisleri (Sırasıyla)	97
Şekil 5.16. Karakter temizleme, karakter temizleme+durak kelime silme, karakter temizleme+normalizasyon, karakter temizleme+normalizasyon+durak kelime silme uygulanan setlerle elde edilen karmaşıklık matrisleri (Sırasıyla)	97
Şekil 5.17. Karakter temizleme, karakter temizleme+durak kelime silme, karakter temizleme+normalizasyon, karakter temizleme+normalizasyon+durak kelime silme uygulanan setlerle elde edilen karmaşıklık matrisleri (Sırasıyla)	97
Şekil 6.1. T-P11 Hunter uygulaması akış diyagramı	100
Şekil 6.2. T-P11 Hunter ana ekran görüntüsü	101
Şekil 6.3. Analiz süreci ekran görüntüsü	102
Şekil 6.4. Tivit analiz ekranı	103
Şekil 6.5. İfşa histogram ekranı	104
Şekil 6.6. Tivit histogram ekranı.....	104
Şekil 6.7. Güvenirlik analizi ekranı	105

Şekil	Sayfa
Şekil 6.8. Twitter clone üzerinde ifşa riski içerdiği tespit edilen paylaşımların gösterilmesi	106
Şekil 6.9. fastText ve BERT modeli karmaşıklık matrisleri	112



SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
API	Application Programming Interface (Uygulama Programlama Arayüzü)
BERT	Bidirectional Encoder Representation from Transformer (Çift Yönlü Transformatör Kodlayıcı Temsilleri)
BOW	Bag of Words (Kelime Çantası)
EWOM	Elektronik Word of Mouth (Elektronik Ağızdan Ağıza İletişim)
GDPR	General Data Protection Regulation (Genel Veri Koruma Tüzüğü)
IoT	Internet of Things (Nesnelerin İnterneti)
K-NN	K-Nearest Neighbour (K-En Yakın Komşu)
KVKK	Kişisel Verilerin Korunması Kanunu
KVKK_U	Kişisel Verilerin Korunması Kanunu ile Uyumlu
KVKK_UD	Kişisel Verilerin Korunması Kanunu ile Uyumlu Değil
PII	Personal Identifiable Information (Kişisel Tanımlanabilir Bilgiler)
SVM	Support Vector Machine (Destek Vektör Makinesi)
TF-IDF	Term Frequency-Inverse Document Frequency (Kelime Frekansı-Ters Doküman Frekansı)
T-PII	Turkish Personal Identifiable Information (Türkçe Kişisel Tanımlanabilir Bilgiler)
TODIM	Iterative Multi Criteria Decision Making (Etkileşimli ve Çok Kriterli Karar Verme)
YSA	Yapay Sinir Ağı

1. GİRİŞ

Sosyal ağların hayatın bir parçası haline gelmesi ile beraber etkileşim ve gizlilik arasında karar verilmesi zor bir ikilem ortaya çıkmıştır. Aslında kullanıcılar yıllardır güvenlik kaygılarından uzak ve gelecekte nelerle karşılaşabileceğinden habersiz bir şekilde sosyal ağların ana aktörü olarak birçok önemli verisini paylaşmaktadır. Günümüzde artan farkındalık, kanuni altyapıların tartışılmaya ve oluşturulmaya başlaması ve gizlilik ihlallerinin devletler seviyesinde kontrol edilip cezalandırılır hale gelmesi ile beraber kullanıcı tarafında da verilerinin akıbetine ilişkin soru işaretleri oluşmaya başlamıştır. Ancak kullanıcıların verilerinin kendileri tarafından ifşa edildikten sonraki süreçte nasıl işlemlerden geçtiğinin kestirilememesi kaygıların giderek yükselmesine sebep olmaktadır.

Özellikle son zamanlarda ortaya çıkan ve gündem oluşturan bazı veri sızıntıları sosyal medya üzerinden yapılan paylaşımların, beğenilerin, içeriklerin güvenliği yönünde büyük bir soru işareti oluşturmuştur. Bazı büyük ölçekli kişisel verilerin sızıntısına yönelik olaylar Çizelge 1.1’de sunulmuştur.

Çizelge 1.1. Büyük ölçekli kişisel veri sızıntıları

Veri Sızıntısı Olayı	Yıl	Veri Boyutu	Açıklama
Cambridge Analitica [1]	2018	87 Milyon	Cambridge Analytica şirketi Facebook kullanıcıların kişisel verilerini uygunsuz bir şekilde edinmiştir.
First American Financial Corp. [2]	2019	885 Milyon	Müşterilerin 2003 yılından itibaren kaydedilen banka hesap numaraları, durumları, mortgage ve vergi kayıtlarını içeren veriler sızdırılmıştır.
UniCredit [2]	2019	3 Milyon	İtalyan bankanın müşterilerinin isimleri, telefon numaraları, e-posta adresleri ve hatta ikametlerini içeren bilgiler sızdırılmıştır.
Poshmark [2]	2019	50 Milyon	Amerika merkezli moda firmasının müşterilerin isimleri, cinsiyet bilgileri, e-posta adresleri, kullanıcı adları ve hatta beden bilgileri ile giyim tercihlerini içeren bilgiler yetkisiz bir uygulama tarafından sızdırılmıştır.
CafePress [2]	2019	23 Milyon	Kişiselleştirilmiş t-shirt üreten firmanın müşterilerinin isim, kullanıcı adı, e-posta adresleri, parolaları ve ikamet adresleri sızdırılmıştır.

Çizelge 1.1’de de görüleceği üzere kullanıcılara ait birçok veri günümüzde ekonomik kaygılar, siber saldırılar ya da yapılan yanlışlıklar nedeniyle kolayca ifşa edilebilmektedir. Her ne kadar devletler söz konusu veri sızıntılarından dolayı yaptırım uygulasa da her geçen gün daha fazla verinin ortaya saçıldığı görülmektedir. Cambridge Analytica skandalında Facebook 5 Milyar Dolar cezaya çarptırılmış, firma söz konusu cezayı ödeyeceğini açıklamıştır. Buradan hareketle önemsiz, gündelik hayatımızın bir parçası olarak sosyal medya ortamlarında yaptığımız paylaşımlar, beğeniler, üye olunan gruplar gibi tüm işlemlerin veriyi doğru şekilde kullanabilenler için çok büyük öneme sahip olduğu görülmektedir.

Gelişen teknoloji, kolaylaşan erişim imkânları ile birlikte sosyal ağ ortamları insanların günlük hayatının vazgeçilmez bir parçası haline gelmiştir. Bu ilgi ve gelişmeler bir yandan sosyal ağ platformlarının tür ve sayılarını arttırırken bir yandan da kullanıcı sayılarının her geçen gün artmasını da sağlamaktadır. Son 5 yılda iki kat artışla 4,2 milyar aktif kullanıcı sayısına ulaşılan sosyal medya ortamlarında harcanan zamanın 1,5 kat artarak günlük ortalama 2 saat 25 dakikaya ulaştığı günümüz dijital yaşantısında kişisel veri içeren sosyal verinin güvenliği de ciddi bir problem olarak ortaya çıkmaktadır [3].

Kişilerin sosyal ağ ortamlarına karşı sahip olduğu güven eksikliğine rağmen sosyalleşme içgüdüsündeki baskınlık kişilerin sosyal ağlarda gizlilik ve mahremiyetlerini ihlal etmelerine sebep olabilecek paylaşımlar yapmasına ortam hazırlamaktadır. Yapılan araştırmada sosyal ağ kullanıcılarının %56,3’ü interneti kullanma amacının arkadaşları ve ailesi ile iletişim içerisinde olmak olduğunu belirtmeleri de sosyalleşme içgüdüsünün önemini göstermektedir [3]. Mobil kullanım oranlarının Türkiye için %70,5’lere dünya ortalaması olarak %55,7’lere ulaşması [5] sayesinde kişilerin sosyal ağ ortamlarında devamlı çevrimiçi olması ve kişisel farkındalık eksikliği gibi nedenlerle de sosyal ağlarda kişisel veri ifşaları sıklıkla yaşanır hale gelmiştir.

Kişiler açısından konu dikkatle incelendiğinde gündelik yaşantıları içerisinde üreticisi pozisyonunda oldukları sosyal verinin öneminin farkında olmadıkları da görülmektedir. Kullanıcılar tarafından sosyal ağ ortamları kişiye özel olarak görülmesine rağmen mahrem verilerini bu platformlarda açık olarak paylaşmaktadırlar [6]. Ancak, kişilerin aksine saldırganlar bu konuda yüksek motivasyon ve farkındalığa sahiptir. IBM tarafından 2021 yılında veri sızıntılarının maliyetlerine ilişkin yayınlanan raporda müşterilerin tanımlanabilir

kişisel bilgilerinin (PII) çalınmasına yönelik saldırıların tüm çalışmaya konu saldırılar içerisinde %44'lük bir yer tuttuğu, kişisel verinin çalınması ya da kaybedilmesi durumunda her bir kayıt için 180 \$ değer ile en maliyetli veri türü olduğu ortaya konulmuştur [7].

Veri sızıntılarının sektörlere maliyeti değerlendirildiğinde ise 2021 yılında ilk 5 sırayı; sağlık, finans, ilaç, teknoloji ve enerjinin aldığı görülmektedir [7]. Sağlık sektöründe ortalama maliyetin 2020 yılında 7,13 milyon Dolar iken 2021 yılında %29,5'lik bir artışla 9,23 milyon Dolara çıktığı [7], 2021 yılında bir önceki yıla göre sağlık verilerine yönelik gerçekleştirilen saldırılarda %10,9'luk bir artış olduğu belirtilmiştir [8].

Büyük veri uygulamalarının artması ve yaygınlaşması ile beraber sosyal medya ortamlarında paylaşılan kişisel verilerin önemi her geçen gün daha da artmaktadır. Aramalar, bağlantılar, beğeniler, paylaşımlar ve sanal ortamlarda gerçekleştirilen hareketler başta her türlü bilgiye erişmek isteyen istihbarat örgütleri, gücünü arttırmak isteyen devletler olmak üzere başkalarının özel hayatlarını takip etme takıntısı olan kişiler, kar amaçlı firmalar ve saldırganlar tarafından kullanılabilir [9].

Verinin kullanılmasının yanı sıra sanal ortamda gerçekleşen başarılı saldırı ve veri sızıntılarının ortalama, spam e-postalar, bir linkin açılması, bir dokümanın açılması ve bilgilerin iletilmemesi gereken kişilere iletilmesinden kaynaklandığı belirtilmektedir [10]. Kişisel verilerin ifşa edilmesinde doğrudan sosyal medya ortamlarında yaptığı paylaşımlar ya da sosyal mühendislik saldırılarının kurbanı olarak ana aktör insandır. Gemalto firmasının elde ettiği veri sızıntı istatistikleri konunun ne kadar ciddi olduğunu ortaya koymaktadır. Yapılan çalışma neticesinde 2018 yılının ilk çeyreğinde 3 353 172 708 verinin sızdırıldığı, her gün 18 525 816 adet, her saniye 214 adet verinin kaybedildiği ya da çalındığı tespit edilmiştir [11].

Sızdırılan veriler içerisinde özellikle kişilerin gizlilik ve mahremiyetini ihlal edecek veriler büyük öneme sahiptir. Bu kapsamdaki verilere yönelik yaşanan olayların temel nedenleri genel olarak 4 ana başlık altında toplanmıştır. Bunlar; kullanıcıların zayıf bilgi güvenliği farkındalığı, kişisel bilgilerin güvenliğine ilişkin kanun ve düzenlemelerdeki eksiklikler, büyük verinin güvenliğine yönelik teknolojik gelişmelerin yavaşlığı ve kazanç motivasyonu olarak belirtilmiştir [12].

Birey birey incelendiğinde kişiler, bireylerin bileşkesi incelendiğinde toplumsal bilgilere erişilmesine imkân sağlayan (Amerika seçimleri, Arap Baharı gibi) kişisel verilerin bir kez ifşa edildikten sonra kontrolü oldukça zor olup her geçen gün daha da zorlaşmaktadır. Bu nedenle kullanıcıların sosyalleşme içgüdüsünün de engellenmeden sosyal ortamlarda kendini ifade edebileceği bir denge kurularak kişisel verilerine yönelik doğru kararları verebilmesi sağlanmalıdır. Bu da ancak farkındalığın artırılması ile gerçekleştirilebilecektir.

Problem

Doğrudan kullanıcının farkındalık eksikliği, sosyal ağında yer alan arkadaşlarının farkındalık eksikliği, saldırganlar ya da politikadaki eksiklikler gibi birçok farklı etkenin kullanıcı verilerinin gizliliğinin ihlaline sebep olduğu görülmektedir. Bu durum, kullanıcının gizlilik attığı verilerini bir kez paylaştıktan sonra veri üzerindeki kontrolünü kaybettiğini açıkça ortaya koymaktadır. Paylaşılan kadar özel olan bir bilgi paylaşıldığı andan itibaren kamusallaşmakta ilgisiz kişilerin erişimine de açılmaktadır.

2021 yılında yapılan araştırmaya göre veri sızıntılarının %85'inin insan faktöründen kaynaklandığı [13] da göz önüne alındığında veri sızıntılarının sadece teknolojik önlemlerle engellenemeyeceği açıktır. Kaldı ki kişisel veriler sadece kurumsal ortamlarda saklanmamakta kişiler tarafından sosyal ağ ortamları, bloglar gibi herkese açık platformlarda gizlilik ayarı yapılmadan paylaşılarak kamulaştırılmaktadır. Sosyal medya ortamlarında genel olarak kişilerin gizliliğinin ihlaline sebep olan verilerin;

- Kullanıcıların doğrudan paylaştığı veriler,
- Kullanıcının arkadaşları/tanıdıkları/takipçileri vb. tarafından kendisine ilişkin paylaşılan veriler,
- Üçüncü parti yazılımlar aracılığıyla kullanıcının haberi olmaksızın elde edilen veriler,
- Sosyal medya güvenlik tedbirlerinin eksikliğinden dolayı (ya da öyle lanse etmeleri) verilerin sızdırılması ile ortaya saçılan veriler,
- Kişilerin sosyal medya ortamı kullanımına yönelik farkındalık eksikliklerinden dolayı elde edilen veriler,

- Sosyal medya ortamlarının kullanıcı sözleşmelerinin okunmaması ya da kabul etmek dışında farklı bir alternatif sunulmaması nedeniyle kullanıcı tarafından bilinçsizce teslim edilen verilerden oluştuğu görülmektedir.

Veri sızıntıları, kişisel veri ifşaları, zorunlu kılınan kullanıcı sözleşmeleri, genişleyen siber saldırı yüzeyi, teknolojik güvenlik çözümlerinin yüksek maliyetli ve saldırılara göre daha yavaş ilerlemesi gibi sebeplerle günümüzde kişisel verilerin güvenliği oldukça zor sağlanmaktadır. Ancak, tüm bu olumsuz etkenlerin etkileri farkındalık sayesinde azaltılabilmektedir. Tüm belirtilen hususlar göz önüne alındığında kullanıcılar tarafından gerçekleştirilen kişisel veri ifşalarına yönelik çözülmesi gereken 3 temel problem tespit edilmiştir. Bunlar;

- Kişilerin sosyal medya ortamlarında bilinçsizce yaptıkları paylaşımların kişisel verilerin ifşasına sebep olması ve kişilerin gizliliğini geri dönüşü olmayacak şekilde ortadan kaldırması,
- Kişilerin gizlilik farkındalık seviyesinin artırılabilmesi için kişinin mevcut durumunun ölçülmesine imkân sağlayacak kriter, model ve yöntem bulunmaması ve
- Kişilerin bilinçsizce yaptığı kişisel veri ifşaları ile gizlilik farkındalık seviyesini görüntüleyebilecekleri, geri besleme alabilecekleri etkileşimli bir platform bulunmamasıdır.

Tezin Amacı, Kapsamı ve Önemi

Bu tez çalışması kapsamında, 4 ana başlık altında toplanan verilerin ifşasına sebep olan temel nedenlerden [12] “zayıf bilgi güvenliği farkındalığı” başlığına ve “kullanıcıların doğrudan paylaştığı” veriler (metin verisi) üzerinden bilinçsizce gerçekleştirilen gizlilik ve mahremiyet ihlallerine ilişkin kullanıcı farkındalığı kaynaklı problemlere çözüm üretilmesi hedeflenmektedir.

Söz konusu ihlallerin azaltılabilmesi ve kullanıcıların farkındalığının artırılabilmesi maksadıyla;

- Kişilerin gizlilik farkındalık seviyelerinin kendi paylaşımları üzerinden büyük veri yaklaşımı ile ölçülmesi,
- Gizlilik farkındalık seviyesinin büyük veri ile ölçümüne ilişkin kriter, model ve yöntemin ortaya konulması ile
- Gizlilik farkındalık seviyesini olumlu/olumsuz etkileyen paylaşımlarının davranış değişikliği yaratmak amacıyla bir uygulama üzerinden gösterilmesi ve bu sayede farkındalığın arttırılması amaçlanmaktadır.

Tez çalışmasının amaçları doğrultusunda kullanıcıların Twitter ortamında yaptıkları metin paylaşımlarının incelenmesi hedeflenmiştir. Twitter ortamından elde edilen metinlerin metin işleme yöntemleri ile analiz edilerek kişisel veri ifşa riski barındıran paylaşımların tespit edilmesi ve çalışma kapsamında geliştirilen farkındalık ekranı üzerinden kullanıcıya geri besleme sağlayacak şekilde sunulması hedeflenmektedir.

Yapılan literatür incelemesinde (Bkz. Çizelge 2.2) sosyal medya ortamları ülkemizde son yıllarda birçok teze konu olmuş olmakla beraber sosyal medya ortamlarında gizlilik farkındalığının büyük veri ile ölçülmesine yönelik bir çalışma bulunmamaktadır. Gizlilik farkındalığının arttırılmasının başta veri sızıntıları olmak üzere, kişisel verilerin ifşasının önüne geçilmesine dolayısı ile de adli bilişim vakaları arasında yer alan kimlik hırsızlığı, dijital dolandırıcılık, kişilik haklarına saldırı gibi birçok olayın önüne geçilmesini sağlayacak proaktif bir önlem olarak kullanılabileceği değerlendirilmektedir.

Gerçekleştirilecek çalışmanın;

- Tamamı çalışma kapsamında elde edilerek işlenmiş özgün Türkçe veriler ile gerçekleştirilecek olması ve çalışma kapsamında hazırlanan veri setleri/veri sözlüklerinin bu alanda gerçekleştirilecek çalışmalarda kullanılmak üzere sunulması,
- Kişilerin gizlilik/mahremiyet farkındalığının analizi ve skorlanabilmesine altlık sağlayacak kriter, model ve yöntem ortaya konulması,
- Sosyal ağlarda mahremiyet ve gizlilik farkındalığının literatürde yer alan ölçüm yöntemlerine ilave olarak sosyal veri ile analiz edilmesi,

- Sonuçların görselleştirilmesi ile farkındalığın artırılmasına yönelik etkileşimli uygulama içermesi,
- Kişisel Verilerin Korunması Kanunu’nda yer alan hususları referans alacak şekilde büyük veri ile kişisel veri ifşalarının sınıflandırılmasına yönelik Türkçe veriler ile gerçekleştirilen ilk çalışma olması ve
- Kapsamlı bir alan araştırması içermesi,

yönleriyle literatüre önemli bir katkı sağlayacağı değerlendirilmektedir.

Sınırlılıklar

Gerçekleştirilen tez çalışması Twitter ortamından elde edilen Türkçe veriler üzerinden gerçekleştirilmektedir. Twitter platformunda yapılan paylaşımların karakter sayısının yarattığı kısıtlamayı en düşük seviyeye indirebilmek için paylaşımlar genişletilmiş (extended) modda 280 karakter olacak şekilde elde edilmiştir. Ancak, kullanıcı alışkanlıkları ve Twitter platformunun kullanım şekli de göz önüne alındığında verilerin birçoğu çok az sayıda kelimeden oluşmaktadır. Hatta veri ön işleme adımlarından geçirildiğinde hiç kelime içermeyen paylaşımlar oluşabilmektedir. Kelime sayısının azlığı metin sınıflandırma işlemlerinde başarıyı olumsuz etkileyebilecek faktörlerden birisidir.

Kısa paylaşımların yanı sıra Twitter ortamında kullanıcıların dönemselsel olarak popüler olan jargonları kullanması, yazım ve imla kurallarına dikkat edilmemesi, çeşitli emoji, etiket ve hashtagler kullanarak bazı duygu ve düşüncelerini ifade etmesi gibi hususlar da paylaşımların anlaşılmasını ve buna bağlı olarak da yüksek doğrulukla sınıflandırılmasını güçleştirmektedir. Ayrıca, alaycı ifadeler, hatalı yazımlar, dolaylı anlatımlar, metin dışı materyaller birleştirildiğinde (Ses, resim vb.) gerçek anlamı ortaya çıkan paylaşımlar da yapılan çalışmada elde edilecek sonuçları kısıtlayan faktörler olarak karşımıza çıkmaktadır.

Twitter platformu ve kullanıcı davranışlarının dışında Türkçe dil özelliklerinin beraberinde getirdiği yapısal zorluklar da çalışmalarda başarıyı düşüren bir diğer faktör olarak görülmektedir. Her ne kadar bu dezavantajlı durumların ortadan kaldırılmasına yönelik doğal dil işleme adımları uygulanmış olsa da kök alma, kelime düzeltme gibi doğal dil işleme süreçlerinde de hata payları bulunmaktadır.

Twitter üzerinden veri çekilmesine yönelik olarak belirli kelimeler ile son 7 gün içerisinde yapılan paylaşımlar, çalışma kapsamında kullanılan API anahtarları ile kullanıcı profilindeki son 200 paylaşım elde edilebilmektedir. Söz konusu kısıtlar sınıflandırma için oluşturulan veri setinde bazı sınıflarda yeterli bilgi etiketlenmesini zorlaştırmakta ve kullanıcı profillerinin analizinde 200'den daha fazla paylaşımı bulunan kişilerin tüm paylaşımlarının değerlendirilmesine engel olmaktadır. Her ne kadar farklı tür ve seviyelerde veriye erişime imkân sağlayan API anahtarları bulunsa da Twitter platformu anahtar dağıtımı konusunda son yıllarda daha katı davranmakta olup daha yüksek sayıda tivit (tweet) elde edilmesine yönelik başvurularımıza olumsuz dönüş alınmıştır.

Tez çalışması kapsamında elde edilen tivitlerin doğruluğu ve kişiye gerçekten aitliği konusunda herhangi bir belirleme yapılamadığından tivitler kullanıcının paylaşımı yapma amacı ve paylaşımın doğruluğundan ari olarak paylaşıldığı şekli ile değerlendirilmiştir.

2. MEVCUT ÇALIŞMALARIN İNCELENMESİ

Tez çalışmasının bu bölümünde öncelikle gizlilik ve mahremiyet konuları kavramsal olarak ele alınmış, sosyal ağ kullanımı ile söz konusu kavramlar arasında bir ilişki olup olmadığı araştırılmıştır. Sonrasında sosyal ağlarda mahremiyet farkındalığının ölçülmesine yönelik literatürde yer alan çalışmalar incelenerek literatürün bu alanda güçlü ve zayıf yönleri ortaya konulmuştur. Literatüre başvuru bir diğer konu ise sosyal büyük veri kullanılarak gerçekleştirilen uygulama çalışmalarıdır. Tez çalışması kapsamında gerçekleştirilecek uygulamaya ışık tutması açısından sosyal büyük veri kullanılarak son 5 yıl içerisinde gerçekleştirilmiş uygulama çalışmaları araştırma sahası, araştırma hedefi, veri kaynağı, veri boyutu, metot ve araçlar ile amaç yönlerinden incelenmiştir.

2.1. Gizlilik, Mahremiyet ve Sosyal Ağ Kullanımına Kavramsal Bakış

Publilius'un "Güven ruh gibidir, bir kere ayrıldı mı bedenden asla geri dönmez." sözü aslında gizlilik için de aynı şekilde kullanılabilir. Gizlilik bir kez ihlal edildiğinde günümüz internet ve bilgi ortamının da özelliklerini göz önüne aldığımızda geri dönüşü olmayacak şekilde kişisel bilgilerin ifşasına sebep olacaktır. Bugünün elektronik ortamında eğlence, iş, sosyalleşme gibi nedenlerle ifşa edilen kişisel verilerin kullanılmasına ve depolanmasına ilişkin Kim? Ne? Nasıl? Niçin? Nerede? Ne zaman? (5N1K) sorularına net bir cevap bulunamamaktadır. Günümüzde farkındalığın geçmiş yıllara göre artması ile beraber bu sorular da en azından sorulmaya sorgulanmaya başlamıştır. Ancak, kullanıcıların toplumsal bir dünyada görünür olma içgüdüğü tüm dezavantajlarına rağmen özellikle sosyal medya ortamlarında bulunma ve etkin olmasına yol açmaktadır.

Kullanıcılar açısından değerlendirildiğinde bilgilerini en çok paylaştıkları ancak en az güven duydukları ortamın sosyal medya ortamları olduğu ortaya konulmuştur. Yapılan çalışmada [4] %56 ile en az sosyal medya en az güvenilen ortam olmuş, Hükümetlere %66, Google/Yahoo gibi büyük firmalara %68, bankalara %76 oranında güven duyulurken en çok güven %87 ile doktorlara duyulmuştur. Kullanıcıların en az güven duyduğu ancak en çok veriyi açık olarak paylaştığı sosyal medya ortamları da dâhil olmak üzere internette paylaştıkları verilerden haberdar olmadıkları görülmüştür. Yapılan çalışmada [4] kullanıcıların sadece %27'si sosyal ağ arkadaş listesini, %25'i konum bilgilerini, %18'i

iletiřim gemiřini (Chat tarihesi vb.), %17'si IP adresini ve %13' web arama gemiřini paylařtıklarından haberdar oldukları grlmřtr. Gene aynı alıřmada arpıcı sonulardan biri de farklı lkelerde yařayan bireyler farklı bilgilere verdikleri deėerin farklı olmasıdır. rneėin Almanya'da en deėerli veri olarak saėlık bilgileri karřımıza ıkarken Amerika'da kimlik bilgileri olarak karřımıza ıkmıřtır.

Kiřilerin en az gven duydukları ortam olmasına raėmen baskın iėdleri ve sosyalleřme istediėi nedeniyle yer aldıėı sosyal aė platformları gnmzde gizlilik kaygılarını da hızla arttırmaktadır. İlk olarak 1890 yılında ortaya konulan gizlilik kavramı bařlangıta duygu, grř ve dřnceleri iermekten [14] gnmzde birok farklı bileřeni kapsar hale gelmiřtir. Alan Westin'e gre gizlilik, toplumdaki bireylere ve gruplara zerkliėin korunması ile rol yapmaktan kurtulma, z deėerlendirme iin zaman ve korumalı iletiřim saėlar [15]. "Mahremiyet bir zerliktir ve yalnız bırakılma hakkını kapsar. Mahremiyet bizimle ilgili bilgiyi kontrol hakkını ierir. Mahremiyet hakkı, sırlarımızı gizleme hakkını ve onları yalnızca zel konuřmalarda paylařmayı kapsar" [16]. Bahse konu tanımlamalardan da grleceėi gibi yalnızca bilgilerin paylařılması deėil kiřilerin bilgilerini paylařma ya da paylařmama konusundaki seici kontrol de gizlilik kavramının ierisinde deėerlendirilmektedir.

Gizliliėe iliřkin literatrde kavramsal anlamda yapılan alıřmalardan birinde Clarke gizliliėi kiřisel iletiřim gizliliėi ve veri gizliliėi olarak iki boyutta ele almıřtır. Kiřisel iletiřim gizliliėi kiřinin iletiřiminin izlendiėi ya da elde edildiėine ynelik tereddt yařamadan evresi ile eřitli ortamlar zerinden iletiřim kurma hakkı olarak tanımlanmaktadır. Veri gizliliėi ise kiřisel verinin gvenliėinin garanti edilmesi ve veri bařkalarının eriřimine aıldı ise kiřisin verisi ve verisinin kullanımına iliřkin bazı kontrolleri saėlayabilmesi olarak aıklanmıřtır [10]. Genel olarak deėerlendirildiėinde byk veri analizlerinin yaygınlařması ile bilgi gizliliėi zerinde etkilerinin de artacaėı aık olarak grlebilir. Byk veri ile sosyal medya uygulamaları zerinde kullanıcılar arasındaki konuřmaların toplanması kiřisel iletiřimin gizliliėini ihlal edebilir. Dahası, kiři kiřisel bilgilerinin toplandıėından haberdar deėil ve kullanımına iliřkin bir kontrol yoksa kiřisel veri gizliliėinin ihlaline de yol amaktadır [17].

Esasen kullanıcılar sosyal medya ortamlarında bir mesaj yayınlayacaėında bu eylemi gerekleřtirmenin fayda ve risklerini deėerlendirmektedir. Ancak karar verme srecinin

karmaşık olması ve genelde kullanıcıların yayınlayacakları mesajın kimler tarafından görüntüleneceği ya da nasıl kullanacağına ilişkin net bir bilgiye sahip olmaması nedeniyle doğru kararları verme konusunda sıkıntılar yaşanmaktadır. Tüm bunlara ilave olarak özellikle gençler için karşılaşılabilecekleri tüm durumların öngörülmesi çok zordur [18].

Tüm durumların öngörülememesine yönelik bir örnek ile durumu açıklamak gerekirse kullanıcıların paylaşım yaptıkları konum bilgileri toplanarak yapılan bir araştırmada [19], yapılan tüm paylaşımların %40'ının kullanıcıların evinden yapıldığı ve %80'inin kullanıcıların en sık ziyaret ettiği 10 yerde yapıldığı tespit edilmiştir. Çalışmada elde edilen bu bilgi doğrultusunda 30 kullanıcının 3 hafta boyunca yaptığı paylaşımlar takip edilerek kullanıcıların %85'inin ev konum bilgileri ve en çok ziyaret ettikleri 5 yer doğru olarak tespit edilmiştir. Kullanıcı sadece sıradan konulara ilişkin paylaşım yaptığını düşünürken aslında ev konumunu da ifşa etmektedir.

Her ne kadar kişisel bilgilerin sosyal medya ortamlarında ifşa edilmesi olumsuz gibi görünse de Zhang ve Sun [20], kişisel bilgilerin sosyal medya ortamlarında paylaşılmasını “iki ucu keskin kılıç” olarak betimlemiştir. Kullanıcılar tarafından bilgilerin açık hale getirilmesi genel anlamda sosyalleşme isteğinin giderilmesi için bir zorunluluk olarak değerlendirilirken, kullanıcıların bilgilerinin toplanması ile sanal ortamda spam, oltalama gibi zararlı saldırıların gerçekleşmesinin önünü açılmaktadır.

Gizlilik ve mahremiyet insan özgürlüğünün en temelinde yer almaktadır. Bu hakkın ihlali özgürlüğün de ihlal edilmesine dolayısı ile kontrol duygusunun insan üzerindeki olumsuz etkisinin artmasına sebep olabilecektir. Sosyal ağların yarattığı dönüşüm ile beraber kullanıcı alışkanlıkları, gizliliğe bakış açısı ve öncelikler de değişmektedir. Kullanıcıların kolay kolay kapılarını açmadıkları evleri, aileleri, kimseye söylemediği düşünceleri bile artık çoğunu hiç tanımadığı kişiler tarafından erişilebilir bir hale gelmiştir.

2.2. Sosyal Ağlarda Mahremiyet Farkındalığına Yönelik Yapılan Çalışmalar

Sosyal ağlarda gizlilik ve mahremiyet farkındalığına yönelik çalışmaların son yıllarda çıkan veri sızıntılarının maliyetleri, kullanıcılarda oluşturduğu güvensizlik, marka değerlerinin zarar görmesi ve ülke güvenliğine yönelik tehditleri içermesi sebebiyle arttığı görülmektedir. Çok farklı disiplinlerin ilgisini çeken sosyal ağlar ve medya ortamlarına ilişkin adli bilişimin

yanı sıra psikoloji, gazetecilik, iletişim, pazarlama, işletme, bilgi güvenliği, bilgisayar bilimleri ve daha birçok farklı disiplin alanında çalışmalar gerçekleştirildiği görülmektedir. Bu bölümde sosyal ağlarda gizlilik ve mahremiyet farkındalığının ölçülmesine yönelik literatürde yer alan çalışmalar özetlenmiştir.

2.2.1. Metodoloji

Literatür incelemesi kapsamında ele alınacak çalışmalar Çizelge 2.1’de sunulan anahtar kelimeler ve yıl kriterleri doğrultusunda veri tabanlarında sorgulanarak tespit edilmiştir. Sorgulamalar sonucunda ortaya çıkan toplam 36 çalışma özet ve başlık bilgileri doğrultusunda inceleme kapsamında ele alınmıştır.

Çizelge 2.1. Anahtar kelimeler ve veri tabanları

Arama Terimleri	Veri Tabanı	Zaman Aralığı
KEY ("awareness" AND "social media") OR KEY ("awareness" AND "measurement") OR KEY ("awareness" AND "score") OR KEY ("privacy" AND "social media")	WOS (Web of Science), SCOPUS, IEEE, Science Direct	10 Yıl (Bazı hariç tutulan çalışmalar dışında)

Sosyal ağlarda mahremiyet farkındalığının ölçülmesine yönelik model ve yöntemlerin anlaşılması amacıyla gerçekleştirilen bu inceleme doğrultusunda öncelikle çalışmalar özetlenmiş, sonrasında kapsam, veri/kaynak, etkileşim ve açıklama başlıkları altında karşılaştırmalı olarak sunulmuştur. Yapılan değerlendirme ve analiz çalışmaları doğrultusunda aranan hedef verileri içeren 17 adet çalışmaya ilişkin hazırlanan özet tablo Çizelge 2.2’de sunulmuştur.

2.2.2. Mevcut çalışmaların incelenmesi

Sosyal ağlarda suç farkındalığına yönelik yapılan çalışmada [21], sosyal ağların kullanıcılar tarafından suç mecrası olarak nasıl kullanıldığı araştırılmış ve kullanıcıların bu konuya ilişkin farkındalığı tespit edilmeye çalışılmıştır. Bu amaçla çeşitli meslek gruplarından kullanıcılarla görüşmeler yapılarak betimsel analizler gerçekleştirilmiştir. Yapılan çalışma sonucunda kullanıcıların bu suçlara ilişkin yeterli farkındalığa sahip olmadıkları değerlendirilmiştir.

Sosyal ağlarda mahremiyetin sağlanabilmesi için yapılan bir çalışmada [22] herhangi bir paylaşım gerçekleştirilmeden önce söz konusu paylaşım içerisinde yer alan tarafların bilgilendirilerek müzakere edilmesi, onay alındığı takdirde yayınlanması amaçlanmıştır. Söz konusu çalışma kapsamında geliştirilen müzakere uygulaması ile mahremiyet ihlallerinin önüne geçilebileceği değerlendirilmiştir.

Sosyal ağlarda kullanıcıların paylaştığı tarihsel konum bilgilerinin incelenerek bir sonraki konumun tahmin edilmesinin amaçlandığı çalışmada [23] konum bilgileri ile insan hareketliliği 4 farklı model ile gerçekleştirilerek modeller arası başarımlar karşılaştırılmıştır. Söz konusu çalışmada Nokia Mobil Veri Yarışması tarafından sağlanan 80 kullanıcıya ait bir yıl boyunca toplanan konum bilgilerinden oluşan veri seti kullanılmıştır.

Sosyal ağlarda profil ve etkileşim alışkanlıkları üzerinden büyük 5 olarak adlandırılan kişilik özelliklerinin tespitine yönelik bir çalışma gerçekleştirilmiştir [24]. Söz konusu çalışma kapsamında kişilik özellikleri ile sosyal ağ kullanımı arasında korelasyon olduğu değerlendirilmiştir. Çalışma kapsamında myPersonality Project kapsamında sunulan veriler kullanılmış olup, verilerin 2018 yılından itibaren paylaşımı durdurulmuştur.

Devlet, pazarlama şirketleri ve bilgisayar korsanlarının kullanıcıların gizliliklerine yönelik ihlalleri basında çıkan haberler doğrultusunda ele alan çalışma kapsamında [16] kullanıcıların ihlallere yönelik düşüncelerini ve farkındalıklarını ölçmek amacıyla bir anket geliştirilmiştir. Çalışma sonucunda kullanıcıların farkındalıklarının yüksek olduğu değerlendirilmiş olsa da ihlallere rağmen davranışlarında değişim olmadığı tespit edilmiştir.

Sosyal ağlarda kullanıcıların açıklık analizinin akıllı bir sistem ile gerçekleştirilmesine yönelik hazırlanan bir tez çalışmasında [25] kullanıcılara yönelik gerçekleştirilen saldırılar 18 başlık altında sınıflandırılmış ve kullanıcılara bu başlıklara yönelik sorular hazırlanarak bir anket çalışması gerçekleştirilmiştir. Anket sonucunda elde edilen veriler sayısallaştırılarak tasarlanan YSA'nın eğitilmesi ve testinde kullanılmıştır. Yapılan çalışma sonucunda kullanıcıların söz konusu anketi doldurduklarında sosyal ağlarda saldırılara karşı seviyelerini belirleyebilecekleri ön görülmüştür.

Farklı sosyal ağ hesaplarında oluşturulan aynı kullanıcıya ait hesapların eşleştirilmesine yönelik gerçekleştirilen çalışmada [26] kullanıcıların yaşayabileceği gizlilik sorunları ortaya

konulmuştur. Veri madenciliği algoritmaları kullanılarak gerçekleştirilen çalışmada kullanıcı isimleri, durum güncellemeleri, gerçek isimler gibi niteliklerde yüksek oranda tespit edilmiş olup kullanıcıların farklı hesaplarda oluşturduğu ancak bilinmesini istemediği profillerin tespit edilebileceği değerlendirilmiştir.

Üniversite öğrencisi olan sosyal ağ kullanıcılarının mahremiyet algısına yönelik yapılan çalışmada [27], 18 üniversite öğrencisi ile mülakatlar gerçekleştirilmiştir. Çalışmada öğrencilerin mahremiyet algısı, sosyal ağ ortamını kamusal mı yoksa özel alan olarak mı gördükleri ve yurtdışından gelen öğrenciler ile Türkiye Cumhuriyeti vatandaşı olan öğrenciler arasında mahremiyet algısında bir farklılık olup olmadığı soruları araştırılmıştır.

Instagram sosyal ağ örneği üzerine yapılan çalışmada [28], Erciyes Üniversitesi'nde öğrenim gören 600 öğrenciye anket uygulaması yapılarak gelir, cinsiyet, kullanım süresi ve arkadaş sayılarının mahremiyet ihlalleri ile bir ilişkisi olup olmadığı araştırılmıştır. Özellikle gelir durumunun artması ile mahremiyet ifşalarının daha sık gerçekleştirildiği tespit edilmiştir.

Sosyal ağ ortamlarında yapılan paylaşımların İnsan Kaynakları yönetimi bağlamında kullanılıp kullanamayacağının araştırıldığı çalışmada [29], çalışmaya konu olan 47 kişinin son 50 paylaşımından kişilik özelliklerinin %79,57 oranında doğru tespit edildiği ortaya konulmuştur.

Twitter üzerinde toplanan veriler ile sosyal ağ profillemesi yapılması ve profillemeye ile kişilerin siyasi eğilimlerinin tahminlenmesi amaçlanan bu çalışmada [30], derin öğrenme kullanılarak %87.7'lik bir doğrulukla siyasi eğilimlerin tahmin edilebildiği belirtilmiştir. Verinin kısıtlanması için Türkiye'deki siyasetçiler, siyasetli ilişkili yazarların ve gazetecilerin hesapları kullanılarak büyük boyutlu bir ilişki matrisi oluşturulmuş, veriler Twitter üzerinden bot hesap ile 24 Haziran seçimleri öncesindeki 1 aylık süre boyunca toplanmıştır.

Kramer ve Schawel'in çalışmasında [31], insanların sosyal ağlarda memnuniyet ve gizlilik risklerini her zaman doğru değerlendirerek rasyonel kararlar veremediği belirtilmiştir. Aksine insanların rasyonel değerlendirmeleri engelleyen kanılara karşı da savunmasız olduğu, kullanıcıların kişisel ifşasının önüne geçebilmek için teknik gizlilik desteği

sağlanması ya da gizlilik okuryazarlığının arttırılması olarak en azından 2 yöntemin kullanılabileceği belirtilmiştir.

Genç kullanıcıların sosyal ağlarda gizlilik farkındalığının arttırılması maksadıyla [18], 42 kullanıcı ile PSEDIA adlı akademik çalışmalarda kullanılmak üzere oluşturulan sosyal ağda deneyimlenen çalışma sonucunda kullanıcıların davranışlarında önemli değişiklikler tespit edilmiştir. Kullanıcıların yapacağı paylaşımların hangi kullanıcılar tarafından görüntüleneceğinin görüntüleyecek kullanıcıların profil resimlerinin gösterilmesi ile, kaç kullanıcıya ulaşacağı ise sayıların belirtilmesi ile gerçekleştirilmiştir. Her iki ikazın da kullanıcı davranışlarında ciddi değişikliklere sebep olduğu ortaya konulmuştur.

Cep telefonu kullanıcılarının gizliliklerinin sağlanması ve farkındalıklarının arttırılması amacıyla gerçekleştirilen çalışmada [32], 3. parti yazılımların kullanıcıların haberi olmadan sağladığı erişimlerin yönetilmesi ve ikaz edilmesi amacıyla kullanılan AppOps adlı uygulama ile kullanıcıların davranışlarında ortaya çıkan değişimler araştırılmıştır. Katılımcıların %95'inin ilk haftanın sonunda izinleri gözden geçirerek yeniden değerlendirdiği, %58'inin ise izinlerde kısıtlamalar yaptığı tespit edilmiştir. Kullanıcı paylaşımlarının yanı sıra uygulamaların doğrudan topladığı bilgilerle tehlikenin boyutlarının büyüyebileceği açıkça görülmektedir.

eWOM (Ağızdan ağıza iletişim) yönteminin sosyal ağ ortamları üzerinde kullanılmasının bilgi güvenliği farkındalığının arttırılmasına etkilerinin araştırıldığı çalışmada [33], kullanıcının katılımı ile bir anket araştırması yapılmıştır. Söz konusu çalışma neticesinde eWOM'un bilgi paylaşımı konusunda olumlu etkileri olduğu, bilgi güvenliği farkındalığına ise farkındalığın bilgi, tutum ve davranış olarak 3 boyuttan oluşması nedeniyle doğrudan etkisi olmadığı, diğer 2 boyutun davranışa dönüşmesi daha uzun bir süreç olduğu için doğrudan gözlemlenemediği belirtilmiştir.

Çinlilerin gizlilik ile ilgili düşüncelerini araştırmak ve bu düşünceler doğrultusunda güvenlik önlemleri geliştirilmesi amaçlanan çalışmada [14], kullanıcılar cinsiyet olarak 2, yaşlara göre de 6 gruba ayrılmıştır. Yapılan çalışma neticesinde kadınların erkeklere göre gizlilik konusunda daha hassas oldukları ancak teknoloji kullanımındaki zayıflıktan dolayı uygun güvenlik ayarlarını gerçekleştiremedikleri, genel olarak tüm yaş gruplarının kişisel gizliliğin sağlanması konusunda yetersiz oldukları ortaya konulmuştur. Gizlilik konseptinin okul

çağından itibaren öğretilmesinin, gizliliğe yönelik yenilikçi girişimlerin desteklenmesinin ve gizliliği koruma yeteneklerine yönelik eğitimlerin sunulmasının alınabilecek önlemler olduğu belirtilmiştir.

Sosyal ağ ortamlarının kullanımı ve kişisel veri güvenliğine yönelik yapılan araştırmada [34], 300 kişiye anket gönderilerek genel olarak sosyal ağ kullanım amaçları, verilerinin ifşa olması ve sosyal ağ ortamlarının kullanıcı verilerini depolamasına yönelik düşüncelerinin ne olduğu araştırılmıştır. Çalışma sonucunda katılımcıların %41'inden fazlasının günlük hayatlarını sosyal ağ ortamlarında paylaşmaktan rahatsızlık duymadıkları, ancak istenmeyen durumlarla karşılaşmamak için kişisel verilerini korumaları gerektiği, bir kişi için kabul edilebilir bir riskin başkaları için kabul edilebilir olmayabileceği ve sosyal ağ ortamlarını sosyalleşme, bilgi ve iş için kullandıkları tespit edilmiştir.

Çizelge 2.2. Sosyal ağlarda gizlilik/mahremiyet farkındalığına yönelik gerçekleştirilen çalışmaların karşılaştırılması

Çalışma	Kapsam	Veri/Kaynak	Etkileşim	Açıklama
[21]	Meslek Grupları	Görüşme Tutanakları	-	Sosyal ağların suç mecrası olarak nasıl kullanıldığı ve kullanıcıların bu konuya ilişkin farkındalığı araştırılmıştır.
[22]	Sosyal ağ kullanıcıları	-	Var	Sosyal ağlarda paylaşılacak içeriğin geliştirilen uygulama yardımı ile taraflarla müzakere edilerek yayınlanması amaçlanmıştır.
[23]	Sosyal ağ kullanıcıları	Nokia Mobil Veri Yarışması tarafından sağlanan veri	-	Sosyal ağ ortamlarında paylaşılan konum bilgileri ile insan hareketliliği 4 farklı model ile gerçekleştirilerek modeller arası başarımlar karşılaştırılmıştır.
[24]	Sosyal ağ kullanıcıları	MyPersonality Project kapsamında sunulan veri	-	Sosyal ağlarda profil ve etkileşim alışkanlıkları üzerinden büyük 5 olarak adlandırılan kişilik özelliklerinin tespitine yönelik bir çalışma gerçekleştirilmiştir.
[16]	Sosyal ağ kullanıcıları	Basında yer alan haberler, Anket	-	Kullanıcıların ihlallere yönelik düşüncelerini öğrenmek ve farkındalıklarını ölçmek amacıyla bir anket geliştirilmiştir.
[25]	Sosyal ağ kullanıcıları	Anket	-	Sosyal ağlarda kullanıcılara yönelik gerçekleştirilen saldırılara karşı farkındalık seviyelerinin ölçülmesi amaçlanmıştır.
[26]	Sosyal ağ kullanıcıları	Twitter/ Facebook	-	Farklı sosyal ağ hesaplarında oluşturulan aynı kullanıcıya ait hesapların eşleştirilmesine yönelik yapılan çalışma ile kullanıcıların yaşayabileceği gizlilik sorunları ortaya konulmuştur.
[27]	Üniversite Öğrencileri	Görüşme	-	Türkiye ve yurtdışından gelen öğrencilerin gizlilik farkındalığı açısından farklılıkları olup olmadığı araştırılmıştır.
[28]	Üniversite Öğrencileri	Anket	-	Instagram örneği üzerine yoğunlaşılan çalışmada anket uygulaması yapılarak gelir, cinsiyet, kullanım süresi ve arkadaş sayılarının gizlilik ihlalleri ile bir ilişkisi olup olmadığı araştırılmıştır.

Çizelge 2.2. (devam) Sosyal ağlarda gizlilik/mahremiyet farkındalığına yönelik gerçekleştirilen çalışmaların karşılaştırılması

Çalışma	Kapsam	Veri/Kaynak	Etkileşim	Açıklama
[29]	Sosyal ağ kullanıcıları	Anket/ Twitter	-	Çalışmaya konu olan 47 kişinin son 50 paylaşımından kişilik özelliklerinin %79,57 oranında doğru tespit edildiği ortaya konulmuştur.
[30]	Sosyal ağ kullanıcıları	Twitter üzerinden bot hesap ile veriler toplanmıştır	-	Twitter üzerinde toplanan veriler ile sosyal ağ profillemesi yapılması ve profillemeye ile kişilerin siyasi eğilimlerinin tahminlenmesi amaçlanmış, derin öğrenme yöntemi ile %87.7'lik bir başarı sağlanmıştır.
[33]	Sosyal ağ kullanıcıları	Anket	-	eWOM (Ağızdan ağıza iletişim) yönteminin sosyal ağ ortamları üzerinde kullanılmasının bilgi güvenliği farkındalığının artırılmasına etkileri araştırılmıştır.
[18]	Sosyal ağ kullanıcıları	PSEDIA adlı sosyal ağdan elde edilen veriler kullanılmıştır	Var	Çalışma kapsamında 2 yöntem kullanılmış olup bunlardan ilki resim ikazları (nudge), ikincisi sayı ikazları (nudge) olarak adlandırılmıştır. Her iki ikazın da kullanıcı davranışlarında ciddi değişikliklere sebep olduğu ortaya konulmuştur.
[32]	Cep telefonu kullanıcıları	AppOps uygulaması ile toplanan veriler kullanılmıştır	Var	3.parti yazılımların kullanıcıların haberi olmadan sağladığı erişimlerin yönetilmesi ve ikaz edilmesi amacıyla kullanılan AppOps adlı uygulama ile kullanıcıların davranışlarında ortaya çıkan değişimler araştırılmıştır. Katılımcıların büyük çoğunluğu izinlerde kısıtlamalar yapmıştır.
[14]	Farklı cins ve yaşta kullanıcılar	Anket	-	Kişisel verilerin korunmasına yönelik gerçekleştirilen çalışmada Çinlilerin gizlilik ile ilgili düşüncelerini araştırılmıştır.
[34]	Sosyal ağ kullanıcıları	Anket	-	300 kişiye anket gönderilerek genel olarak sosyal ağ kullanım amaçları, verilerinin ifşa olması ve sosyal ağ ortamlarının kullanıcı verilerini depolamasına yönelik düşüncelerinin ne olduğu araştırılmıştır.
[35]	Üniversite Öğrencileri	Anket	-	Öğrencilerin gizlilik algısının belirlenebilmesi amacıyla 25 lisans öğrencisine açık uçlu sorular sorularak ölçek geliştirilmiş, geliştirilen ölçek ise 386 katılımcıya uygulanarak sonuçlar değerlendirilmiştir.

2.2.3. Değerlendirmeler

Sosyal ağ ortamlarında gizlilik/mahremiyet farkındalığına yönelik yapılan çalışmaların neredeyse tamamının gerçekleştirilen anketlere dayandırıldığı, kısıtlı miktarda çalışmada belirli verilere yönelik (konum bilgisi gibi) analizler gerçekleştirildiği ya da etkileşimli uygulamalarla kullanıcı farkındalığı oluşturulmaya çalışıldığı görülmüştür. Farklı disiplinlerin sosyal medya ortamlarında yer alan verilere ilgi duyduğu ve son yıllarda bu alan üzerinde yapılan çalışmaların hızla arttığı ancak gizlilik farkındalığının ölçülmesine yönelik uygulama bulunmadığı görülmüştür.

Literatürde kullanıcıların gizlilik ve mahremiyet farkındalığına ilişkin yapılan anket çalışmaları genel olarak değerlendirildiğinde;

- Kullanıcıların kişisel verilerine yönelik endişe duyduğu,
- Verilerinin güvenliğine yönelik en az güven duydukları ortamın sosyal ağ ortamları olduğu,
- Sosyal ağ ortamlarında hangi verilerini paylaştıklarından çoğu zaman haberdar olmadıkları,
- Kullanıcıların yaşadığı ülkeye göre verilere verdikleri değerin farklı olduğu (Almanya’da sağlık verileri, Amerika’da kimlik bilgileri) ve
- Sosyal medya ortamını özel olarak görmesine rağmen mahrem verilerini bu alanda kamulaştırdığı tespit edilmiştir.

Kullanıcıların mahremiyet kaygılarına rağmen, farkındalık eksiklikleri, elde edilen veriler ile neler yapılabileceği konusundaki öngörüden yoksun olmaları gibi sebepler nedeniyle gizlilik ihlallerine sıkça maruz kalmasının temel sebebinin sosyalleşme içgüdüğü olduğu çalışmalarda ortaya konulmuştur. Bu nedenle kişilerin sosyal ağ kullanımından kaçınmasını beklemenin bir çözüm olmadığı, gizlilik/mahremiyet ihlalleri ile sosyalleşme duygusu arasında güçlü bir ilişki olduğu değerlendirilmektedir.

Sosyal ağlarda gizlilik ve mahremiyet farkındalığına yönelik gerçekleştirilen çalışmalar incelendiğinde etkileşimli uygulamalar, durum tespiti, düşünce tespiti ve ilişkilerin belirlenmesine yönelik çalışmalar olarak gruplandırılabilen değerlendirilmektedir.

Kullanıcı izinlerinin denetlenmesi, paylaşımların etki alanının (kaç kişiye ulaşacağı vb.) gösterilmesi ve paylaşılacak içeriğin kullanıcılarla müzakere edilmesi gibi etkileşimli uygulamalar içeren çalışmalar kısıtlı sayıda da olsa yapılmıştır. Söz konusu çalışmaların kullanıcı davranışlarında yarattığı değişiklikler çalışmalardan elde edilen sonuçlar doğrultusunda değerlendirildiğinde gizlilik ve mahremiyet farkındalığının artırılması konusunda katkı sağlayabileceği görülmektedir. Durum tespitine yönelik çalışmalar kapsamında, kullanıcıların konum bilgileri üzerinden hareketliliğinin tespiti, kullanıcıya ait farklı hesapların eşleştirilmesi ve kullanıcı profillemesine (5 büyük karakter, siyasi eğilim vb.) yönelik etkileşim içermeyen ancak durum tespiti yapılmasına ve mevcut veriler

kullanılarak örtük bilgilerin açığa çıkarılmasını sağlayan çalışmalar bulunduğu görülmektedir.

Kullanıcıların sosyal ağların suç ortamı olarak kullanılması, gizlilik mahremiyet ihlallerine ilişkin düşünceleri, sosyal ağları kullanım amaçları, gizlilik ihlaline ortam hazırlayabilecek saldırılara ilişkin düşünceleri ve verilerin depolanması gibi konularda görüşlerinin alınarak düşüncelerinin tespit edilmesine yönelik farklı disiplinler altında anket çalışmaları yapılmıştır.

Anket çalışmalarının bir diğer amacının ise çeşitli unsurlar ile gizlilik/mahremiyet farkındalığı arasındaki ilişkilerin belirlenmesi olduğu görülmektedir. Cinsiyet, kullanıcı sayısı, kullanıcıların ülke aidiyeti, ekonomik ve sosyal statüsü, kullanım süreleri, arkadaş sayısı gibi unsurların gizlilik farkındalığı ile ilişkilerinin belirlenmesi maksadıyla çalışmalar gerçekleştirilmiştir.

Gizlilik ve mahremiyet farkındalığına yönelik yapılan çalışmaların kapsamının, meslek grupları, öğrenciler, sosyal ağ kullanıcıları ve cep telefonu kullanıcıları olarak gruplandırıldığı görülmektedir. Söz konusu grupların gizlilik ve mahremiyet farkındalığının ölçülmesi için, sosyal ağlardan elde edilen veriler, çeşitli projeler vasıtası ile toplanan veriler, kullanıcılar ile mülakat yapılarak elde edilen veriler ve yoğunlukla anket uygulamaları sonucunda elde edilen verilerin kullanıldığı görülmektedir. Gizlilik ve mahremiyet konusunda yapılan çalışmalarda verilerin paylaşılmaması nedeniyle çalışmaların tekrar edilebilirliğinin bulunmaması bir dezavantaj olarak karşımıza çıkmaktadır. Öyle ki çeşitli projeler ile araştırmacılara sunulan verilerin daha sonradan gizlilik politikaları ve kişisel verilere yönelik hassasiyetin artması nedeniyle paylaşımı durdurulmuştur.

2.3. Sosyal Ağ Verileri ile Gerçekleştirilen Uygulama Çalışmaları

Bu bölümde sosyal ağ verileri kullanılarak gerçekleştirilen uygulamalara yönelik literatürde yer alan çalışmalar araştırma sahası, araştırma hedefi, veri kaynağı, veri boyutu, metot ve araçlar ile amaç yönlerinden incelenerek özetlenmiştir.

2.3.1. Metodoloji

Mevcut çalışmalara ilişkin gerçekleştirilen literatür incelemesi Şekil 2.1’de sunulan metodoloji doğrultusunda gerçekleştirilmiştir.



Şekil 2.1. Metodoloji

Belirlenen metodoloji doğrultusunda öncelikle inceleme kapsamında incelenecek çalışmalar tespit edilmiştir. Bu kapsamda Çizelge 2.3’te sunulan anahtar kelimeler ve yıl kriterleri doğrultusunda veri tabanlarında sorgulamalar yapılmıştır. Sorgulamalar sonucunda ortaya çıkan çalışmalar arasından yüksek atıf alan (Bazı hariç tutulan çalışmalar dışında) ve uygulama içeren toplam 147 çalışma özet ve başlık bilgileri doğrultusunda inceleme kapsamında ele alınmıştır.

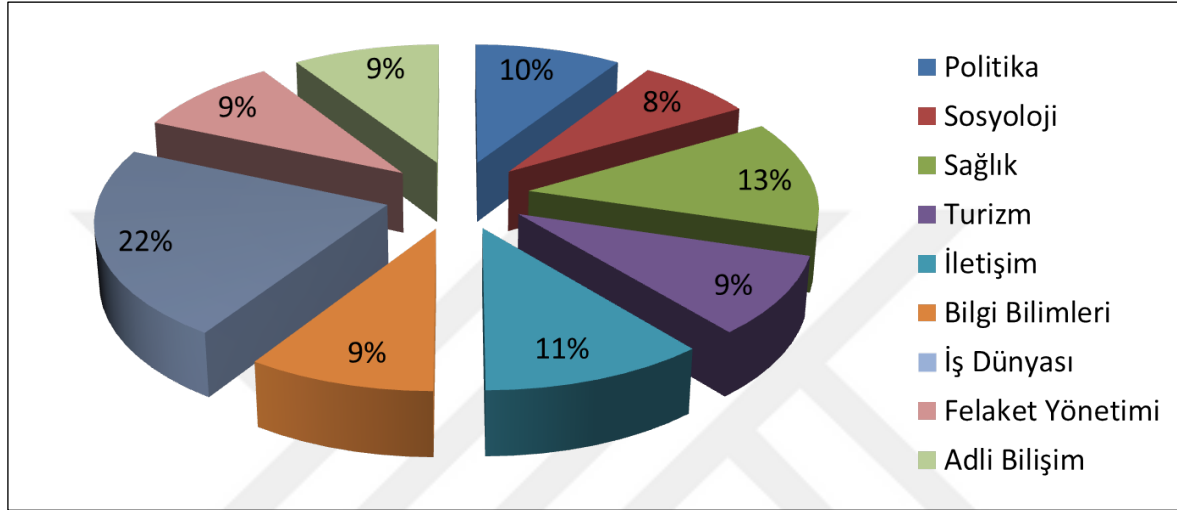
Çizelge 2.3. Anahtar kelimeler ve veri tabanları

Arama Terimleri	Veri Tabanı	Zaman Aralığı
KEY ("big data" AND "social media") OR KEY ("big data" AND "twitter") OR KEY ("big data" AND "facebook") OR KEY ("big data" AND "sina weibo")	WOS (Web of Science), SCOPUS, IEEE, Science Direct	5 Yıl (Bazı hariç tutulan çalışmalar dışında)

Sosyal medyadan elde edilen büyük verilerin uygulama alanları, amaçları, kullanılan method/teknikler ile kullanılan araçların anlaşılması çalışmamızın ana hedefleri olduğu için özellikle bir alanda uygulama yapılmış çalışmalar tercih edilmiştir.

2.3.2. Çalışmaların konularına göre sınıflandırılması

Yapılan değerlendirme ve analiz çalışmaları doğrultusunda Çizelge 2.3'te sunulan hedef verileri içeren 53 adet çalışma konularına göre 9 farklı çalışma alanında sınıflandırılarak alt başlıklar halinde özetlenmiştir. Çalışmaların konularına göre dağılımı Şekil 2.2'de görülmekte olup çalışmalara ilişkin hazırlanan özet tablo Çizelge 2.4'te sunulmuştur.



Şekil 2.2. Çalışmaların konularına göre dağılımı

Son 5 yılda yapılan çalışmalar göz önüne alındığında politika, sağlık ve iş dünyasına yönelik çalışmalarda ciddi bir artış olduğu görülmektedir. Literatür incelemesi kapsamında ele alınan çalışmalar 9 alt başlıkta gruplanmış olsa da sosyal büyük veri kullanılarak gerçekleştirilen çalışmalar bu alanlarla sınırlı değildir.

Politika

Ülkeyi 30 yıl yöneten Mısır Cumhurbaşkanı'nın görevden alınmasıyla sonuçlanan protestolara ilişkin gerçekleştirilen çalışmada, İngilizce ve Arapça tivitler toplanarak Mısır'daki çevrimiçi protestoyu inceleyen bir yöntem oluşturulmuştur [36].

2017 Almanya seçimlerine ilişkin yapılan bir çalışmada [37] partilerin Facebook duvarlarında yapılan etkileşimlere ilişkin veriler toplanmış bu verilerden yapılan analizde birden fazla partiyi takip eden vatandaşlar, seçim çalışmaları esnasında meydana gelen takipçi artışları, ayda en az bir kez parti Facebook sayfasını ziyaret eden sadık partililerin

tespiti gerçekleştirilmiştir. Ayrıca, partilerin sayfalarında etkileşime giren kullanıcıların üzgün, mutlu, alaycı, sevgi, beğeni içeren etkileşimleri de analiz edilmiştir. İsim bilgilerinden hareketle partileri destekleyen kişiler arasında cinsiyet değerlendirmesi de yapılmıştır.

GPU ile hızlandırılmış sosyal medya verisi işleme sistemi ile [38] sosyal medyadan elde edilen verilerin canlı olarak işlenmesi amaçlanmıştır. Bu maksatla “election” konu başlığı ile atılan twitlerin 6 ay boyunca toplanması ile 69,96 GB’lık veri elde edilmiş, çalışma kapsamında 1,5 GB’lık bölümü tekli cihazda işleneceği için kullanılmıştır. Duygu analizi, aktivite yoğunluğu ve konuma göre tivitlerin analizleri yapılmış ve GPU kullanımı ile tekil bilgisayarlarla canlı akış analizi yapılabileceği belirtilmiştir. Duygu analizi pozitif ve negatif sözlüklerle tivit içerisindeki kelimelerin karşılaştırılması ile skor üretilerek gerçekleştirilmiştir.

Politik veriler ile tahmin analizi yapılan çalışmada [39], sosyal medya verileri kullanıcıların politik değerlerini analiz etme ve sınıflandırma ile tahminde bulunma amacıyla kullanılmıştır. Çalışma modelinde K-NN algoritması ve Logistic Regression algoritmaları kullanılmıştır.

Twitter kullanıcılarının politik eğilimlerini ölçmek ve çıkarımlarda bulunmak amacıyla yapılan çalışmada [40] kullanıcıların politik tivit ve retivitlerinin tutarlı olduğu ve benzer kullanıcıların benzer topluluklar tarafından retivit edildiği kabul edilmiştir. Daha sonrasında 2012 yılında 7 ay boyunca ABD Başkanlık seçimine yönelik kampanyalara ilişkin atılan 119 milyon tivit toplanmıştır. Sıklıkla retivit edilen kaynaklar üzerinden yapılan çalışmada %94’lük başarımlar sağlanmış, sıklıkla retivit edilen 1000 kaynak üzerinden 232 000 kullanıcının politik demografisi çıkarılmıştır.

Hilary Clinton ile ilgili atılan tivitlerin zaman, konum ve takipçi sayılarına göre duygu analizlerini (pozitif, negatif, nötr) yaparak grafik olarak gösterilmesine yönelik yapılan çalışmada [41] Hadoop uygulaması kullanılmış, Map Reduce yapılarak işlemler daha hızlı gerçekleştirilmeye çalışılmıştır.

Sosyoloji

Mahalle memnuniyeti araştırmacılar için yeni bir trend haline geldiğinden İsveç'te yerleşim yerlerinin değerlendirilmesi için “şehir aşkı” adlı bir yöntem geliştirilmiştir. Veri setini oluşturmak için mutluluk, nüfus değişimi, cep telefonu konumları ve TripAdvisor verileri kullanılmıştır [42].

Beijing'te bulunan 127 farklı parkın ziyaretlerine ilişkin yapılan analiz çalışmasında, Weibo'da yapılan 581 354 konum bildirimi dikkate alınarak istatistiksel yöntemlerle parkların kullanımını etkileyen faktörlere ilişkin analizler yapılmıştır. Park boyutu, şehir merkezine yakınlık ve giriş ücretinin ziyaret oranlarını ciddi şekilde etkilediği, 15 parkın toplam ziyaret sayısının %74,6'sını oluşturduğu ortaya konulmuştur [43].

Sosyal medya metin verilerinden toplum düşüncesinin araştırıldığı çalışmada [44] etiketlenen az miktarda veri ile büyük miktarda verinin etiketlenmesini sağlayacak yarı danışmanlı bir sistem tasarlanmıştır. Bu kapsamda, 11,75 milyonluk bir veri seti elde edilmiştir. Yarı danışmanlı sistemin eğitilmesi için ise silah hakları ve silah kontrolünü destekleyen kuruluşlar tespit edilmiş ve 171 profilin 8 448 gönderisi etiketlenmiştir. Yapılan çalışmada %95,6 doğruluk ile silah kontrolü/destekçiliği konusunda ön yargılı düşüncelerin sınıflandırılabilirdiği belirtilmiştir.

Sağlık

Wuhan (Çin)'da Covid-19'un ilk tespit edildiği Aralık 2019'dan başlayarak pandemi sırasında alınan önlemlerin insan hareketini ve etkinliğini analiz etmek için gerçekleştirilen çalışmada Twitter verileri ve günlük Covid-19 vaka sayıları kullanılmıştır [45].

En yaygın zihinsel hastalıklardan biri olan depresyonun Facebook durum paylaşımlarından tahminine ilişkin yapılan çalışmada, 2008-2015 yılları arasında depresyon teşhisi konulmuş kişilerin 949 530 Facebook durum paylaşımı toplanmış, %72 doğruluk ile ilk teşhisten 3 ay öncesine kadar depresyona girecek kullanıcıların tespit edilebildiği ortaya konmuştur [46].

Büyük veri yaklaşımı ile gelecekte meydana gelebilecek zihinsel hastalıkların tahminlenmesi amaçlanan çalışmada Reddit Sosyal Medya sayfasından elde edilen 515 374

gönderi kullanılmıştır. Zihinsel hastalığın konuşulduğu alt sayfalardan (Subreddit) hastalığa işaret eden sözcükler elde edilerek makine öğrenmesi yöntemleri ile tahminleme yapılmıştır [47].

Twitter verilerinden grip trendlerinin tahmin edilmesine yönelik gerçekleştirilen çalışmada [48] 2016 Kasım ile 2017 Ocak tarihleri arasında arasında Birleşik Arap Emirlikleri bölgesi içerisinde kalan kullanıcıların attıkları tivitler filtreleme, dil sınıflandırması ve sonrasında tivit sınıflandırması işlemlerinden geçirilerek influenza hastalığının yayılmasına ilişkin tespit ve tahminlerde bulunulmuştur. Hastane kayıtları ile yapılan karşılaştırmalarda 0,78 oranında tutarlılık tespit edilmiş olup yönetimler tarafından Twitter verilerinin güvenilir bir şekilde kullanılabileceği ifade edilmiştir.

Ebola ve Zika virüsü salgını döneminde Twitter verilerinden değer üretmek amacıyla yapılan çalışmada [49] yaklaşık 60 milyon tivit toplanarak analiz edilmiştir. Çalışmada öncelikle tivitlerden faydalı bilgilerin çıkarılması sonrasında Hadoop tabanlı makine öğrenmesi kütüphanesi olan Mahout ile konu modelleme tekniği kullanılmıştır. Daha sonrasında aşılama ile ilişkin duygu analizleri gerçekleştirilmiştir.

Sırasıyla 2014 ve 2016 yıllarında meydana gelen Ebola ve Zika salgınlarına ilişkin gerçekleştirilen çalışmada kullanılmak üzere toplam 350 000 tivit toplanmıştır. Sağlık riskleri, önleme, semptomlar, bulaşma ve tedavi olmak üzere 5 tür tivit'i sınıflandırabilmek ve analizi için Word2Vec kullanılmıştır. Gerçekleştirilen çalışmada %92 doğruluk oranı elde edilmiştir [50].

Turizm

Metin verileri kullanılarak yürütülen çalışmalardan farklı olarak gerçekleştirilen çalışmada, turizm sitelerinin çekiciliğini tespit etmek için Flickr görüntüleri kullanılmıştır. Bu çalışma kapsamında 26 392 görüntü toplanmış ve görüntülerin makine öğrenmesi algoritmaları ile analiz edilmesi için Mathematica yazılımı kullanılmıştır. Seçilen 6 İtalyan şehrinde deneysel uygulama yapılmıştır [51].

Paylaşılan her bir tivit, kişilerin fikir ve duygularını içeren bir iz oluşturduğu kabul edilmektedir. Bu kabulden hareketle Twitter'dan elde edilen coğrafi etiketli verileri

kullanarak bölgesel refahı tespit etmenin mümkün olup olmadığının araştırıldığı çalışmada konum verisi içeren 1,5 milyardan fazla tivit elde edilmiş, veriye dayalı ve kelime düzeyinde yöntemlerle incelenmiştir [52].

Turistlerin zamansal ve mekânsal olarak aktivitelerinin ayak izlerinin çıkarılmaya çalışıldığı çalışmada, farklı büyük veri kaynaklarından (Panoramio, Twitter ve Foursquare) elde edilen veriler karşılaştırılmıştır. Yapılan çalışma ile turistlerin Madrid şehrinde aktivitelerinin nerelerde hangi yoğunlukla gerçekleştirildiği görselleştirilmiştir [53].

Büyük veri analitiğinin turizmde stratejik karar destek sistemi olarak kullanılmasına yönelik gerçekleştirilen çalışmada, Flickr üzerinde paylaşılan fotoğraflar kullanılarak Melbourne şehri ele alınmıştır. Çalışmada MATLAB ve Google Maps'ten faydalanılarak turist davranışları analiz edilmiş ve tahminlerde bulunulmaya çalışılmıştır [54].

İletişim

Sosyal medyada bulunan tüm bilgiler doğru değildir, bazıları sadece yanlış söylentilerdir. Bu problemin çözümüne yönelik olarak söylenti çürütme yöntemi üzerine bir araştırma yapılmış olup araştırmanın veri setini oluşturmak için toplam 483 327 Sina Weibo gönderisi toplanmış, toplanan veri doğal dil işleme yöntemleri ile analiz edilmiştir [55].

George Floyd'un ölümü ve Covid-19 medyada ve sosyal medya ortamlarında uzun süre viral olmuştur. Kullanıcılar tarafından oluşturulan farklı içerik kaynakları genelinde kalıpları ve eğilimleri yakalayan Çok Modelli Analiz Platformu oluşturulması amaçlanan çalışmada doğal dil işleme ve görüntü işleme süreçleri büyük veri teknikleriyle entegre edilmiştir [56].

Günlük içerik ve fikir paylaşan yüksek takipçi sayısına sahip sosyal medya kullanıcıları fenomen olarak adlandırılmaktadır. Bu sayede pazarlamanın etkili araçlarından biri haline gelen fenomenleri tespit etmek için Twitter verileri üzerinde büyük veri teknolojilerini kullanan bir yöntem önerilmiştir [57].

Yaklaşık 500.000 Flickr görüntüsü kullanılarak sosyal medya ortamları için bir öneri sistemi oluşturmak maksadıyla bir yöntem geliştirilmiştir. Söz konusu yöntem ile kullanıcıların göz atma etkinliklerini incelenerek ilgili içeriğin bulunması amaçlanmaktadır.

Benzerlik deęerlendirmesi iin En Yakın Komşu Sorgusu kullanılmış olup elde edilen sonuçlar önerilen yöntemin mevcut alışmalara göre daha yüksek doęruluęa sahip olduğunu göstermiştir [58].

Akıllı Trafik Yönetim Platformu (Smart Traffic Management Platform-STMP) oluşturulması amaçlanan alışmada sosyal medya, IoT sensörleri ve CCTV, hava durumu gibi veriler kullanılarak Trafik Tahminlemesi, Akıllı Trafik Kontrolü, Sosyal Medya Tabanlı Yolcu (Commuter) Duygu Analizi ve Etki Yayılımı tahminleri yapılmıştır. Avusturalya'daki ana arterler üzerinde gerçekleştirilen deneysel alışmada önerilen modelin başarılı ve gerçek zamanlı olarak tekrarlayan ve tekrarlamayan olayları tespit edebildięi ve otomatik olarak sosyal medyadan elde edilen verilerle doęrulandığı belirtilmiştir [59].

Sosyal aęlarındaki aktivitelerinden kullanıcıların ilgi alanlarının tahmin edilmesini amaçlayan alışmada [60] kullanıcının beęendięi sayfalara ilişkin bilgiler kullanılmıştır. İlave olarak kabalık kaynaklı veriler kullanılarak geçmiş verileri doęrultusunda gelecekteki kullanıcılara uygun olmayacak olanlar filtrelenmiştir. Bu filtrelenen bileşenler ve en az 10 adet açığa çıkarılan ilgi alanı ile kullanıcının gelecekteki ilgileri %80 güvenilirlikle tahmin edilebilmenin mümkün olduğu belirtilmiştir.

Veri Bilimleri

Konu deęerlendirmesi amaçlanan alışmada [61] Twitter üzerinden elde edilen 467 milyon satırlık veri ön işlemden geçirilerek parametrik olmayan CRP (Chinese Restaurant Process), DTM ve online LDA algoritmaları ile deęerlendirilmiştir. Sonuçlar karşılaştırıldığında en iyi konu gruplamasının CRP kullanarak oluşturulan modelle ortaya konulduğu gösterilmiştir.

Sosyal medya verileri ile seyirci sayısı ve TV reytinglerinin belirlenmesi amacıyla yapılan büyük veri analizi alışmasında [62] 2014-2016 yılları arasında Danimarka Futbol Federasyonuna ilişkin Facebook üzerinden toplanan sosyal medya verileri, seyirci sayıları ve TV reytinglerine ilişkin veri setleri kullanılmıştır. Yapılan alışma sonucunda Facebook'tan elde edilen veriler kullanılarak çok yüksek doęruluk oranı ile TV reytinglerini ve seyirci sayılarının tahmin edilebildięi ortaya konulmuştur.

2014 FIFA Dünya Kupası'na ilişkin atılan tivitlerin analiz edilerek duygu analizi yapılması amaçlanan çalışmada [63] toplanan tivitlerden eğitim için ayrılanlar el ile pozitif/negatif olarak sınıflara ayrılmıştır. Bayesian Logistic Regression (BLR) algoritması ile eğitilerek sınıflandırmalar gerçekleştirilmiş, gerçekleşen olaylar ile duygular arasında ilişki olup olmadığı araştırılmıştır. Pozitif ve negatif tivitlerin ayrıştırılması için harici sözlük kullanılmıştır. Ayrıca Unigram ve Bigram özellikleri belirlenmiş ve özelliklerin en çok kullanılanlarını belirleyebilmek için TF-IDF (Term Frequency-Inverse Document Frequency) kullanılmıştır. Yapılan çalışma sonucunda gerçekleşen olaylarla duygu analizleri arasında ilişki olduğu örnek durum çalışmalarından elde edilen veriler ile ortaya konulmuştur.

KNIME uygulaması kullanılarak gerçekleştirilen büyük veri ve duygu analizi çalışmasında [64] kullanılmak üzere 812 176 tivit ile 419 624 değerlendirme (review) toplanmıştır. Tivitler KNIME uygulaması üzerinden elde edilirken çevrimiçi değerlendirmeler Apache Nutch ile elde edilmiştir. Online değerlendirmeler 7 başlık altında 1-5 arası değerlendirilirken tivitler nötr, pozitif ve negatif olarak sınıflandırılmıştır. Yapılan çalışmada online değerlendirmelerin tespitinin metin içeriklerinin daha standart ve anlaşılabilir olması nedeniyle yüksek başarımla gerçekleştirildiği, tivitlerin doğası gereği sloganlar, kısa ifadeler içermesi ve kişiye özgü yazımlara sahip olması nedeniyle daha zor olduğu belirtilmiştir.

İş Dünyası

Herhangi bir markanın ana endişesi her zaman ürünlere olan gelecekteki talep olmuştur. Günlük paylaşılan bilgilerin boyutu nedeniyle sosyal medya bilgi kaynağı olarak en iyi ortam haline geldiğinden ürünlere yönelik gelecekteki talebi tahmin etmek amacıyla Facebook ve Twitter gönderilerini kullanan bir yöntem geliştirilmiştir. Söz konusu çalışma kapsamında Naive Bayes ve Standard Vector Machine algoritmaları kullanılarak 1,2 milyondan fazla gönderi analiz edilmiştir [65].

Starbucks hakkında atılan tivitlere odaklanılan çalışmada seçilen marka hakkındaki duygular üzerinde bir inceleme gerçekleştirmiştir. Marka özgünlüğünü tespit etmek için duygu polaritesi beş boyutta incelenmiş olup Standart Vektör Makinesi algoritması ile 2 milyonun

üzerinde tivit analiz edilmiştir. Sonuçlar, önerilen yöntemi kullanarak tivitlerin marka duyarlılığını tahmin etmek için kullanılabileceğini göstermiştir [66].

Twitter verilerinden firmalara ilişkin duygu analizi ve borsa işlem hareketlerinin tahmin edilmesine yönelik gerçekleştirilen çalışmada borsada işlem gören 30 firmaya ilişkin 200 milyon tivit elde edilmiş, NASDAQ ve NYSE (Londra ve New York Borsası) elde edilen veriler kullanılmıştır. Yapılan çalışmada T+3 günlük sürede borsa hareketleri ile tivitler arasında 0,79 doğrulukla bir ilişki olduğu ortaya konulmuştur. Ayrıca yapılan çalışmada SMeDA-SA adlı mevcut makine öğrenmesi algoritmalarından farklı bir algoritma geliştirilerek kullanılmış, bu alanda yaygın olarak kullanılan SVM, Naïve Bayes ve C4.5 algoritmaları ile kıyaslanarak daha yüksek doğruluğa sahip sonuçlar elde edilmiştir. Diğer algoritmalarından farklı olarak kavram haritaları oluşturarak ağırlıklandırmalar yapmaktadır. Örneğin Apple Inc. Firması ile ilgili bir sınıflandırma yapılacağında batarya, Iphone, MacBook Pro vb. sözcükleri de hiyerarşik olarak ağırlıklandırarak Apple Inc ile kavramsal olarak ilişkilendirdiği bir kavram haritası oluşturmaktadır [67].

Potansiyel müşterilerin ürün performansına ilişkin tüketici görüşleri aracılığıyla alternatif ürünleri değerlendirmelerine yardımcı olmak için genişletilmiş bir olasılıksal dilbilimsel TODIM (PL-TODIM) yöntemi sunulan çalışmada 4 farklı SUV araca yönelik durum çalışması gerçekleştirilmiş, mevcut modellerin başarımları ile önerilen model kıyaslanmıştır. Çalışmada kullanıcı yorumlarının yer aldığı inceleme web sitelerinden elde edilen veriler kullanılmıştır [68].

Türk Hava Yolları müşteri etkileşiminin büyük sosyal medya verileri üzerinden analiz edildiği çalışmada [69], büyük sosyal veri konseptleri, müşteri memnuniyeti, duygu analizi, veri ve metin madenciliği ve makine öğrenmesi yeteneklerinden faydalanılarak araştırma sorularına cevap aranmıştır. Söz konusu çalışmada iki tür veri seti kullanılmıştır. İlki iş verisi olarak adlandırılan ve şirketler tarafından açık olarak yayınlanan hisse senedi fiyatı, çeyrek gelirleri ve aylık taşınan yolcu sayısı verilerinden oluşmaktadır. İkincisi ise 5 488 066 satırlık Türk Hava Yolları Facebook sayfasında yapılan gönderi, yorum ve yorumlara cevapları içeren yapısal olmayan (sadece belirli bir formatta olmaması değil sadece insanların anlam çıkarabilmesi nedeniyle bu şekilde ifade edilmiştir) verilerden oluşmaktadır. Yapılan çalışmada ilk veri seti ile ikinci seti arasında güvenilir bir ilişki bulunamamıştır. Ancak, Facebook verilerinin servislere ilişkin kullanıcı memnuniyetini ölçebilecek önemli bir değer

olarak kullanarak gelecek bilet satışlarını arttırabileceğini ve memnuniyetsizlik yaratan gözden kaçmış hususların tespit edilebileceğini ortaya koymuştur.

Duygu analizi yapılması amaçlanan çalışmada [70] Hindistan'da servis sağlayıcı olan Airtel firması ile ilgili olarak #Airtel_presence konu başlığı ile atılan yaklaşık 80 000 tivit Twitter API ile elde edilmiştir. Apache Mahout ve Hadoop ortamları verinin işlenmesi için kullanılmıştır. Tivitlerin sınıflandırılması için veri sözlüğü kullanılmış olup Naive Bayes algoritması ile %70 başarımlı sağlandığı ifade edilmiştir. Firmaya ilişkin atılan tivitlerin ise %20'sinin negatif, %38'inin nötr ve %40'ının pozitif olduğu ortaya konulmuştur.

Twitter verileri üzerinden iPhone satışlarının tahmin edilmesine yönelik gerçekleştirilen çalışmada [71] sosyal sosyal veri kavramsal modeli temel alınmıştır (aktörler, hareke, aktiviteler, ürünler ile konular, anahtar kelimeler, zamirler ve duygular). Lineer regresyon modeli ile iPhone tivitleri kullanılarak çeyrek dönemde yapılan iPhone satışları yatırım bankasından alınan tahmin modelleri ile küçük bir ortalama fark ile tahmin edilmiştir. Duygu analizinin de sürece dahil edilmesi ile daha güçlü bir ilişki elde edilmiştir.

Felaket Yönetimi

Son dönemde tüm dünyada yaşanan afetlerde sayısız can kaybedilmesi nedeniyle afete dayanıklı akıllı şehirlerin karma bir veri analizi yapılması amaçlanmıştır [72]. Sosyal medya (Twitter), kirlilik (gaz sensörleri), trafik (karayolu trafik simülatörü) ve yangın (yangın dinamik simülatörü) verileri Hadoop ve Apache Spark kullanılarak analiz edilmiştir. Nayomi Kankanamge ve arkadaşları tarafından yapılan benzer bir çalışmada (2020) afet şiddeti değerlendirmesi amacıyla karar ağacı makine öğrenme algoritması kullanılarak 16 782 konuma ilişkin tivitler incelenmiştir [73].

Çin'de Sina Weibo adında yaygın olarak kullanılan bir sosyal ağ verileri kullanılarak gerçek zamanlı acil durum olaylarını tanımlamak için bir yöntem geliştirilmiştir. Yöntem, gönderiler tarafından cevaplanacak 5N1K, Ne, Nerede, Ne Zaman, Kim ve Neden sorularından oluşmaktadır. Geliştirilen yöntem kullanılarak Çin'in en büyük iki şehrinde meydana gelen yangın ve kaçırma olmak üzere iki farklı olay için deneysel analiz yapılmıştır [74].

Küresel ısınmayla birlikte artan yağmur fırtınası, su basması gibi afetleri Çin'de büyük problemler haline dönmüştür. Bu problemlere yönelik gerçekleştirilen çalışmada Sina Weibo'dan elde edilen 6 385 veri kullanarak acil durum lojistiğine yönelik bir çalışma yürütülmüştür [75].

Felaketlerden etkilenen insanların duygularının otomatik olarak analiz edilmesi amaçlanan çalışmada Twitter üzerinden elde edilen 70 817 tivit kullanılmıştır. Subjektif terimler ve bigram özellikli makine öğrenmesi algoritmaların en yüksek doğruluğa sahip sonuçları verdiği ortaya konulmuştur [76].

Adli Bilişim

Endonezya'da topluma karşı bir tehdit oluşturan motosiklet çetelerinin yapılarını anlamak amacıyla gerçekleştirilen çalışmada Netvizz uygulaması kullanılarak Facebook'taki hayran sayfalarından kullanıcı verileri toplanarak analiz edilmiştir. Çalışma sonucunda, 2 000'den fazla aktif üyeye sahip 25 farklı çete tespit edilmiştir [77].

Twitter üzerinde paylaşılan verinin çeşitliliği tüm hareketlerin izlenmesini mümkün kılmaktadır. Bu doğrultuda gerçekleştirilen çalışmada Twitter gönderileri terörist davranışlarının tespit edilmesi amacıyla analiz edilmiştir. Söz konusu çalışma kapsamında Arapça tivitler elde edilmiş olup 10 000 adet tivit toplanmıştır [78].

Sosyal medya ortamlarında faydalı içeriklerin yanı sıra bazı rahatsız edici içerikler de paylaşılmaktadır. Belirli gruplara yönelik nefret söylemi de bu rahatsız edici içeriklerden biri olarak bilinmektedir. Irk ve dini hedef alan nefret söylemleri arasında bir bağlantı olup olmadığını görmek için yapılan çalışmada 21 milyonu aşkın Twitter verisi toplanmış ve Support Vector Machine ve Bag of Words kullanılarak verilerin analizi gerçekleştirilmiştir [79].

Vatandaşların güvenlik algısını ölçmek için yapılan çalışmada [80] Twitter üzerinden elde edilen veriler kullanılmış olup veri toplama, ön işlem, sınıflandırma, indeksleme ve görselleştirme için büyük veri uygulamalarından faydalanılmıştır. 111 günlük periyotta Bogota şehrinde atılan 2 476 426 adet tivit elde edilmiş olup bu tivitlerin güvenlik ile ilgili olup olmadığının tespiti için makine öğrenmesi yöntemleri kullanılmıştır. Güvenlik ile

alakalı olduğu değerlendirilen 3 141 kelimelik sözlük oluşturulmuş ve modelin eğitilmesi için Google Predicion API kullanılmıştır. Çalışmada coğrafi noktaların gösterilmesi ve sıcaklık haritası üretilerek sonuçların görselleştirilmesi maksadıyla Google Fusion Table kullanılmıştır.

Sosyal medya ortamları herhangi bir ürün için büyük bir pazarlama yeri haline gelmiştir. Ancak, bu durum vahşi yaşam pazarlamasını içeren suç faaliyetleri tarafından kötüye kullanılabilir. Yasadışı vahşi yaşam pazarlamasını tespit etmek için Facebook gönderileri üzerinde yapılan araştırmada 10 303 Facebook gönderisi bu amaçla toplanmış ve analiz edilmiştir [81].

Sosyal ağ verisi kullanılarak gerçekleştirilen uygulama çalışmalarına yönelik literatür incelemesi kapsamında 9 araştırma alanı altında ele alınan çalışmalar çalışmanın hedefi, çalışmada kullanılan veri kaynağı, çalışma kapsamında kullanılan verinin boyutu, gerçekleştirilen çalışmada kullanılan yöntem ve araçlar ile çalışmanın amacı başlıklarını kapsayacak şekilde karşılaştırmalı olarak Çizelge 2.4'te sunulmuştur.

Çizelge 2.4. Sosyal ağ verisi ile gerçekleştirilen uygulama çalışmalarının karşılaştırılması

Alan	Çalışma	Çalışmanın Hedefi	Veri Kaynağı	Veri Boyutu	Kullanılan Yöntem ve Araçlar	Amaç
Politika	[36]	Mısır'daki ayaklanmaların duygu analizi.	Twitter	187 131 tivit	Logistic regresyon, 2 faktörlü varyans analizi	Analiz
	[37]	2017 Almanya Seçimlerinde Yapılan Paylaşımlardan Partili Analizi	Facebook	900 000' den fazla kullanıcı verisi	Veri analizi yapılmıştır	Analiz
	[38]	Sosyal Medyada Seçimlere İlişkin Anlık Verilerin Görselleştirilmesi	Twitter	3 milyondan fazla tivit	Gerçek zamanlı verilerin işlenebilmesi için GPU ile hızlandırılmış model oluşturulmuştur.	Analiz
	[39]	Kullanıcıların Politik Değerlerinin Analiz Edilmesi, Sınıflandırılması ve Tahmini	Facebook	N/A	K-NN algoritması, Lojistik regresyon kullanılmıştır.	Analiz, Tahmin
	[40]	Sosyal Medya Kullanıcılarının Politik Eğilimlerinin Ölçülmesi ve Analizi	Twitter	119 milyondan fazla tivit	Makine öğrenmesi yöntemleri uygulanmış ve sonuçları karşılaştırılmıştır.	Analiz

Çizelge 2.4. (devam) Sosyal ağ verisi ile gerçekleştirilen uygulama çalışmalarının karşılaştırılması

Alan	Çalışma	Çalışmanın Hedefi	Veri Kaynağı	Veri Boyutu	Kullanılan Yöntem ve Araçlar	Amaç
Sosyoloji	[82]	Bölgelerin çekicilik değerlendirmesi	TripAdvisor Anket Sonuçları	N/A	Lineer regresyon modeli	Analiz
	[43]	Beijing’te bulunan parkların ziyaret rakamlarının büyük veri ile analizi.	Sina Weibo	581 354 konum	İstatistiksel yöntemler kullanılmıştır (Kruskal Wallis Test, Spearman’s Correlation).	Analiz
	[44]	Silah Kontrolü, Destekçiliği Konusunda Toplum Düşüncesi Tespiti	Twitter	11,75 milyon	Semi-Supervised Label Prediction yöntemleri kullanılmış ve VDCNN, n-grams+tfidf, fastText ile karşılaştırılmıştır	Analiz
	[83]	Kentsel alanların ortak ziyaret ağı değerlendirme	Sina Weibo	2,4 milyon gönderi	NetMiner Software	Analiz
Veri Bilimleri	[61]	Sosyal Medya Verilerinin Konu Gruplamasının Yapılması	Twitter	467 milyon	CRP (Chinese Restaurant Process), DTM ve online LDA algoritmaları ile değerlendirilmiştir	Analiz
	[62]	Sosyal Medya Verilerinden Futbol Seyirci Sayısı ve TV reytingi Tahmini	Facebook	2 milyon üzerinde	Lineer Regresyon	Tahmin
	[63]	Sosyal Medyada FIFA 2014 İle İlgili Paylaşımların Duygu Analizi	Twitter	30 milyon	Bayesian Lojistik Regresyon (BLR) kullanılmıştır.	Analiz
	[64]	Cihazlara İlişkin Sosyal Medya Verileri ve Değerlendirme Sitelerinden Elde Edilen Verilerle Duygu ve Düşünce Analizi	Twitter Değerlendirme Siteleri	1.2 milyon üzerinde	Veriler Apache Nutch ve KNIME uygulamaları ile elde edilmiştir.	Analiz
Sağlık	[50]	Ebola ve Zika hakkında atılan tivitlerin sağlık riskleri, korunma, belirtiler, bulaşma ve tedavi olarak sınıflandırılması.	Twitter	350 000 tivit	Word2Vec	Analiz
	[45]	Covid-19’un yayılmasının izlenmesi	Twitter	N/A	Hadoop	Analiz
	[46]	Facebook durum güncellemelerini kullanarak depresyona girmesi muhtemel hastaların tahmini	Facebook (Hastane verisi de kullanılmıştır)	949 530 bilgi	Makine öğrenmesi, dlatk.wwwbp.org analiz altyapısı	Tahmin
	[47]	Sosyal medya verileri ile gelecekte karşılaşılabilecek bir zihinsel hastalığın tahminlenmesi.	Reddit (Subreddit Depresyon, Anksiyete)	515 374 gönderi	TF-IDF, L2 Penalized Regression Model, Makine öğrenmesi	Tahmin
	[48]	Grip Trendlerinin Tahmin Edilmesi	Twitter, Hastane Verisi	N/A	Lineer Regression yöntemi ile tahminler yapılmış ve gerçek hastane verileri ile karşılaştırılmıştır.	Tahmin
	[49]	Sosyal Medya Verilerinden Ebola ve Zika Virüsü Salgınına ve Aşılama Konusunda Duygu Analizi	Twitter	60 milyon tivit	Apache Mahout ve Hadoop ortamları verinin işlenmesi için, LDA algoritması ile sınıflandırılmıştır.	Analiz
	[84]	Covid-19 pandemi ülke imajını araştırmak	Twitter	6 milyon tivit	Bidirectional Encoder Representations from Transformer (BERT)	Analiz

Çizelge 2.4. (devam) Sosyal ağ verisi ile gerçekleştirilen uygulama çalışmalarının karşılaştırılması

Alan	Çalışma	Çalışmanın Hedefi	Veri Kaynağı	Veri Boyutu	Kullanılan Yöntem ve Araçlar	Amaç
Turizm	[51]	Turizm bölgelerinin çekiciliğini keşfetmek	Flickr	26 392 resim	Mathematica yazılımı	Analiz
	[52]	Bölgelerin refah değerlendirmesi	Twitter	1,53 milyar tivit	Data-driven ve word-level methodlar	Analiz
	[53]	Madrid Şehrindeki turist aktivitelerinin belirlenmesi.	Panoramio, Twitter, Foursquare	234 159 tivit 20 076 konum	Spatial Autocorrelation, Clustering (K-Means), Ordinary Least Square, Census Tract Maps	Analiz
	[54]	Konum bilgisi içeren fotoğraflardan Tur Organizatörleri (DMO) için anlamlı bilgi ve tahmin çıkarımı.	Flickr	238 290 resim	Matlab, Google Maps	Tahmin
	[85]	Facebook beğenilerinin turizm alanında tahminleme yeteneğinin araştırılarak Google Trends verileri ile karşılaştırılması.	TourMIS, Google Trends, Facebook	N/A	ADL (Auto Regressive Distributed Lag) Model Class, MIDAS (Mixed Data Sampling) Model Class	Tahmin
Felaket Yönetimi	[72]	Afete dayanıklı akıllı şehirlerin analizi	Yangın ve yol trafik sensörleri, Gaz sensörü, Twitter	74 GB	Hadoop ekosistemi ve Spark Engine	Analiz
	[73]	Afet şiddeti değerlendirmesi	Twitter	16 782 tivit	Karar ağacı, makine öğrenmesi algoritmaları kullanılmıştır.	Analiz, Karar Destek
	[74]	Gerçek zamanlı kentsel acil durumların tanımlanması	Sina Weibo	N/A	-	Analiz
	[75]	Afet sonrası kurtarma yollarının optimizasyonu	Sina Weibo	6 385 gönderi	ICTCLAS, NSGA-III algoritması	Karar Destek
	[76]	Felaketlerden etkilenen insanların sosyal ağlardaki paylaşımlarından duygu analizi yapılması.	Twitter, Followthe-hashtag	70 817 tivit	SVM algoritması, Lexicon tabanlı sınıflandırma, Apache Spark büyük veri ortamı	Analiz
Adli Bilişim	[77]	Motosiklet çetelerinin topluluk yapısının tespiti	Facebook	14 112 profil	Veri toplama için Netvizz kullanılmıştır.	Analiz
	[78]	Terörist davranış tespiti	Twitter	10 000 tivit	Microsoft Azure ML Studio (Machine learning)	Analiz
	[79]	İrk ve din hedefli nefret söylemi arasındaki bağlantının incelenmesi	Twitter	21,7 milyon tivit	Support Vector Machine (SVM), Bag of Words (BOW)	Analiz
	[80]	Vatandaşların Güvenlik Algısının Ölçülmesi	Twitter	2,4 milyon üzeri	Google Predicion API ve sıcaklık haritası üretilmesi için Google Fusion Table kullanılmıştır.	Analiz
	[81]	Yasadışı vahşi yaşam pazarlamasını tespit etmek	Facebook	10 303 gönderi	-	Analiz

Çizelge 2.4. (devam) Sosyal ağ verisi ile gerçekleştirilen uygulama çalışmalarının karşılaştırılması

Alan	Çalışma	Çalışmanın Hedefi	Veri Kaynağı	Veri Boyutu	Kullanılan Yöntem ve Araçlar	Amaç
İş Dünyası	[86]	Ekonomi sektörlerinin popülerlik kazancının haritalandırılması	Twitter, Instagram Facebook, Bloglar ve Forumlar	5 185 gönderi	Sayısal içerik analizi	Analiz
	[65]	Ürünlerin gelecekteki talep miktarının tahmini	Twitter Facebook	1 208 650 gönderi	Naive Bayes, Support Vector Machine	Tahmin
	[66]	Marka duyarlılığını analiz etme	Twitter	2 282 912 tivit	Support Vector Machine algoritması	Analiz
	[67]	Borsada işlem göre 30 firmaya ilişkin duygu analizi ve borsa hareketlerinin tahmin edilmesi.	Twitter, Borsa Verileri	200 milyon	SMeDA-SA algoritması geliştirilmiş, SVM, Naive Bayes, C4.5 algoritmalarının doğruluk oranları ile karşılaştırılmıştır.	Analiz, Tahmin
	[68]	Potansiyel müşterilerin ürün performansına ilişkin tüketici görüşleri aracılığıyla alternatif ürünleri değerlendirmelerine yardımcı olmak	Online ürün görüşleri	N/A	Probabilistic Linguistic Terms Sets, Multiple Attributed Decision Making Model	Karar Destek
	[69]	THY Müşteri Etkileşiminin Ölçülmesi	Facebook, Çeyrek Gelirleri, Yolcu Sayıları	5 milyondan fazla	Veri analizi yapılmıştır	Analiz
	[70]	Sosyal Medya Verilerinden Airtel Firmasına Yönelik Duygu Analizi	Twitter	80 000'den fazla	Apache Mahout ve Hadoop ortamları verinin işlenmesi için kullanılmıştır. Tivitlerin sınıflandırılması Naive Bayes algortması kullanılmıştır.	Analiz
	[71]	iPhone Satışlarının Tahmin Edilmesi	Twitter	400 milyondan fazla	Çoklu Regresyon Analizi kullanılmıştır.	Tahmin
	[87]	Bankacılık sektöründe büyük veri tabanlı sistematik risk modeli oluşturma.	Twitter, Bankacılık Verileri	N/A	Grafiksel Gaussian Modeli, Naive Bayes.	Karar Destek
	[88]	Havayolu endüstrisindeki pazarlama segmentlerini tespit etmek	Twitter	13 144 etkileşim	Görselleştirme için Gephi ve istatistiksel hesaplama yöntemleri.	Analiz
	[89]	Airport service quality assessment using OSNs	Twitter	34 528 tivit	Theysey Software	Analiz
	[90]	OSN'leri kullanarak havaalanı hizmet kalitesi değerlendirme	Twitter	106 350 tivit	Doğal dil işleme, SentiStrength	Analiz

Çizelge 2.4. (devam) Sosyal ağ verisi ile gerçekleştirilen uygulama çalışmalarının karşılaştırılması

Alan	Çalışma	Çalışmanın Hedefi	Veri Kaynağı	Veri Boyutu	Kullanılan Yöntem ve Araçlar	Amaç
İletişim	[55]	Sosyal medya dedikodularının çürütülmesi	Sina Weibo	483 327 gönderi	Doğal dil işleme	Tahmin
	[56]	Paternlerin ve eğilimlerin yakalanması için doğal dil işleme ve görüntü işlemenin entegrasyonu	Twitter	2 milyon tivit 76 000 haber makalesi 10 000 resim	Doğal dil işleme, Görüntü işleme	Tahmin
	[57]	Sosyal fenomenlerinin tespiti	Twitter	556 150 tivit	-	Analiz
	[58]	Sosyal ağlar için tavsiye sisteminin oluşturulması	Flickr	500 000 resim	En yakın komşu sorgusu	Karar Destek
	[59]	Trafik veri akışlarından dinamik kalıplar yakalamak ve gerçek zamanlı trafik analizi gerçekleştirilmesi amaçlanan yeni bir Akıllı Trafik Yönetimi Platformu oluşturmak	Akıllı sensörler, Twitter	190 milyon	Online Incremental makine öğrenmesi algoritması L2, derin öğrenme, danışmasız makine öğrenmesi	Karar Destek
	[60]	Sayfa Beğenilerinden Gelecekteki İlgili Alanlarının Tahmini	Facebook	N/A	Perceptual Prediction Lineer yöntemi kullanılmıştır	Tahmin

2.3.3. Çalışmaların incelenmesi ve amaçlarına göre sınıflandırılması

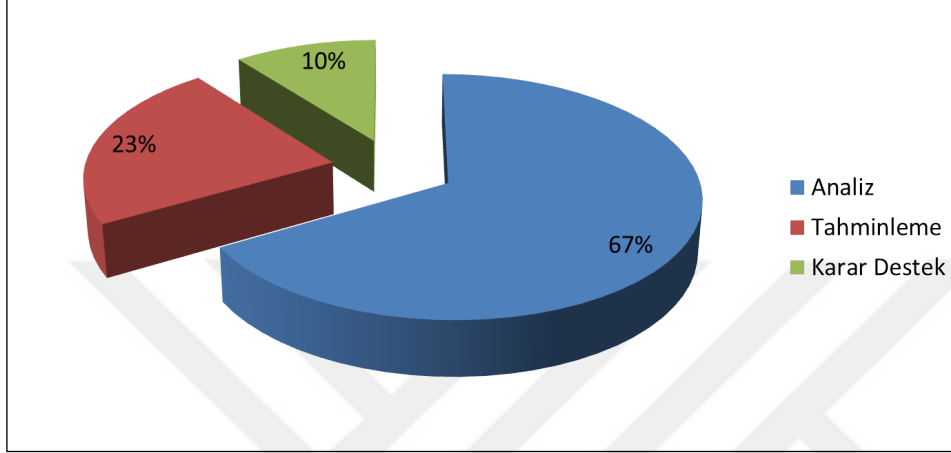
Literatürde yapılan çalışmalar incelendiğinde konularına göre çok geniş bir alanda farklı çalışmalar gerçekleştirildiği görülmektedir. Ancak, bu çalışmaların tamamı geniş bir perspektiften incelendiğinde amaçlarına göre esasen 3 temel sınıfta sınıflandırılmasının mümkün olduğu değerlendirilmektedir.

Bu kapsamda Çizelge 2.4'te sunulan çalışmalar amaçları ve içerikleri bakımından incelendiğinde;

- **Karar Destek:** Bir konuya ilişkin geçmişten gelen tüm verileri de göz önüne alarak geleceğe ilişkin alınacak kararlarda en iyi hamlelerin (stratejik) belirlenmesi amacı güdülen çalışmalar,
- **Tahminleme:** Mevcut durum verileri göz önüne alınarak gelecekteki durumun tahmine edilmeye çalışıldığı çalışmalar,

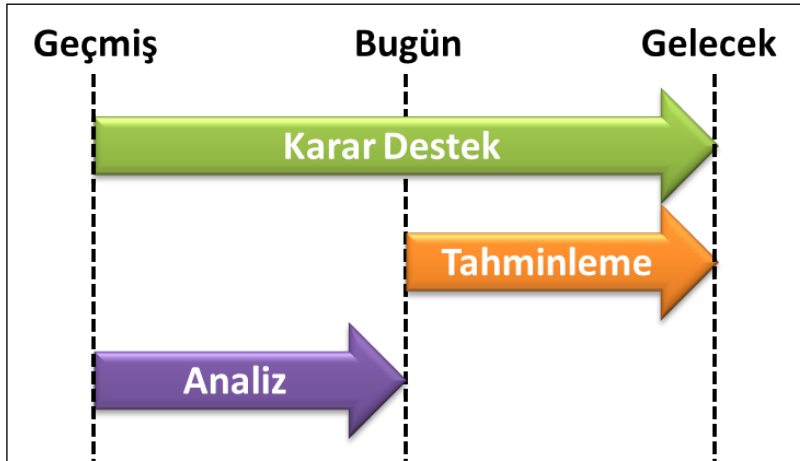
- **Analiz:** Bir konunun mevcut durumunun ortaya konulabilmesi amacıyla geçmişten mevcut duruma kadar olan çalışmaların analiz edildiği çalışmalar,

olarak 3 sınıfta sınıflandırılabilceği görülmekte olup çalışmaların amaçlarına göre oranları grafiksel olarak Şekil 2.3'te sunulmuştur.



Şekil 2.3. Çalışmaların amaçlarına göre dağılımı

Literatür incelemesi kapsamında seçilen çalışmalar incelendiğinde karar destek, analiz ve tahminleme amaçlı çalışmaların bir zaman skalası üzerinde belirli alanlara karşılık geldiği değerlendirilmekte olup Şekil 2.4'te sunulmuştur. Her bir amaç için alt başlıklar halinde değerlendirme yapılacaktır. Büyük veri ile gerçekleştirilecek çalışmalarda söz konusu zaman skalasının dikkate alınmasının çalışmanın amaç ve kapsamının belirlenmesine, aynı zamanda elde edilen veri ile hedeflenen çalışmanın gerçekleştirilip gerçekleştirilemeyeceği noktasında doğru karar verilmesine ciddi katkı sağlayacağı değerlendirilmektedir.



Şekil 2.4. Amaç tabanlı zaman skalası

Analiz

Analiz amaçlı gerçekleştirilen çalışmalar geçmişten bugüne kadar oluşturulmuş büyük verinin incelenmesi ile bir değerlendirme yapılmasını, dolayısıyla bir konuya ilişkin durum tespiti için ortaya konulmasını sağlamaktadır. Literatürde yer alan çalışmalar göz önüne alındığında bu durum tespiti bir firmanın bir hizmete ilişkin müşteri memnuniyetini, bir şehirdeki parkların kullanım oranlarını, bir hastalığın belirtilerinin neler olabileceğini, toplumun bir konu hakkındaki düşüncesi gibi birçok konuyu kapsayabilmektedir.

Literatürde yer alan çalışmalar genel olarak değerlendirildiğinde Şekil 3'te sunulan grafikte de görüleceği üzere analiz amaçlı çalışmaların yoğunlukla gerçekleştirildiği görülmektedir.

Analiz amaçlı çalışmalarda yoğunlukla;

- Duygu analizi,
- Konu sınıflandırma,
- Düşünce madenciliği,
- Metin madenciliği,
- Ölçüm,
- Görselleştirme,
- Tespit,

işlemleri gerçekleştirilmektedir. Çok geniş yetenekleri olan ve kişi/kurumlara büyük resmi sunan analiz amaçlı çalışmaların giderek yaygınlaştığı görülmektedir.

Tahminleme

Günümüzde özellikle kar amaçlı firmaların en çok elde etmek istediği değerlerin başında geleceğe ilişkin veriler yer almaktadır. Şekil 4'te yer alan zaman skalasında da görüleceği üzere mevcut durumdaki bilgiler (today) kullanılarak gelecekteki durumlara ilişkin beklentilerin büyük veri kullanılarak tahmin edilmesi bu alt başlığın konusunu oluşturmaktadır.

Çok geniş bir alanda etkinlikle kullanılmakta olan tahminleme amacı doğrultusunda bir turizm rotasının yoğunluğundan, yeni rotaların tahmin edilmesine, bir cihaza ilişkin beklenen talep miktarına, bir seçimi hangi partinin kazanacağından, bir parkın hangi profile vatandaşlar tarafından tercih edileceğine kadar çok geniş bir spektrumda büyük veriler kullanılarak çalışmalar yapılmıştır. Bazı çalışmalarda borsa verileri, firma açıklamaları, hastane kayıtları gibi gerçek veriler ile yapılan tahminlere ilişkin karşılaştırmalar da yer almakta olup doğruluk oranlarının yüksek olduğu görülmektedir.

Karar Destek

Sosyal medya ortamlarında oluşturulan büyük veriler, karar vericilere daha fazla iç görü sağlamak için sayısız fırsat yaratmaktadır. Bununla birlikte, büyük veri analitiği üzerine yapılan çok az sayıda çalışma, stratejik karar alma desteği üzerinde yoğunlaşmıştır. Büyük veri, araştırmacıların ve karar vericilerin ilgisini her geçen gün daha fazla çekmektedir. Bu konuda turizm alanından örnekler, turizm rotalarında stratejik planlama amaçlı bilgi üretimi, konaklama yönetimi, müşteri ilişkileri yönetimi ve tur pazarlaması gibi başlıkları içermektedir [54].

Her ne kadar sosyal medyadan elde edilen büyük veri karar destek sistemleri için çok büyük bir avantaj sağlasa da büyük veri bunları otomatik olarak sağlamamakta ve birçok dezavantajı ve iyi yönetilmesi gereken noktaları da içerisinde barındırmaktadır [91].

Şekil 2.3'te sunulan amaç tabanlı zaman skalası doğrultusunda değerlendirildiğinde aslında karar destek amaçlı yapılan çalışmaların analiz ve tahminleme amaçlarını da kapsadığı düşünülebilir. Dolayısı ile karar destek amaçlı çalışmaların tahminleme ve analiz çalışmalarında yer alan teknik/yöntem/araç ve modellere de sıklıkla başvurduğu literatürde yer alan çalışmalarda görülmektedir.

Karar Destek Sistemleri, stratejik kararların alınabilmesi için geçmişin çok iyi analiz edilmesi ve yapılacak tahminler doğrultusunda gelecekteki beklentilerin karşılanabilmesi için en iyi kararların alınmasına yardımcı olunması amaçlanan sistemler olarak tanımlanabilir. Alternatif kararların oluşturulabilmesi ve içlerinden en iyi alternatifin seçilebilmesini amaçlar. Literatürde müşteri değerlendirmeleri kullanarak potansiyel

müşterilere alternatif ürünlerin gösterilmesi, akıllı trafik yönetim platformu oluşturulması, tavsiye sistemi gibi örnek çalışmalar yer almaktadır.

2.3.4. Çalışmalarda karşılaşılan saha problemleri

Çalışmalarda sosyal medya platformlarından elde edilen veriler sıklıkla tercih edilse de yasal düzenlemelere uyum, veri işleme, verilerin gizliliği ve mahremiyeti gibi konular güçlükleri beraberinde getirmektedir. Bu bölümde çalışmalarda karşılaşılan zorluklar ana kategoriler altında kısaca değerlendirilmiştir.

Teknik Konular

İnternete bağlanan milyonlarca cihaz (IoT), mobil cihazlar, sensörlerden elde edilen veriler ve hızla büyüyen sosyal medya platformları gibi sürekli veri üreten platformlar düşünüldüğünde bu kadar büyük veriyi işlemek ve talepleri karşılamak oldukça zor olacağı açıktır. Bahsedilen verilerin gerçek zamanlı olarak işlenmesi ve saklanması ise çok ciddi miktarda kaynak (disk, işlemci vb.) gerektirir [92]. Bu durum kurum ve şirketlerin çalışma şekillerini değiştirerek geleneksel yöntemlerden bulut ortamına geçişine kadar çok farklı sonuç ve dönüşüm ihtiyacını beraberinde getirmektedir.

Kesintisiz veri akışı da problemli konulardan biri olarak görülmektedir. Kullanıcılar tarafından sürekli önemli miktarda veri oluşturulmaktadır. Bu nedenle verilerle öğrenen ve öğrenilen görevlerin gerçekleştirilmesini sağlayan makine öğrenmesi gibi yöntemlerle oluşturulan modellerin değişen veriler doğrultusunda sürekli yenilenmesine ihtiyaç duyulmaktadır [93].

Teknik konularla ilgili bir diğer önemli nokta da altyapı eksikliğidir. Büyük veri uygulamalarını kullanmak için gereken yüksek altyapı maliyeti, araştırmacıların erişimini zorlaştırmaktadır. Çalışmaların genellikle büyük veri uygulamaları yerine makine öğrenmesi yöntemleriyle yapılmasının gerçek nedeninin güçlük olduğu değerlendirilmektedir. Günümüzde bulut servisleri yardımıyla bazı altyapı eksikliği kaynaklı büyük veri uygulamalarının kullanımına ilişkin sorunlar çözülebilmektedir. Ancak, çalışma bazı temel

durumlar dışında kişisel verilere odaklanıyorsa bulut hizmetleri uygun bir seçenek olmayacaktır.

Gizlilik, Yasal ve Kısıtlayıcı Yaptırımlar

Günümüzde sosyal verilerin yaygınlaşması ile hastalık eğilimlerinin belirlenmesinden toplum görüşünün anlaşılmasına, seçim sonuçlarının tahmin edilmesine kadar birçok alanda uygulamalar yapılmaktadır. Bu durum ülkeleri vatandaşlarının verilerinin mahremiyetine ilişkin düzenlemeler yapmaya sevk etmektedir. Kişisel verilere ilişkin ciddi düzenlemeler ve yaptırımlar öngörülmektedir. Örneğin, General Data Protection Regulation (GDPR) [94] gibi yürürlükteki yasalara uygun olarak verileri işlerken çok dikkatli olmak gerekmektedir. GDPR, yeni veri koruma yasalarına uygunluğu sağlamak için şirketler/işletmeler tarafından toplanan tüketicilerin/kişilerin kişisel verilerini kontrol etme yetkisine sahiptir [92]. GDPR'nin genel olarak veri etiği üzerinde de etkisi ve kontrolü vardır. Türkiye’de söz konusu hususlar Kişisel Verilerin Korunması Kanunu (KVKK) ile uyumlu olacak şekilde yürütülmektedir. Diğer ülkelerde de benzer yasal düzenlemeler bulunmaktadır.

Yakın zamana kadar, veri koruma çalışmaları esas olarak kişisel verilerin kontrolüne odaklanmaktaydı. Ancak, büyük veri uygulama ve yöntemleri ile paylaşılan verilerden hassas bilgiler ortaya çıkartılabilmektedir [95]. Bu nedenle, sosyal medyada paylaşılan her kelime günümüzde bir mahremiyet varlığına dönüşmüştür.

Ayrıca, kişisel verilerin uygunsuz kullanımı bir şirketin markasına da zarar verebilmektedir. Facebook hisseleri Cambridge Analytica ile ilgili bir veri ihlali bildirdikten sonra 100 milyar dolardan fazla değer kaybı yaşamıştır [92].

Araştırmacılar, şirketler gibi sosyal büyük veri ile çalışan tüm paydaşların verinin toplanması ve işlenmesi sırasında mahremiyet, yasal ve kısıtlayıcı yaptırımlar konusunda dikkatli olmaları gerekmektedir ve bu birçok çalışmanın gerçekleşmesinin önünde ciddi bir engel teşkil etmektedir.

Veri Kaynağı/Paylaşımı

Çeşitli prosedürler uygulanarak gerçekleştirilen çalışmaların veri setleri paylaşılamamakta, mevcut çalışmaların devamı veya tekrarı niteliğindeki çalışmalar kişisel bilgilerin mahremiyeti sorunları nedeniyle gerçekleştirilememektedir [6]. Platformların veri toplama noktasında getirdiği kısıtlamalar, veri setinin elde edilme süresini uzatmaktadır. Ayrıca veri ön işleme adımlarının uzun sürmesi ve içerdiği zorluklar, araştırmacılar için ciddi zaman kaybına neden olmakta ve yeni model ve uygulamalar geliştirmeye harcanacak zamanı sınırlandırmaktadır.

Kapsamlı çalışmalara temel teşkil edecek şekilde, kamu veya özel kuruluşlar tarafından araştırmacılara yeterli veri kaynağı sağlanmaması da çalışmalarda karşılaşılan bir diğer önemli engeldir. Büyük sosyal veriye sahip şirketlerin önceliğinin kurumsal gelirlerini ve kullanıcı sayısını artırmak olduğu düşünülmekte, bu nedenle veri paylaşımı konusuna öncelik vermediği veya çalışmalarını akademik dünya ile paylaşmadıkları değerlendirilmektedir [6].

Veri Ön-İşleme/İşleme

Çizelge 2.4'te sunulan çalışmaların veri kaynakları incelendiğinde, çalışmaların çoğunun metin verileri kullanılarak gerçekleştirildiği, geri kalanının ise konum ve görüntü verileri üzerinde yoğunlaştığı görülmektedir.

Metin verileriyle yapılan çalışmalar birçok zorluk içermektedir. Örneğin, sosyal büyük verilerle yapılan çalışmalarda duygu analizi yoğun olarak kullanılmaktadır. Ancak dillerin doğası gereği zorlukları bulunmaktadır. Bu zorluklar, İngilizce dışındaki dillerdeki kaynakların azlığı, alaycı ifadelerin tespit edilmesindeki zorluklar, deyimlerin tespiti, farklı kaynaklardan veri elde edilerek oluşturulan heterojen ortam, sosyal medya verilerinin eksik ve yanlış yazımları ve kişiye göre değişebilen metinlerin öznel anlamları olarak karşımıza çıkmaktadır [96].

Bahsedilen zorluklarına sosyal medya ortamlarının doğası gereği, genellikle noktalama işaretleri kullanılmaması, duygu ve düşüncelerin emojilerle ifade edilmesi, sesli harflerin yazılmaması, çok az sayıda kelimededen oluşan cümleler kullanılması, dönemsel slogan ve

tabirlerin ortaya çıkması gibi zorluklar eklenmektedir. Özellikle metin çözümleme/sınıflandırma çalışmalarında bu tür sorunlarla sıklıkla karşılaşilmektedir.

Ayrıca yazım hatalarını düzeltmek için kullanılan kelimelerin kökten çıkarılması ve normalleştirilmesi gibi süreçlerde yaşanan zorluklar düşünüldüğünde, sosyal verilerin işlenebilir hale dönüştürülmesi ciddi bir zaman ve tecrübe gerektirmektedir. İstisna olarak, haber sayfalarının ve resmi hesapların takiplerinde bu konuların resmi bir anlatım dili kullanılması nedeniyle daha kolay yönetilebileceği düşünülmektedir.

2.3.5. Değerlendirmeler

Sosyal ağ verisi ile gerçekleştirilen uygulama çalışmalarına yönelik yapılan literatür araştırması ile sosyal büyük veri uygulamaları ve zorlukları ile ilgili güncel çalışmalar detaylı olarak incelenmiş ve çalışmalar veri kaynağı, veri boyutu, kullanılan yöntem/araçlar ve amaç açısından karşılaştırmalı olarak sunulmuştur. Ayrıca, çalışmalar 9 ana “araştırma alanı” altında sınıflandırılarak özetlenmiş ve 3 ana amaç (analiz, tahmin ve karar destek) altında “amaca dayalı” bir sınıflandırma önerilmiştir.

Yapılan çalışmalar detaylı bir şekilde incelendiğinde, toplumsal olaylara ilişkin duygu analizinden seçim sonuçlarının tahminine, parkların ziyaret oranlarından olası psikolojik rahatsızlıkların tahminine, turistik faaliyetlerin tespitinden akıllı trafik yönetim platformunun oluşturulmasına kadar farklı amaçlarla birçok araştırma alanında çalışmaların yürütüldüğü ve çalışmaların bunlarla sınırlı kalmadığı görülmektedir. Problemin çözümüne yönelik veri elde edilebildiği sürece hemen hemen tüm alanlarda sorunların çözümüne yönelik çalışmaların gerçekleştirilebileceğini söylemek mümkündür.

Literatür araştırması kapsamında tespit edilen bir diğer önemli konu ise kullanılan veri boyutlarının binlerce satırdan başlayıp milyarlarca satıra ulaşmasıdır. Bu da sosyal verilerin ne kadar önemli olduğunu ve yapısal ve anlamsal özellikleri nedeniyle boyutları ne olursa olsun çalışmalar yapılabilceğini göstermektedir.

Çalışmanın temel amaçlarından biri literatürde kullanılan yöntem ve araçları anlamaktır. Yapılan incelemede birçok farklı yöntem ve aracın çalışmalara entegre edildiği ve uygulamalardan elde edilen sonuçların değerlendirildiği görülmüştür. Problemlerin

çözümünde kullanılan yöntem ve araçların temel amaçlarla birlikte sunulmasının araştırmacılara katkı sağlayacağı düşünülmektedir. Ayrıca, literatürdeki yöntem ve araçların zenginliğinin yapılacak yeni çalışmalara da ışık tutacağı değerlendirilmektedir.

Yapılan literatür incelemesinde;

- Çalışmaların büyük bir çoğunluğunun metin verileri kullanılarak gerçekleştirildiği,
- Konum ve görüntü verilerinin çalışmalarda sıklıkla tercih edildiği,
- Uygulamalarda makine öğrenmesi yöntemlerinin en çok ve büyük veri uygulamalarının nadiren kullanıldığı,
- Her ne kadar sosyal medya platformlarında bireyler tarafından kamuya açık olarak paylaşılan veriler kullanılarak çalışmalar gerçekleştirilmiş olsa da yasal düzenlemelere uyum, veri güvenliği ve veri gizliliği gibi hususların veri toplama ve işleme süreçlerinde güçlükler yarattığı,
- Sosyal medya platformlarından veri elde etmek mümkün olmasına rağmen, depolama, iletim, paylaşım gibi zorlukların araştırmacılar için hala büyük engel oluşturduğu,
- Sosyal medya platformundan elde edilen büyük verinin öneminin giderek artan bir trend olduğu ve sosyal büyük verinin günlük ve iş hayatında problem çözme aracı olarak kullanımının giderek yaygınlaştığı,
- Kamu veya özel kuruluşlar tarafından sağlanan yeterli veri kaynağının araştırmacılar için mevcut olmadığı ve
- Büyük veri ile gerçekleştirilen uygulamalarda (Kişisel verilerle gerçekleştirilen çalışmalar dışında) bulut ortamlarının kullanımının giderek yaygınlaştığı,

görülmektedir.

Sosyal büyük veri ile gerçekleştirilen çalışmalar incelendiğinde içerdiği tüm zorluklara rağmen hayatın tüm alanlarındaki problemlere bir çözüm olarak kullanıldığı görülmektedir. Bu nedenle, bu bölümde çalışmalara ilişkin yapılan sınıflandırma ve değerlendirmelerin literatüre katkı sağlayacağı, çalışma özetleri ve hazırlanan karşılaştırmalı çizelgenin sosyal büyük veri uygulamaları üzerinde çalışan araştırmacılara daha geniş bir bakış açısı sunacağı ve daha iyi model ve çalışmaların geliştirilmesine imkân sağlayacağı değerlendirilmektedir.



3. MATERYAL VE METOT

Gerçekleştirilen literatür incelemeleri ışığında, kişilerin sosyal ağlarda bilinçsizce ya da farkında olmaksızın gerçekleştirdiği kişisel veri ifşalarının tespitine yönelik çalışma kapsamında kullanılan materyal ve çalışma metodu bölümde ele alınacaktır.

3.1. Materyal

Sosyal ağlarda mahremiyet farkındalığının analiz edilerek kişisel veri ifşa riski barındıran paylaşımların tespit edilmesi maksadıyla oluşturulması planlanan modele ilişkin yöntemin belirlenmesi, veri setinin hazırlanması, modelin oluşturulması ve farkındalık analiz ve sonuçların görselleştirilmesi maksadıyla geliştirilecek model ve uygulamanın tasarlanması sürecinde yararlanılan materyal Şekil 3.1’de özet olarak sunulmuştur.



Şekil 3.1. Çalışmada kullanılan materyal bilgileri

Yöntemin belirlenmesi

Tez kapsamında ele alınan problemin çözümüne yönelik olarak kapsamlı bir literatür incelemesi gerçekleştirilmiştir (Bkz. Çizelge 2.2, Çizelge 2.4). Gerçekleştirilen literatür incelemesi ile farklı problemlere araştırmacıların yaklaşımları detaylı bir şekilde ele alınmıştır. Çalışmaların amaçları, veri kaynağı, veri boyutu, kullanılan metot ve araçlara ilişkin kapsamlı bir inceleme yapılarak tez çalışmasında kullanılacak yöntemle altlık sağlanmıştır.

Veri setinin oluşturulması

Gerçekleştirilecek tez çalışması kapsamında kullanılacak veri setinin hazırlanması ve görselleştirilmesi amacıyla geliştirilecek uygulamada Twitter'dan elde edilen veriler kullanılmıştır. Twitter'dan veriler kullanıcı sayfalarında yer alan tivitler ve anahtar kelimelerin aratılması sonucunda elde edilen veriler olacak şekilde elde edilmiştir. Anahtar kelimelerin belirlenmesi noktasında yargı kararları, Kişisel Verilerin Korunması Kanunu ve PII verilerine ilişkin akademik çalışmalar, broşürler, firma dokümanları dikkate alınmıştır.

Modelin oluşturulması

Twitter'da kullanıcılar tarafından atılan tivitlerin sınıflandırılması ve ifşa riski barındıran tivitlerin tespit edilmesi amacıyla kullanılacak modelin oluşturulmasına yönelik olarak literatürde yer alan çalışmalar ve bu alanda yaygın olarak kullanılan model ve uygulamalar, kod geliştirme ortamlarının eğitim dokümanları ile bu uygulamalarla geliştirilmiş örnek yazılımlar incelenmiştir. Elde edilen bilgiler doğrultusunda model oluşturulmasına ilişkin çalışmalar gerçekleştirilmiştir.

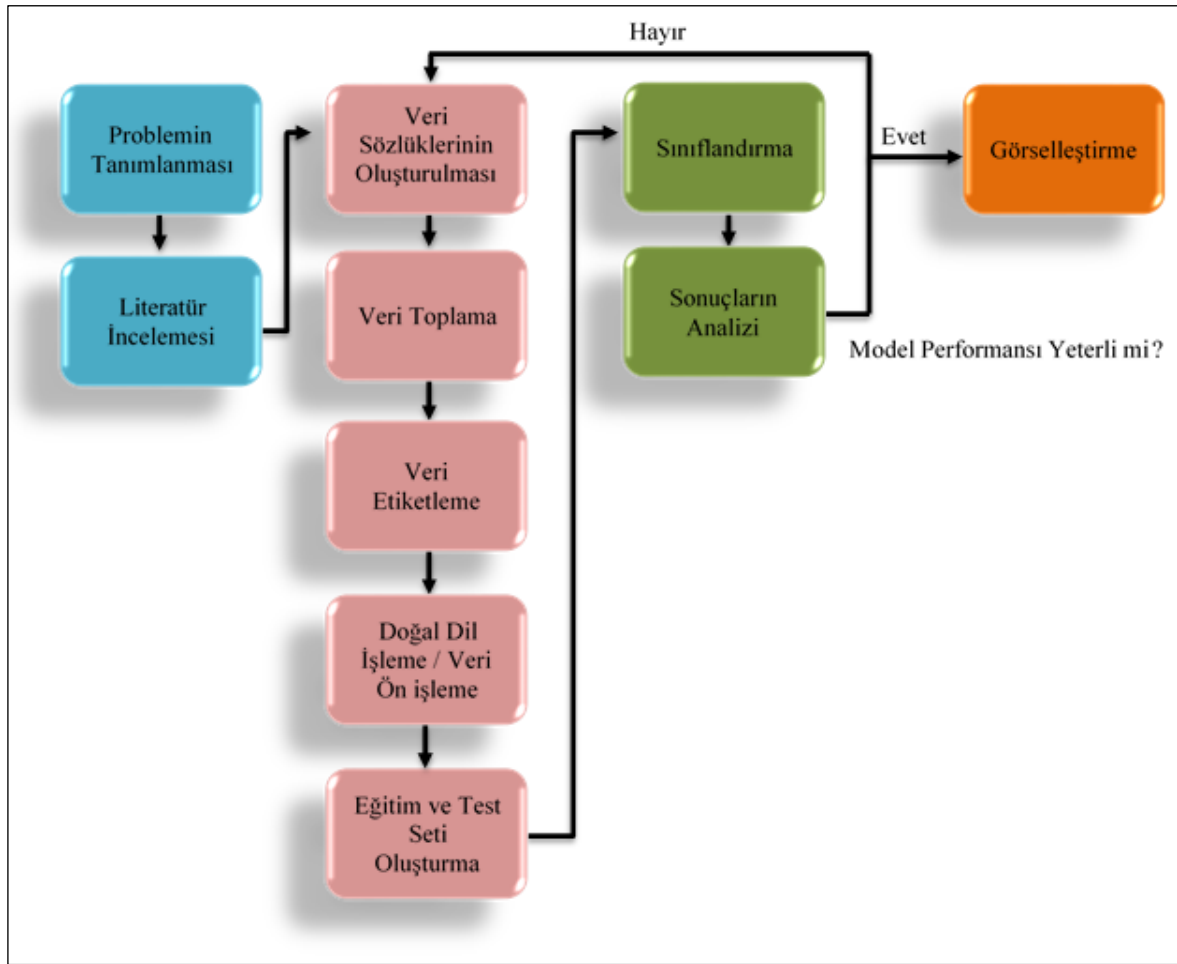
Uygulamanın geliştirilmesi

Literatürde yapılan çalışmalarda kullanıcı etkileşiminin farkındalığın arttırılmasında önemli olduğu örneklerle ortaya konulmuştur. Bu doğrultuda çalışmada ifşa riski barındıran Tivitlerin tespit işleminin kullanıcı ile etkileşim içerecek şekilde sunulmasına yönelik araştırmalar gerçekleştirilmiştir. Söz konusu araştırma kapsamında literatürde yer alan örnek uygulamalar ve kullandıkları yöntemler, kullanılmasına karar verilen uygulamaların eğitim

dokümanları ile Java, Python, Netbeans, Eclipse gibi geliştirme ortamlarına ilişkin bilgi edinilmiştir.

3.2. Metot

Sosyal veri ile kişisel veri ifşa riski barındıran tivitlerin tespit edilmesine yönelik gerçekleştirilen tez çalışması kapsamında Çizelge 2.4'te sunulan çalışmalar ile Çizelge 3.1'de sunulan materyale ilişkin yapılan değerlendirmelerin ışığında Şekil 3.2'de sunulan tez çalışma metodolojisi oluşturulmuş olup çalışma sürecinde takip edilmiştir.



Şekil 3.2. Tez çalışma metodolojisi

Metodoloji doğrultusunda öncelikle problem tanımlanmış, problemin çözümüne yönelik izlenecek yöntemin belirlenmesi maksadıyla geniş bir literatür incelemesi yapılmıştır. Literatür incelemesinden elde edilen bilgiler ışığında Twitter platformundan veriler elde edilerek kişisel veri ifşa riski içerip içermemesine göre etiketlenmiştir. Elde edilen ve

etiketlenen veriler ön işlem den geçirilerek veriler metin sınıflandırma çalışmasına uygun hale getirilmiştir. Öncelikle belirlenen sınıflar için ayrı ayrı sınıflandırma çalışması gerçekleştirilmiştir. Yapılan sınıflandırma sonuçları değerlendirilerek düşük doğruluk, kesinlik (Precision) ve geri çağırma (Recall) değerleri elde edilen sınıflar için veri setinde yer alan örnek sayısı artırılarak eğitim ve test süreci tekrar gerçekleştirilmiştir. Elde edilen dil modelleri ve verinin tamamının birleştirilmesi ile tüm sınıfları kapsayan bütüncül bir kişisel veri sınıflandırması amaçlanmıştır. Tez çalışması kapsamında yapılan sınıflandırma çalışması sonucunda ifşa riski barındırdığı tespit edilen tivitler kullanıcı farkındalığının artırılabilmesi maksadıyla geliştirilen uygulama üzerinden kullanıcıya sunulmuştur.

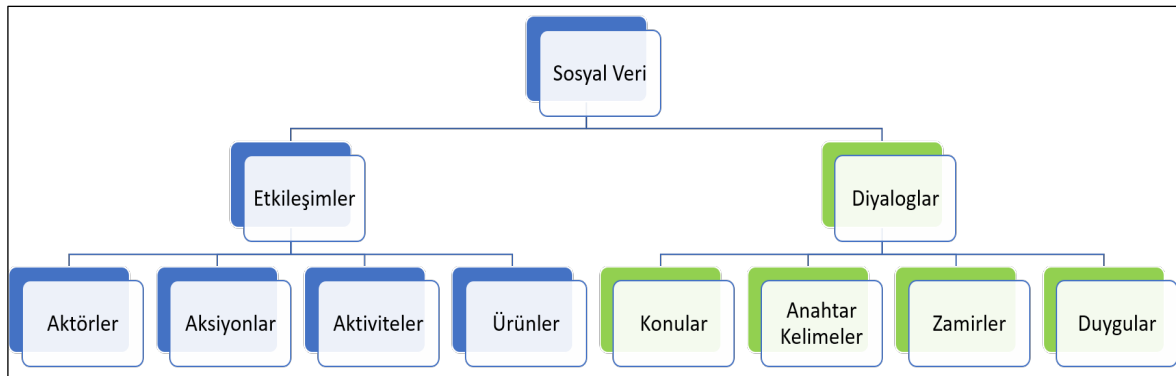
Söz konusu çalışma metodolojisi adımları içerisinde gerçekleştirilen işlemler ile yapılan geliştirme çalışmaları takip eden bölümlerde detaylı bir şekilde ele alınacaktır.

4. SOSYAL VERİ, VERİ SETLERİ, HAZIRLANMASI VE ANALİZLERİ

Doğal dil işleme ve makina öğrenmesi yöntemlerini kullanarak çözülmeye çalışılan sınıflandırma problemlerinde en önemli adımlar veri setinin elde edilmesi, etiketlenmesi ve ön işlemden geçirilmesidir. Bu aşamada yapılacak hatalar ve eksik uygulamalar oluşturulacak modelin başarımını birinci derecede etkileyen faktörlerden olacaktır. Çalışma kapsamında Türkçe paylaşımların elde edilmesi ile gerçekleştirilen veri seti hazırlama süreci 5 ana adımda gerçekleştirilmiş olup her bir adım alt başlıklar halinde açıklanacaktır.

4.1. Sosyal Veri Kavramı ve Platformunun Belirlenmesi

OSN (Online Social Networks)'ler, kullanıcıların kendi profillerini oluşturmaları, kendilerini ifade etmeleri, başkalarıyla iletişim kurmaları, kendi içeriklerini paylaşmaları, diğer kullanıcılar tarafından oluşturulan içerikleri görüntülemeleri ve bunlara yorum yapmaları için bir ortam oluşturur [97]. Literatürde OSN'lerden toplanan tüm veri çeşitlerini içeren bu veriler sosyal veri olarak adlandırılmış olup ortaya konulan kavramsal model Şekil 4.1’de sunulmuştur. Sosyal Veri Kavramsal Modeli [98], bu verilerin iki ana alanda değerlendirilmesi gerektiğini ortaya koymaktadır. Bunlardan ilki, yapılanlarla ilgili bilgileri içeren “Etkileşimler” (aktörler, gönderiler, beğeniler, etiketleme, paylaşım vb.), diğeri ise ne söylendiği hakkında bilgi içeren “Diyaloglar” (konular, anahtar kelimeler, duygular, duygular vb.) olarak tanımlanmaktadır [98]. Elde edilen verinin etiketlenmesi ve dil modelinin doğru oluşturulabilmesi için öncelikle üzerinde çalışılacak verinin kapsamının iyi belirlenmesi ve yapısının anlaşılması gerekmektedir.



Şekil 4.1. Sosyal veri kavramsal modeli (Türkçeleştirilmiştir) [98]

Kavramsal model genel olarak değerlendirildiğinde, sosyal medya ekosisteminde kullanıcıların gerçekleştirdiği diyalogların (metin tabanlı içerik) sosyal ağlarda mahremiyet ve gizlilik farkındalığı konu tez çalışmasının konusunu oluşturduğu görülmektedir.

Literatürde yer alan çalışmalar incelendiğinde sosyal verilerin tercih edilmesinin birçok nedeni ve avantajı bulunduğu görülmektedir. Bunlardan en önemlileri şu şekilde özetlenebilir;

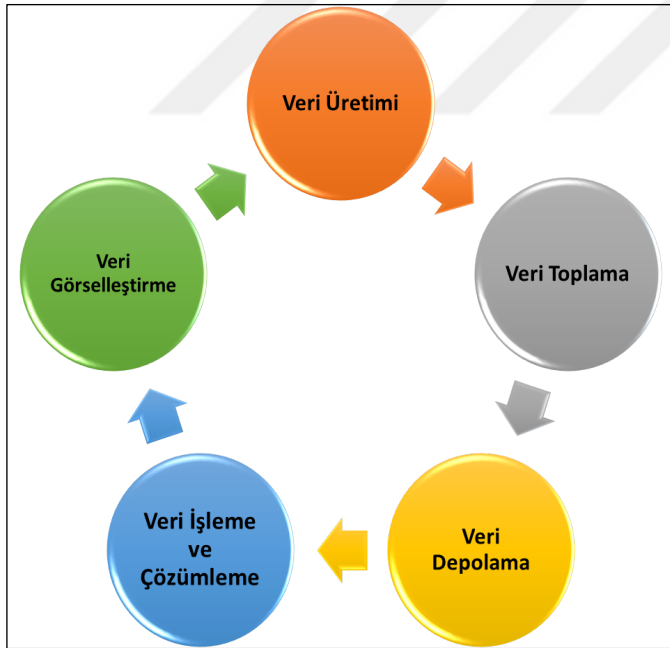
- **Kolay Elde Edilmesi:** Veriler, API'ler veya program parçacıkları kullanılarak elde edilebilmektedir,
- **Açık:** Veriler herkese açıktır (Ek gizlilik ayarlarına sahip hesaplar hariç),
- **Hacim:** Çok büyük boyutlarda veri seti elde edilebilir,
- **Zamanlılık:** Belirli bir zaman dilimine odaklanılabilir,
- **Çeşitlilik:** Görüntü, ses, metin vb.
- **Sınıflandırma:** Hashtag gibi özelliklerden yararlanılarak hedeflenen kullanıcı kitlesi ya da konularda sınıflandırılmış bilgiye erişim imkânı sağlar (LinkedIn, Subreddit, Twitter vb.).

Sosyal veriler her türlü araştırma için kullanılabilecek şekilde kullanıcıların duygu, düşünce ve tercihlerini ortaya koyan metin mesajları, resimler ve videolar içeren yapısal, yapısal olmayan veya yarı yapısal veriler içerebilir [99]. Üretilen veriler incelendiğinde sosyal veriler 3 şekilde elde edilebilmektedir. Yapısal, yapısal olmayan ve yarı yapısal olarak sınıflandırılan veriler gerçekleştirilecek çalışmanın türüne göre tercih edilebilmektedir. Yapısal olmayan ve yarı yapısal veriler geleneksel yöntemlerle işlenemediğinden dolayı [99] büyük veri uygulamaları bu konuda büyük önem kazanmıştır. Hatta yapısal olan veriler içerisinde değer üretme ve analiz konularında da geleneksel yöntemler yerini büyük veri uygulamalarına bırakmıştır. Veri türlerini özetlemek gerekirse [100];

- **Yapısal Veriler:** Sistematik bir şekilde kaydedilen bu veri tipi mevcut verilerin yaklaşık %20'sini kapsamakta ve programlama çalışmalarında kullanılmaktadır. Web logları, sensör verileri, kişisel bilgiler (ad, soyad vb.) bu kategori içerisinde yer almakta olup geleneksel yöntemlerle işlenmektedir.

- **Yarı Yapısal Veriler:** Kendini açıklayan veriler olarak da ifade edilebilmektedir. Yapısal ve yapısal olmayan modellerin bir karışımıdır. Her ne kadar tanımlayıcı veya tutarlı karakteristiğe sahip olsa da ilişkisel veri tabanı gibi katı kuralları yoktur.
- **Yapısal Olmayan Veriler:** Makine ve insan tarafından üretilmiş veriler olarak ayrılan bu veri türünde belirli bir yapı bulunmamaktadır. Uydu görüntüleri, bilimsel veriler, radar verileri, sosyal medya verileri, internet sayfası içerikleri, ses ve video görüntüleri bu tür verilerin kapsamında yer almaktadır.

Veri yapısı, boyutu ve işleme süreci göz önüne alındığında sosyal verilerin günümüzde büyük veri ile benzer bir süreçten geçtiği görülmektedir. Sosyal veriden değer üretme amacıyla gerçekleştirilen çalışmalar kapsamında büyük veri yaşam döngüsünün anlaşılmasının değer üretimi noktasında önemli olduğu değerlendirilmektedir. Büyük veri yaşam döngüsü [101] Şekil 4.2’de sunulmuştur.



Şekil 4.2. Büyük veri yaşam döngüsü

Büyük veri yaşam döngüsünün adımları ve içerikleri aşağıda detaylandırılmıştır.

- **Veri üretimi:** Bu adım sosyal medya gönderilerinden radar sensörlerine kadar verilerin oluşturulduğu adımdır.

- **Veri toplama:** Veri toplama (farklı kaynaklardan belirli formatlarda veri elde edilmesi), veri aktarma (verinin işleneceği ortama aktarılması) ve veri ön işleme (veri birleştirme, dönüştürme, azaltma ya da temizleme gibi) adımlarından oluşur.
- **Veri Depolama:** Verinin depolandığı ve birçok cluster'a dağıtıldığı altyapıdır. Etkinlik ve verimliliğinden bahsedebilmek için hata tolerancesini garanti etmelidir.
- **Veri İşleme ve Çözümleme:** Daha iyi kararlar verebilmek için veri madenciliği, makine öğrenmesi, derin öğrenme ve yapay zekâ süreçlerinin veriye uygulanarak faydalı değerler üretilmesidir.
- **Veri Görselleştirme:** Büyük veri yaşam döngüsünün en önemli adımı olan veri görselleştirme adımı işlenen veriden elde edilen değerlerin hesaplanmasının ve bu doğrultuda karar alınmasını sağlar.

Gerçekleştirilen tez çalışması kapsamında kişinin paylaşımları üzerinden bilgi ifşaları üzerine yoğunlaşılması nedeniyle diyaloglar başlığı altında sınıflandırılan verilerden konular, zamirler, anahtar kelimeler ve duygular çalışmanın odak noktasını oluşturmaktadır.

Verinin elde edilmesinin yanı sıra doğru bir değer üretilmesi için kalitesinin de yüksek olması gerekmektedir. Büyük verinin kalitesinin 4 boyutta değerlendirilmesi gerektiği düşünülmektedir. Bunlar [101];

- **Doğruluk:** verinin doğru bir şekilde kaydedilip edilmediğini ve gerçekçi değerlere sahip olup olmadığını.
- **Zamanlılık:** Verinin güncel olup olmadığı ve değişkenliği.
- **Uyumluluk:** Verinin format ve yapısına uygun olup olmadığını.
- **Eksiksizlik:** Tüm ilgili verilerin kaydedilip edilmediğidir.

Verinin kalitesinin belirlenmesi maksadıyla belirlenen boyutlar doğrultusunda Twitter ortamından verilerin toplanması ile oluşturulan veri setinin kişilerin paylaşımlarını olduğu gibi yansıtması nedeniyle doğruluk, en güncel son 200 tivit ve kullanıcının güncel profil bilgilerinin elde edilmesi ile oluşturulduğu için zamanlılık, tüm verilerin tivit objeleri doğrultusunda oluşturulması nedeniyle format ve yapı olarak uygun olması nedeniyle uyumluluk, gizlilik ve mahremiyet konusunda ihtiyaç duyulan Twitter üzerinden elde

edilebilecek metin tabanlı tüm verileri ihtiva etmesi nedeniyle kalite kriterlerini karşıladığı değerlendirilmektedir. Literatürde yer alan çalışmalarda;

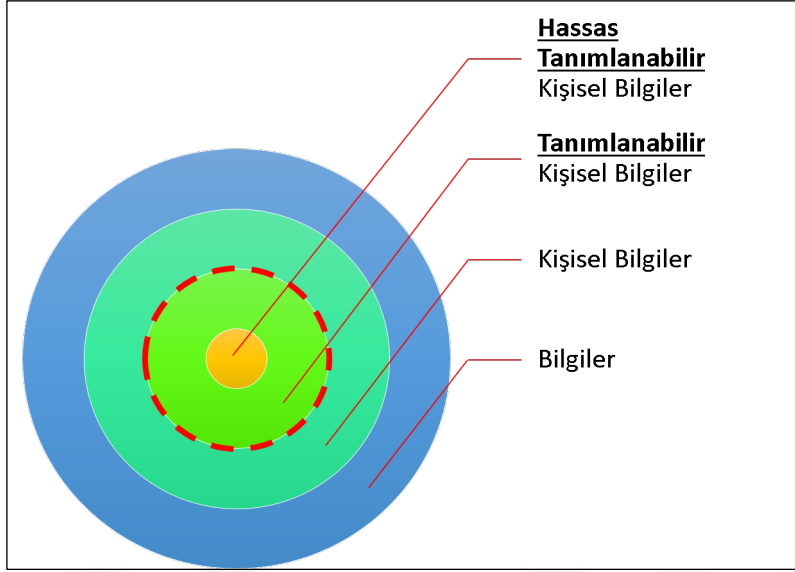
- Twitter'da kullanıcıların verilerine API ile kolay bir şekilde erişimin olması [102], [103], [104],
- Hashtag yapısı ile içerik ve konu tabanlı çalışmaların kolaylıkla gerçekleştirilmesine imkân sağlaması [102], [104],
- Twitter kullanıcılarının yapılan çalışmalar doğrultusunda bilinmeyen topluluğa kişisel bilgilerini paylaşmasının Facebook gibi diğer sosyal ağlara göre daha yüksek ihtimalli olması [103],
- Kullanıcıların diğer birçok sosyal medya ortamının aksine gerçek ismini kullanmak zorunda olmaması nedeniyle sağlanan anonimliğin kullanıcıları hassas verilerini paylaşma konusunda teşvik edici olması [104], [105],
- Anonimlik sayesinde daha az ön yargılı ve doğal bir şekilde çok geniş bir nüfusun kişisel deneyimlerini paylaşmasına imkân sağlaması [105],
- Diğer kullanıcıların verilerine erişim ya da görüntüleme maksadıyla gerçekleştirilen işlemlerde karşılıklı takip zorunluluğunun bulunmaması,

gibi nedenlerden dolayı çalışmaların çok büyük bölümünde verilerin Twitter ortamından elde edildiği görülmektedir.

Bahsedilen avantajlar değerlendirildiğinde veri elde edilmesi ve kişisel veri ifşalarına yönelik yapılacak bir çalışmada olumlu etkileri olacağı düşünüldüğünden çalışmada veri kaynağı olarak sosyal ağ platformlarından Twitter tercih edilmiştir.

4.2. Veri Sözlüklerinin Oluşturulması ve Verinin Elde Edilmesi

Sosyal medya ortamları kişilerin verilerini doğrudan ve istekleri doğrultusunda paylaşmaları nedeniyle sıklıkla veri ifşalarına sebep olmaktadır [106]. Ancak, paylaşılan her veri kişinin kimliğinin tanımlanmasına sebep olabilecek bir veri değildir. Kişisel verilerin 4 ana başlık altında sınıflandırıldığı çalışmada [106]. Hassas Tanımlanabilir Kişisel Bilgiler, Tanımlanabilir Kişisel Bilgiler, Kişisel Bilgiler ve Bilgiler olarak sınıflandırıldığı görülmekte olup görselleştirilmiş hali Şekil 4.3'te sunulmuştur.



Şekil 4.3. Mahremiyet çemberi

Kullanıcı verilerinin sınıflandırılmasına ilişkin gerçekleştirilecek model kapsamında sınıflandırmanın güçlü bir arka plana dayandırılabilmesi için amaçları arasında “Kişilerin mahremiyetini korumak” ifadesi yer alan Kişisel Verilerin Korunması Kanunu temel alınmış, bir kişinin kimliğinin belirlenebilmesini sağlayabilecek paylaşımların tespit edilebilmesi amaçlanmıştır.

Kişisel veri ifşa riski barındıran paylaşımların başarılı bir şekilde tespit edilebilmesi için öncelikle kişisel veri kavramının tanımlanması ve kişisel verilerin kaç farklı sınıf altında tespit edilmesi gerektiğinin belirlenmesi amaçlanmıştır. Kişisel Verilerin Korunması Kanunu’nda [107] “*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” kişisel veri olarak tanımlanmıştır. “*Kişilerin 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*” ise kanunda özel nitelikli kişisel veri olarak tanımlanmaktadır. Bu açıdan baktığımızda kişinin temel ve özel nitelikli bilgileri kişinin kişisel verilerini oluşturmaktadır. GDPR [108] ise kişisel veriyi “*Kimliği belirli veya belirlenebilir bir gerçek kişi (veri sahibi) ile ilgili herhangi bir bilgi*” olarak tanımlamaktadır. Tanımlanabilir gerçek kişi, doğrudan veya dolaylı olarak, özellikle isim, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı veya fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliği gibi bir tanımlayıcı ile tanımlanabilen

kişidir. KVKK'ya benzer şekilde GDPR, ırk, etnik köken, siyasi görüş, dini veya felsefi inanç, sendika üyeliği, genetik veriler, biyometrik veriler, sağlıkla ilgili veriler veya cinsel hayat veya cinsel yönelime ilişkin bilgilerin gerçek bir kişiyi benzersiz şekilde tanımlamak amacıyla işlenmesini yasaklamıştır.

Bahsedilen temel ve hassas nitelikli verilerin kapsamı değerlendirildiğinde tanımlarla benzer şekilde her türlü bilgi kapsama girebilmektedir. Kişisel verilerin ihlaline yönelik bir yargı kararında “*Kişinin; Türkiye Cumhuriyeti kimlik numarası, adı, soyadı, doğum tarihi, doğum yeri, nüfusa kayıtlı olunan yer (İl, İlçe, mahalle veya köy), anne ve baba adı, medeni hali (Evli, bekâr, boşanmış), nüfusa kayıtlı olduğu cilt ve aile sıra no, kan grubu, evlenme tarihi, boşanma tarihi ve mahkeme kararı bilgileri, adı-soyadı veya diğer kayıt düzeltmeleri, vatandaşlıktan çıkarılma bilgileri, evlatlık ilişkisi, adresi, dini, bitirilen okullar (ilk-orta-yüksek), hastalıkları, hastalıkları ile ilgili tahlil sonuçları (DNA bilgileri), mali durumu (servet, aldığı ücretler), ahlaki eğilimleri, zaafları, çevre ile ilişkileri, hatıra, anı ve günlüklerle ilgili defterindeki bilgileri, siyasi görüşü (oy verdiği partiler, üye olduğu dernekler), alışkanlıkları, sevdiği kitaplar veya gazeteler, alışveriş eğilimleri, vergi numarası, e posta adresi ve şifresi, banka bilgileri, bilgisayarının IP numarası, emeklilik ve kurum sicil numarası, aldığı ödüller, parmak izi, avuç içi izleri, mektupları, yazıları, kitapları, telefon numaraları, mesajları, fiziki kimliği (boy, kilo, engellilik durumu, ten rengi, göz rengi, saç rengi ve şekli, sesi, genel görünüm, ayak ve beden numarası) ve çok daha fazla bilgi kişisel veri kapsamında değerlendirilebilecektir.*” şeklinde belirtilmiştir.

Kanunlarda ve yargı kararlarında yer alan tanımlamalar da dikkate alındığında kişisel veri kavramı değerlendirilirken çok net sınırlar çizmenin ve kapsamını çok net bir şekilde belirlemenin mümkün olmadığı görülmektedir.

Kapsamın net olarak belirlenmesi mümkün olmasa da literatürde yer alan çalışmalarda az miktarda farklı türde örnekleri içeren verilerden oluşturulan veri setleri ile veri setinde yer almayan türdeki örneklerin de sınıflandırılmasının başarılı olarak gerçekleştirilebileceği görülmektedir [109]. Dolayısıyla veri toplama sürecinde arama kelimeleri ve etiketlemeler mümkün olduğunca farklılaştırılarak daha geniş bir kümeye ilişkin tespit yapılması amaçlanmış bu sayede kişisel veri kapsamına ilişkin dezavantajın etkisinin azaltılabileceği değerlendirilmiştir.

Kanun ve düzenlemede yer alan tanımlar doğrultusunda değerlendirdiğimizde Şekil 4.3'te sunulan mahremiyet çemberinin merkezinde yer alan hassas tanımlanabilir bilgiler ve tanımlanabilir bilgiler bu tez çalışmasının odak noktasını oluşturmuştur.

Mahremiyet çemberi ve kanunlarda yer alan tanımlamalar kapsamında yapılan değerlendirme doğrultusunda 7 ayrı sınıf altında kişisel verilerin sınıflandırılması amaçlanmıştır. Bunlar;

- Temel bilgiler,
- Siyasi görüş/düşünce,
- Dini görüş/inanç,
- Irk köken bilgisi,
- Cinsel yönelim,
- Ceza/mahkûmiyet bilgileri ve
- Sağlık bilgileri,

olarak sıralanabilir.

Söz konusu sınıfların içeriğinde yer alan verilerin sınırlarının belirlenmesi amacıyla Çizelge 3.1'de özet olarak sunulan materyal incelenmiş ve bu kapsamda arama anahtar kelimeleri belirlenmiştir. Bahsedilen arama kelimeleri doğrultusunda 21.12.2021-23.03.2022 tarihleri arasında tivitler ve replylar Twitter streaming API ile haftalık olarak toplanmıştır.

Söz konusu arama kelimeleri ve toplanan verilerin etiketlenmesi sonucunda elde edilen veri setlerine ilişkin detaylar takip eden alt başlıklarda sunulmuştur.

4.2.1. Temel bilgiler

Kişinin sosyal, kültürel, fiziksel ve ekonomik kimliğini yansıtacak her türlü veriye ilişkin tespitlerinin yapılması amacıyla toplanan veriler “Temel Bilgiler” olarak sınıflandırılmıştır. Kanunun gerekçesinde bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan verilerin yanı sıra, kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin verilerin de kişisel veri niteliğinde olduğu belirtilmiştir. Bu bilgilerin

yanı sıra eğitim, istihdam durumu, aile hayatı, ikamet adresi, kredi kartı gibi bilgiler de açıkça kişisel veri kapsamında kabul edilmiştir [110].

Veri mahremiyetinin sağlanması maksadıyla kurum ve firmalar tarafından kullanılan ürünlerin odak noktasını da bu sınıf içerisinde yer alan veriler oluşturmaktadır. Her ne kadar son yıllarda sağlık, siyasi görüş gibi alanlarda çalışmalar bulunsa da temel bilgiler mahremiyet denildiğinde ilk akla gelen verileri içermektedir.

Tez çalışması kapsamında Türkiye'deki yaygın meslek grupları, kişilerin ad, soyad, doğum tarihi gibi kimlik bilgileri, medeni hali, boyu, kilosu, göz rengi gibi fiziksel özellikleri, kan grubu, lakabı gibi özel bilgileri, yaşı, telefon numarası, adresi gibi iletişim bilgilerine ilişkin veri toplanmasına ve etiketlenmesine karar verilen arama kelimeleri Çizelge 4.1'de sunulmuştur.

Çizelge 4.1. Temel bilgiler sınıfı için kullanılan arama kelimeleri

Etiket	Arama Anahtar Kelimeleri	Etiketlenen Veri Sayısı
asker	Askerim, subayım, astsubayım, asker olduğum, uzman çavuşum	75
avukat	Avukatım	159
bekar	Bekarım	740
bosanmis	Boşandım, boşandık	107
boy	Boyum	264
dgdt	Doğum günüm, doğum tarihim	230
dogumyer	Doğum yerim	28
doktor	Doktorum, doktoruyum, doktor oldum	141
dul	Dulum, dul olduğum, dul olmam	101
emekli	Emekliyim	687
evli	Evliyim, evli olduğum, evli olmam	250
gozrenk	Göz rengim, gözümün rengi, gözlerimin rengi	8
hemsire	Hemşireyim	280
isci	İşçiyim	161
kangrup	Kan grubum	58
lakap	Lakabım	79
maas	Maaşım	196
memleket	Memleketim	716
memur	Memurum, memur olmam, memur olduğum	359
meslek	Mesleğim	128
muhendis	Mühendisim	200
ogretmen	Öğretmenim, öğretmen olduğum, öğretmen olmam	426
polis	Polisim	56
telno	Telefon numaram, telefonum	41
yasinda	Yaşımdayım	350
yasim	Yaşım	241
kvkk_ud	Tüm anahtar kelimelere ilişkin yapılan etiketlemelerde ifşa içermediği değerlendirilen tivitler bu sınıfta toplanmıştır.	7 330

Gerçekleştirilen veri toplama ve etiketleme çalışmaları doğrultusunda 26 farklı etiket altında 45 arama kelimesi kullanılarak 6 081 adedi kişisel veri içeren, 7 330 adet kişisel veri içermeyen olacak şekilde 13 411 adet tivitten oluşan veri seti oluşturulmuştur. Arama kelimeleri kapsamında Türkiye’de yaygın olan meslek gruplarına yer verilmiş olup ele alınmayan meslek gruplarına da veri setinde yer verilebilmesi maksadıyla “mesleğim” gibi genel ifadeler içeren kelimeler de veri toplama sürecinde kullanılmıştır.

İleride gerçekleştirilebilecek çalışmalarda söz konusu sınıfa ilişkin daha detaylı sınıflandırmaların yapılabilmesi için veriler ikili sınıflandırma şeklinde değil her verinin bulunduğu sınıfa göre etiketlenmiştir. Sonrasında veri etiketleri “kvkk_u” ve “kvkk_ud” olarak ikili sınıflandırmaya uygun olacak şekilde değiştirilerek sınıflandırma işlemleri gerçekleştirilmiştir.

Veri setinin karakteristiğinin anlaşılması maksadıyla TF-IDF yöntemi ile veri setinde en sık kullanılan 75 kelime ile oluşturulan kelime bulutu Şekil 4.4’te sunulmuştur.



Şekil 4.4. Temel bilgiler veri seti kelime bulutu

4.2.2. Siyasi görüş/düşünce

Literatürde siyasi görüş ve düşünce tespitine yönelik çalışmaların toplumsal düşünce tespitine yönelik çalışmaların sıklıkla gerçekleştirildiği görülmektedir. Bu çalışmalarda parti

liderlerine yönelik kişilerin duygularının analiz edilmesi [41], ülkede yöneticilerin değişimine vatandaşlar tarafından verilen tepkilerin ve sonucunda meydana gelen toplumsal olayların analizi [36], seçim sonuçlarının tahmini ve analizi [38], [39], partilerin sosyal medya hesabını ziyaret eden ve yorum, retivit gibi etkileşimde bulunan kullanıcılar üzerinden partilere olan sadakatin analizi [37], kullanıcıların politik eğilimlerini ölçmek [40] ve partileri destekleyen kullanıcıların cinsiyet analizlerine [37] ve kişilerin isimleri doğrultusunda kişilerin aidiyet duydukları partilerin tahminine [37] kadar birçok farklı çalışma gerçekleştirilmiştir. Yapılan çalışmalarda kişilerin paylaşımları kullanılarak doğrudan kişinin siyasi görüş ve düşüncesine yönelik risk barındıran tivitlerin tespitine yönelik bir çalışma bulunmamaktadır.

Tez çalışması kapsamında Türkiye’deki siyasi partiler ve yaygın politik temelli düşüncelere ilişkin veri toplanmasına karar verilen arama kelimeleri Çizelge 4.2’de sunulmuştur.

Çizelge 4.2. Siyasi görüş/düşünce sınıfı için kullanılan arama kelimeleri

Etiket	Arama Anahtar Kelimeleri	Etiketlenen Veri Sayısı
digerparti	TİP liyim, tipliyim, Rp liyim, refah partiliyim, rp liyim, İşçi partiliyim, memleket partiliyim, zafer partiliyim, hep liyim, hepliyim, partiliyim	53
akp	Akp liyim, ak partiliyim, akpliyim	561
Ataturk	Atatürkçüyüm	314
chp	Chp liyim, chpliyim	381
demokrat	Demokratım	45
hdp	Hdpliyim, hdp liyim	138
iyiparti	İyi partiliyim	28
kemalist	Kemalistim	87
komunist	Komünistim	53
liberal	Liberalim	45
mhp	Mhp liyim, mhpliyim	95
muhafazakar	Muhafazakarım	31
oyvermek	Partisine oy, oy verdim, oy vereceğim, partisine vereceğim, oyum	159
sagci	Sağcıyım, sağcıyız	47
solcu	Solcuyum, solcuyuz	150
spdeva	Saadet partiliyim, sp liyim, spliyim, devalıyım, deva partiliyim	33
ulkucu	Ülkücüyüm, ülkücüyüz	192
kvkk_ud	Tüm anahtar kelimelere ilişkin yapılan etiketlemelerde ifşa içermediği değerlendirilen tivitler bu sınıfta toplanmıştır.	2 815

Gerçekleştirilen veri toplama ve etiketleme çalışmaları doğrultusunda 17 farklı etiket altında 43 arama kelimesi kullanılarak 2 412 adedi kişisel veri içeren, 2 815 adet kişisel veri içermeyen olacak şekilde 5 227 adet tivitten oluşan veri seti oluşturulmuştur. Arama

Çizelge 4.3. Dini görüş/inanç sınıfı için kullanılan arama kelimeleri

Etiket	Arama Anahtar Kelimeleri	Etiketlenen Veri Sayısı
alevi	Aleviyim	393
ateist	Ateistim	732
budist	Budistim	7
deist	Deistim	159
dinim	Dinim	243
hristiyan	Hristiyanım	40
mezhep	Hanefi/Hanbeli/Maliki/Şafiyim, mezhebim, mezhebine tabiyim, Şiiyim	10
müslüman	Müslümanım, müslüman oldum, müslüman olduğum, müslüman olmam	377
yahudi	Yahudiyim	15
kvkk_ud	Tüm anahtar kelimelere ilişkin yapılan etiketlemelerde ifşa içermediği değerlendirilen tivitler bu sınıfta toplanmıştır.	2 043

Gerçekleştirilen veri toplama ve etiketleme çalışmaları doğrultusunda 9 farklı etiket altında 18 arama kelimesi kullanılarak 1 976 adedi kişisel veri içeren, 2 043 adet kişisel veri içermeyen olacak şekilde 4 019 adet tivitten oluşan veri seti oluşturulmuştur. Arama kelimeleri kapsamında ele alınmayan dini görüş ve inançların da yakalanabilmesi için "dinim", "mezhebim" gibi genel ifadeler içeren ve tüm dini görüş ve inançlara ilişkin paylaşımlar içerisinde yer alabilecek arama kelimeleri de veri toplama sürecinde kullanılmıştır.

İleride gerçekleştirilebilecek çalışmalarda söz konusu sınıfa ilişkin daha detaylı sınıflandırmaların yapılabilmesi için veriler ikili sınıflandırma şeklinde değil her verinin bulunduğu sınıfa göre etiketlenmiştir. Sonrasında veri etiketleri “kvkk_u” ve “kvkk_ud” olarak ikili sınıflandırmaya uygun olacak şekilde değiştirilerek sınıflandırma işlemleri gerçekleştirilmiştir. Veri setinin karakteristiğinin anlaşılması maksadıyla TF-IDF yöntemi ile veri setinde en sık kullanılan 75 kelime ile oluşturulan kelime bulutu Şekil 4.6’da sunulmuştur.



Şekil 4.6. Dini görüş/inanç veri seti kelime bulutu

4.2.4. Irk köken bilgisi

Literatürde gerçekleştirilen çalışmalar incelendiğinde kişilerin ırk ve etnik kökenlerinin tespitine yönelik bir çalışma bulunmadığı görülmüştür. Çok geniş bir araştırma alanını içeren bu sınıfta arama kelimelerinin oluşturulabilmesi maksadıyla Türkiye’deki yaygın ırk ve etnik kökenler doğrultusunda veri toplanmasına ve etiketlenmesine karar verilen arama kelimeleri Çizelge 4.4’te sunulmuştur.

Çizelge 4.4. Irk köken bilgisi sınıfı için kullanılan arama kelimeleri

Etiket	Arama Anahtar Kelimeleri	Etiketlenen Veri Sayısı
digerirk	Afganım, Çerkezim, Çerkesim, Arabım, Arnavutum, Tatarım, Gürcüyüm, Azeriyim, Bulgarım, Boşnakım, Boşnağım, Çeçenim, Çingeneyim, Makedonum, Yunanım, Zazayım	332
alman	Almanım	36
ermenii	Ermeniyim	52
kokenirk	Kökenimiz, Köken olarak, Kökenim, Kökenliyim, Irkımdan, Irkım	115
kurt	Kürdüm	1 052
suriyeli	Suriyeliyim	60
turkmen	Türkmenim	27
turk	Türküm	1 237
kvkk_ud	Tüm anahtar kelimelere ilişkin yapılan etiketlemelerde ifşa içermediği değerlendirilen tivitler bu sınıfa toplanmıştır.	1 941

alanını içeren bu sınıfta arama kelimelerinin oluşturulabilmesi maksadıyla yaygın cinsel yönelim ve eğilimlere yönelik veri toplanmasına ve etiketlenmesine karar verilen arama kelimeleri Çizelge 4.5’te sunulmuştur.

Çizelge 4.5. Cinsel yönelim sınıfı için kullanılan arama kelimeleri

Etiket	Arama Anahtar Kelimeleri	Etiketlenen Veri Sayısı
biseks	Biseksüelim, bisexüelim, biseksim, bisexim	22
digeryonelim	Erkeksiyim, kadınsıyım, aktifim, pasifim, cinsel yönelimim, homoseksüelim, ilgi duymuyorum	236
escinsel	Eşcinselim, eşcinselliğim, eşcinsel olmam, eşcinsel olduğum, eşcinsel olmaktan	16
gay	Gayım, gay olduğum, gay olmaktan, geyim, gey olduğum, gey olmaktan	291
lez	Lezim, lezbiyenim, lezbiyen olduğum, lezbiyen olmaktan	107
lgbt	Lgbt bireyiyim, lgbt savunucusuyum, lgbt destekçisiyim	26
trans	Transım, tarans bireyim, trans olduğum için, trans olmam	19
travesti	Travestiyim	1 053
kvkk_ud	Tüm anahtar kelimelere ilişkin yapılan etiketlemelerde ifşa içermediği değerlendirilen tivitler bu sınıfta toplanmıştır.	1 749

Gerçekleştirilen veri toplama ve etiketleme çalışmaları doğrultusunda 8 farklı etiket altında 34 arama kelimesi kullanılarak 1 770 adedi kişisel veri içeren, 1 749 adet kişisel veri içermeyen olacak şekilde 3 519 adet tivitte oluşan veri seti oluşturulmuştur. Veri setinin karakteristiğinin anlaşılması amacıyla TF-IDF yöntemi ile veri setinde en sık kullanılan 75 kelime ile oluşturulan kelime bulutu Şekil 4.8’de sunulmuştur.



Şekil 4.8. Cinsel yönelim veri seti kelime bulutu

İleride gerçekleştirilebilecek çalışmalarda söz konusu sınıfa ilişkin daha detaylı sınıflandırmaların yapılabilmesi için veriler ikili sınıflandırma şeklinde değil her verinin bulunduğu sınıfa göre etiketlenmiştir. Sonrasında veri etiketleri “kvkk_u” ve “kvkk_ud” olarak ikili sınıflandırmaya uygun olacak şekilde değiştirilerek sınıflandırma işlemleri gerçekleştirilmiştir.

4.2.6. Ceza/Mahkûmiyet bilgileri

Literatürde gerçekleştirilen çalışmalar incelendiğinde kişilerin ceza ve mahkûmiyet bilgilerinin tespitine yönelik bir çalışma bulunmadığı görülmüştür. Çok geniş bir araştırma alanını içeren bu sınıfta arama kelimelerinin oluşturulabilmesi maksadıyla kişinin mahkûmiyetini ve aldığı ceza bilgilerini içerebilecek ifadeler doğrultusunda veri toplanmasına ve etiketlenmesine karar verilen arama kelimeleri Çizelge 4.6’da sunulmuştur.

Çizelge 4.6. Ceza/Mahkûmiyet sınıfı için kullanılan arama kelimeleri

Etiket	Arama Anahtar Kelimeleri	Etiketlenen Veri Sayısı
beraat	Beraat ettim	113
ceza	Ceza aldım, cezası aldım, cezalandırıldım, ceza verdiler, cezalandırıldım, ceza yedim	321
dava	Davam devam, dava açtım, dava açtılar, davalık oldum, dosyam, dava ettiler	252
durusuma	Duruşmam var	24
gozalti	Gözaltına alındım, gözaltındayım,	67
hapis	Hapis yattım, hapse girdim, hapis cezası verdiler, hapis cezası aldım	200
ifade	İfade verdim, ifademi aldılar, ifadeye çağrıldım	119
ihraç	İhraç oldum, ihraç ettiler, ihraç edildim, iade ettiler, iade oldum	205
khk	KHKlıyım, KHK’lıyım, KHK’lıyız, KHKlıyız, KHK ile	213
mahkeme	Mahkemelik oldum, mahkemeye verdiler, mahkemem, mahkemeye verdim, mahkemem var	81
mahkumiyet	Mahkum ettiler, mahkum oldum, hakkımda mahkumiyet, mahkum edildim,	74
sicil	Sicilim, adli kaydım	8
tutuklu	Tutuklandım, tutukladılar, tutuklu kaldım,	79
yargi	Yargılandım, yargılanıyorum, yargılamam devam	119
kvkk_ud	Tüm anahtar kelimelere ilişkin yapılan etiketlemelerde ifşa içermediği değerlendirilen tivitler bu sınıfta toplanmıştır.	2 228

Gerçekleştirilen veri toplama ve etiketleme çalışmaları doğrultusunda 14 farklı etiket altında 50 arama kelimesi kullanılarak 1 875 adedi kişisel veri içeren, 2 228 adet kişisel veri içermeyen olacak şekilde 4 103 adet tivitten oluşan veri seti oluşturulmuştur.

durumları/salgınlar/hastalıklara ilişkin analiz ve duygu analizi gibi çalışmalar [115], [116] literatürde sıklıkla yer almakta ve bu konulara olan ilgi de gün geçtikçe artmaktadır.

İncelenen çalışmalarda genel olarak “psikolojik rahatsızlık”, “kalp krizi riski” gibi belirli hastalıklara özgü çalışmaların yapıldığı görülmektedir. Genel sağlık geçmişinin tespitine yönelik çalışmalar oldukça kısıtlıdır. Bu çalışmada kişilerin tüm sağlık geçmişine ilişkin verilerin sınıflandırılması amaçlanmıştır. Bu nedenle hastalık isimlerinin yanı sıra “ameliyatı oldum”, “değerlerim düşük”, “hastasıyım”, “hastası olduğumu” gibi genel arama kelimeleri de kullanılarak sağlık veri kümesinin tamamına ilişkin farklı hastalık bilgilerinin yakalanması amaçlanmıştır. Çalışma kapsamında veri toplama süreçlerinde kullanılan arama kelimeleri Çizelge 4.7’de sunulmuştur.

Çizelge 4.7. Sağlık Bilgileri sınıfı için kullanılan arama kelimeleri

Etiket	Arama Anahtar Kelimeleri	Etiketlenen Veri Sayısı
ameliyattahlil	Ameliyat olmam, tahlillerim, değerlerim düşük, tahlil sonuçlarım	272
astim	Astım hastasıyım	48
colyak	Çölyak hastasıyım	6
covid	Testim pozitif, covid oldum, korona oldum, karantinadayım	237
dehb	DEHBli olduğumu, DEHBli olduğumuzu, DEHBliyim	13
diyabet	Diyabet hastasıyım	11
engelli	Engelliyim	365
epilepsi	Epilepsi hastasıyım	12
fitik	Bel fıtığım var, fitik ameliyatı oldum, fitik hastasıyım	58
hamile	Hamileyim, hamile olduğumu	55
hastalik	Hastalığına yakalandım, rahatsızlığım var	212
hastasi	Hastasıyım, hastası olduğumu	196
hepatit	Hepatit hastasıyım, hepatit olduğumu	23
kalp	Kalp hastasıyım, kalp krizi geçirdim	88
kanser	Kanser hastasıyım, kanseri olduğumu, kanseri oldum	55
losemi	Lösemi hastasıyım, lösemi hastası olduğumu	33
migren	Migren hastasıyım, migrenim var, migrenim	30
msals	MS hastasıyım, ALS hastasıyım, MS/ALS hastası olduğumu	15
otistik	Otistik bireyim, otistiğim, otistik	15
romatizma	Romatizma hastasıyım, romatizma şikayetim var, romatizma hastası olduğumu, romatizmam	6
sedef	Sedef hastasıyım, sedef hastası olduğumu	5
seker	Şeker hastasıyım, şeker hastası olduğumu	68
tansiyon	Tansiyon hastasıyım, tansiyonum, tansiyon hastası olduğumu	73
tedavi	Tedavim, tedavisi görüyorum, tedavim başladı, tedavisine başladım	102
teshis	Teşhisi kondu, teşhisi koyuldu, teşhisi koydu, teşhis edildi	114
tiroid	Tiroid hastasıyım	43
yetmezlik	Kalp yetmezliği, böbrek yetmezliği, yetmezliği	37
kvkk_ud	Tüm anahtar kelimelere ilişkin yapılan etiketlemelerde ifşa içermediği değerlendirilen tivitler bu sınıfta toplanmıştır.	2 565

Gerçekleştirilen veri toplama ve etiketleme çalışmaları doğrultusunda 27 farklı etiket altında 66 arama kelimesi kullanılarak 2 192 adedi kişisel veri içeren, 2 565 adet kişisel veri içermeyen olacak şekilde 4 757 adet tivitten oluşan veri seti oluşturulmuştur.

İlberde gerçekleştirilebilecek çalışmalarda söz konusu sınıfa ilişkin daha detaylı sınıflandırmaların yapılabilmesi için veriler ikili sınıflandırma şeklinde değil her verinin bulunduğu sınıfa göre etiketlenmiştir. Sonrasında veri etiketleri “kvkk_u” ve “kvkk_ud” olarak ikili sınıflandırmaya uygun olacak şekilde değiştirilerek sınıflandırma işlemleri gerçekleştirilmiştir. Veri setinin karakteristiğinin anlaşılması amacıyla TF-IDF yöntemi ile veri setinde en sık kullanılan 75 kelime ile oluşturulan kelime bulutu Şekil 4.10’da sunulmuştur.



Şekil 4.10. Sağlık bilgileri veri seti kelime bulutu

4.2.8. Tüm kişisel bilgiler

Tez çalışması kapsamında bütüncül bir yaklaşımla kişilerin kişisel veri ifşa riski barındıran tivitlerinin tespiti amaçlanmaktadır. Bu nedenle Kişisel Verilerin Korunması Kanunu ile uyumlu olacak şekilde oluşturulan farklı sınıflara ait veri setlerinin birleştirilerek ikili sınıflandırmaya uygun hale getirilmesi amaçlanmıştır. Veri setinde yer alan sınıflar ve etiketli veri sayılarına ilişkin özet tablo Çizelge 4.8’de sunulmuştur.

4.3. Verinin Etiketlenmesi

Doğal dil işleme ile metinlerin otomatik olarak işlenmesi ve anlamlandırılması oldukça zordur. Çünkü metinlerin anlamları içerikten bağımsız olabilmektedir [117] Bu nedenle otomatik yüksek seviye anlamsal etiketleme günümüzde hala birçok alanda yeterli doğrulukla kullanılamamaktadır [118]. Bu nedenle doğal dil işleme süreçlerinde Gold Standard Corpora olarak adlandırılan manuel olarak etiketlenmiş veri setleri sıklıkla kullanılmaktadır. Yüksek kalitedeki bir Gold Standard Corpora ancak birden fazla uzmanın görüşü ve çoklu etiketleyiciler arasındaki uyum ile sağlanabilmektedir. Etiketleyicilerin kararları ise verinin belirsizliği, etiketleme kuralları ve etiketleyicinin yeteneklerinden etkilenmektedir [117]. Etiketlemelerin birden fazla etiketleyici tarafından ve manuel olarak gerçekleştirilmesi ise süreci oldukça maliyetli hale getirmektedir.

Süreçlerin maliyetlerinin azaltılması maksadıyla yapılan çalışmalarda birden çok alan uzmanı tarafından yapılan etiketlemelerde %90 üzerinde benzerlik elde edildiği, dolayısıyla tek bir alan uzmanı tarafından gerçekleştirilen etiketlemenin yeterli olacağı, alan uzmanı olmayan kişilerden oluşturulan çalışma gruplarında ise 4 kişilik bir ekibin %90 üzerinde benzerlik ile etiketlemeyi gerçekleştirebildiği, bu nedenle alan uzmanı olmayan grupların 4 kişiden oluşturulmasının yeterli olacağı tespit edilmiştir [119].

Çalışma kapsamında anahtar kelimeler doğrultusunda sınıflara ilişkin elde edilen veriler metin dosyaları halinde etiketlemeyi gerçekleştirecek etiketleyicilere teslim edilmiştir. Bu doğrultuda Gold Standard Corpora elde edilebilmesi için kurallar ve örnekler her bir sınıf için gönüllü olarak katılım sağlayan 4 etiketleyiciye aktarılmış, oluşturulan ekip tarafından tivitler Kişisel Verilerin Korunması Kanunu ile uyumlu (kvkk_u) ya da Kişisel Verilerin Korunması Kanunu ile uyumlu değil (kvkk_ud) şeklinde etiketlenmiştir.

Gerçekleştirilen veri etiketleme çalışmalarında;

- Tivit içerisinde kişinin açık ve net bir şekilde kendisine ait bir kişisel veri ifşasında bulunup bulunmadığı,
- Sağlık bilgilerine yönelik etiketleme çalışmalarında ise Kişisel Verilerin Korunması Kanunu ile uyumlu olarak kişinin doğrudan kendisine ya da aile bireylerinin sağlık geçmişine ilişkin net bir kişisel bilgi ifşasının yer alıp almadığı,

- Tivitlerin içerik ve anlamlarının kullanıcının tivit atma amacından bağımsız olarak salt metin üzerinden değerlendirilmesi (Dolandırıcılık gibi faaliyetler için kendine ait olmayan telefon numarasını kendisine ait gibi yazması, kişisel veri sınıfına girecek şekilde ancak yalan veya hatalı bilgi paylaşımında bulunulması vb.) ve
- Alaycı, dolaylı anlatım içerecek şekilde paylaşılan tivitlerin kişisel veri ifşası olarak değerlendirilmemesi (“Bunlar Müslümansa ben Yahudiyim” örneğinde olduğu gibi kişisel veri ifşası değil alaycı bir anlatım yapılmaktadır),

Çizelge 4.9. (devam) Örnek etiketlenmiş tivitler

Cinsel Yönelim	ablamin bisex olduğumu bilmesi ve düşündüğüm şeyi açıkça söylebilmemin verdiği rahatlık:) https://url	kvkk_u
	@username bu cinsel yönelim mevzusunun muhabbetini yapacağınıza kadın şiddeti tecavüzü ve tacizi aynı şekilde hayvan haklarında da bu kadar üstünde dursanız zaten bir şeyler hallolma yoluna girer	kvkk_ud
Ceza/Mahkûmiyet Bilgileri	@username Sosyal medyada hakaret adı altında onbinler ce insan mahkemeye verilerek ..avukatlar insanlardan inanılmaz derecede para istiyorlar..bu olaya acilen el atılması gerekir ..en büyük mağduriyeti yaşayan benim ...58 gün hapis bile yattım	kvkk_u
	3 gün takip cezası aldım... helali hoş olsun... mutlaka takiplere geri döneceğim 📌 @username listelerinde takibe dönenler için herkese günaydınlar 🤖 ♂ 🤖 ♂ 🤖 ♂	kvkk_ud
Sağlık Bilgileri	#TehlikeliPlan Merhaba bir umutla bu mesajı size yazıyorum ben 5 yıldır kolon ve rektum kanseri ile mücadele ediyorum bu 5 yıl içinde bir böbreğimi ve bütün bağırsaklarımı kaybettim yatalağım 100'de/94 ağır engelliyim lütfen yardım eli uzatın çok zordayım tlfon 0538(telno)	kvkk_u
	@username Senden küçük ama senden daha yaşlı gösteren insanları stalklama hastalığına yakalanmamışsın daha	kvkk_ud

4.4. Veri Ön İşleme

Sınıflandırma modelinin oluşturulabilmesi için veri setinin ön işlemden geçirilmesi gerekmektedir. Birçok sınıflandırma çalışmasında, önceden işlenmiş verilerle daha iyi sonuçlar elde edilmiştir [120]. Daha küçük vektör uzayına ve daha yüksek performansa sahip olmak için ön işleme adımları uygulamaktadır. Bu çalışma kapsamında Türkçe için geliştirilmiş açık kaynak Zemberek kütüphanesinin [121] kullanılmasına karar verilmiş ve Java programlama dilinde kod geliştirmeleri gerçekleştirilmiştir. Zemberek kütüphanesi içerisinde yer alan modüller Çizelge 4.10'da sunulmuştur.

Çizelge 4.10. Zemberek-NLP modülleri [121]

Modüller	Açıklama
Core	Sözlüğe kelime ekleme, kelime analizi gibi yardımcı fonksiyonları
Morphology	Türkçe morfolojik analiz, kelime üretimi, kök çıkarımı, anlamsal kök çıkarımı
Tokenization	Cümle ve kelime sınırlarının belirlenmesi
Normalization	Yazım denetimi, hatalı yazım düzeltme, kelime önerme
NER	Türkçe Varlık İsmi Tanıma modeli oluşturulması
Classification	FastText tabanlı metin sınıflandırma
Language Identification	Metin dillerinin tanınması
Language Modeling	Dil modeli sıkıştırma
Applications	Konsol uygulamaları
gRPC Server	Diğer dilerden gRPC sunucusuna erişim

Söz konusu modüllerden “core”, “morphology”, “tokenization”, “Normalization”, “NER”, “Classification” ve “Language Identification” adlı modüllere ilişkin örnek çalışmalar gerçekleştirilmiş ve ön işleme adımlarında ihtiyaç duyulan modüller çalışmaya entegre edilmiştir.

Ortaya konulan büyük veri işleme modeli doğrultusunda problemin tanımlanması ve verilerin elde edilmesi bölümü hali hazırda tamamlanmış olup büyük veri çalışmalarında çok önemli adımlardan biri olan veri ön işlemden geçirilmesi adımına yönelik araştırmalar gerçekleştirilmiştir. Literatürde yer alan çalışmalar [48], [64], [69], [122], [123] genel olarak değerlendirildiğinde veri ön işleme sürecinde sıklıkla uygulanan işlemler şu şekildedir;

- Çalışılacak dil dışındaki dillerde veri mevcut ise silinmesi,
- Çift kayıtlar varsa silinmesi,
- Konu ile ilgili olmayan, analize katkı sağlamayacak kayıtların silinmesi,
- Noktalama işaretlerinin silinmesi,
- Durak kelimeler (Stop words) olarak adlandırılan cümleye anlamsal olarak katkı sağlamayan kelimelerin silinmesi,
- Rakamsal ifadelerin silinmesi,
- URL’lerin silinmesi,
- @... şeklinde etiketlenmiş kullanıcıların silinmesi,
- #Hashtaglerin silinmesi,
- Tüm metinlerin küçük harfe dönüştürülmesi,
- Çalışma kapsamında belirlenen sayıdan daha az kelimedenden oluşan kayıtların silinmesi,
- Tokenization yapılması,
- Kök çıkarımı (Stemming) yapılması,

Veri setinin yapısına, araştırmada ele alınan probleme ve kullanılan algoritma/model/yönteme bağlı olarak uygulanacak ön işleme adımlarının sayısı ve sırasında değişiklikler olduğu görülmektedir. Bu tez çalışması kapsamında elde edilen veri seti aşağıda sunulan sırada ön işleme adımlarından geçirilmiştir.

- Çift kayıtların silinmesi,

- Kelimelerle birleşik yazıldığında veri ön işleme sürecinde hatalı sonuçlara sebep olduğu tespit edilen özel karakterler, noktalama işaretleri ve emojilerin silinmesi (Mention, hashtag ve etiketlemede kullanılan @, #, _ özel karakterleri ve bu karakterler başlayan metinler hariç)
- Eksik harf, hatalı yazım gibi kullanıcı tarafından gerçekleştirilen hataların giderilmesi maksadıyla normalizasyon işleminin yapılması,
- Mentionların ve hashtaglerin silinmesi,
- URL adreslerin silinmesi,
- Türkçe’de bir kelimenin birden fazla anlamı bulunabilmesi nedeniyle kelimenin metin içindeki anlamına en yakın kök değerini tespit etmek için anlamsal kök çıkarımı uygulanması,
- Anlamsal katkısı olmadığı değerlendirilen durak kelimelerin silinmesi,
- Tüm kelimelerin küçük harfe dönüştürülmesi,
- Çift kayıtların silinmesi (Ön işleme adımları tamamlandıktan sonra çift kayıtlar oluşabilmektedir).

Çalışma kapsamında elde edilen veri setinden seçilen tivate uygulanan veri ön işleme sürecine ilişkin örnek gösterim Çizelge 4.11’de sunulmuştur.

Çizelge 4.11. Veri ön işleme adımları örnek gösterim

Orijinal Tivit	#22aralık1914 #Sarıkamış şehitlerimize Allah'tan rahmet diliyorum. Onlar bu vatan için soğukta donark ölen KARDELENLER... Mekânları cennet olsun. ☆☆☆NE MUTLU TÜRK'ÜM DİYENE☆☆☆ https://url
Karakter Temizleme	#22aralık1914 #Sarıkamış şehitlerimize Allah'tan rahmet diliyorum. Onlar bu vatan için soğukta donark ölen KARDELENLER... Mekânları cennet olsun. ☆☆☆NE MUTLU TÜRK'ÜM DİYENE☆☆☆ https://url
Hatalı Yazım Düzeltme	#22aralık1914 #Sarıkamış şehitlerimize Allah tan rahmet diliyorum Onlar bu vatan için soğukta donark ölen KARDELENLER Mekânları cennet olsun NE MUTLU TÜRK ÜM DİYENE https://url
Mention ve Hashtag silme	#22aralık1914 #Sarıkamış şehitlerimize Allah tan rahmet diliyorum Onlar bu vatan için soğukta donarak ölen KARDELENLER Mekânları cennet olsun NE MUTLU TÜRK ÜM DİYENE https://url
URL adreslerinin silinmesi	şehitlerimize Allah tan rahmet diliyorum Onlar bu vatan için soğukta donarak ölen KARDELENLER Mekânları cennet olsun NE MUTLU TÜRK ÜM DİYENE https://url
Anlamsal kök çıkarımı ve küçük harfe dönüştürme	şehitlerimize Allah tan rahmet diliyorum Onlar bu vatan için soğukta donarak ölen KARDELENLER Mekânları cennet olsun NE MUTLU TÜRK ÜM DİYENE
Durak Kelimelerin silinmesi	şehit allah rahmet dilemek o bu vatan için soğuk donmak ölmek kardelen mekan cennet olmak ne mutlu türk demek
Çıktı	şehit allah rahmet dilemek vatan soğuk donmak ölmek kardelen mekan cennet olmak mutlu türk demek

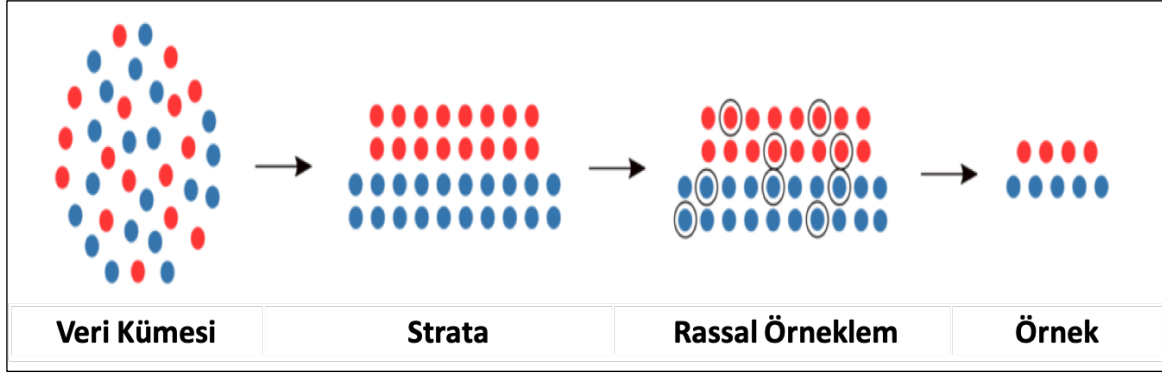
Zemberek kütüphanesi kullanılarak hatalı yazım düzeltme (normalizasyon), anlamsal kök çıkarımı, mention ve hashtaglerin çıkarılması gibi doğal dil işleme adımları gerçekleştirilmiştir. Benzer şekilde Java programlama dili üzerinde geliştirilen program parçacığı ile anlamsal katkısı olmadığı değerlendirilen durak kelimeler (stopwords) silinmiş tüm kelimeler küçük harfe dönüştürülerek veri setine son hali verilmiştir.

4.5. Test ve Eğitim Veri Setlerinin Hazırlanması

Çalışma kapsamında temel bilgiler, siyasi görüş/düşün, din, görüş/inanç, ırk köken bilgileri, cinsel yönelim, ceza/mahkûmiyet bilgileri ve sağlık bilgilerini içeren tivitlerden oluşan 7 farklı veri seti elde edilmiştir. Söz konusu veri setleri birleştirilerek tüm kişisel veri ifşalarının genel bir ikili sınıflandırma ile elde edilmesine yönelik ayrı bir veri seti daha elde edilmiştir.

Dil modelleri oluşturulurken eğitim ve test verilerinin oluşturulması adımı özellikle dengesiz (Unbalanced) veri setleri ile yapılan çalışmalarda yüksek doğrulukta sonuçlar alınabilmesi açısından çok önemlidir. Eğitim ve test setlerinin araştırmanın amacına uygun şekilde oluşturulması amacıyla kullanılan birçok farklı örnekleme metodu bulunmaktadır. Literatürde örnekleme metotları simple, random, stratified, cluster ve multistage sampling türlerini içeren olasılıksal ve purpose, convenience, snowball ve quota sampling türlerini içeren olasılıksal olmayan olarak iki ana başlık altında sınıflandırılmaktadır [124].

Hazırlanan veri setleri ele alındığında her bir etikete ait veri sayılarının farklı olması nedeniyle, çalışma kapsamında hazırlanan tüm veri setlerinde yer alan toplam 107 farklı etikete sahip verilerin orantılı olarak tüm eğitim ve test setlerinde yer alması gerekmektedir. Aksi takdirde bazı katlamalarda olduğundan düşük bazı katlamalarda olduğundan yüksek sonuçlarla karşılaşılabilir. Bu nedenle tabakalı örnekleme modelinin araştırmada kullanılacak veri setine uygun olduğu değerlendirilmiştir. Bu modelde tüm etiketlere ait veriler strata adı verilen alt gruplara ayrılmakta sonrasında eğitim ve test setlerine eşit oranda temsil edilecek şekilde rastgele dağıtılmaktadır [124]. Örnek gösterim Şekil 4.12’de sunulmuştur.



Şekil 4.12. Tabakalı Örnekleme yöntemi örnek gösterim (Türkçeleştirilmiştir) [125]

Stratified sampling ve 10 katlamalı çapraz doğrulama olacak şekilde verinin eğitim ve test veri seti olarak ayrıştırılması için Python programlama dilinde Scikit-Learn kütüphanesi kullanılmıştır [126]. İşlemler gerçekleştirilirken öncelikle her bir sınıf için veriler tüm etiketler dikkate alınarak eğitim ve test setleri olarak ayrıştırılmış sonrasında etiketler “kvkk_u” ve “kvkk_ud” olacak şekilde ikili sınıflandırmaya uygun hale getirilmiştir.

5. MODELLERİN OLUŞTURULMASI VE TEST EDİLMESİ

Literatürde yer alan çalışmalarda verinin ön işleminden geçirip hazır hale getirilmesinden sonra bir değer üretebilmek için makine öğrenmesi, derin öğrenme gibi yöntemlerin uygulandığı metin madenciliği, düşünce madenciliği, metin sınıflandırması gibi yöntemlerin sıklıkla kullanıldığı görülmektedir. Danışmanlı ve danışmansız makine öğrenmesi yöntemleri kullanılarak farklı araştırma alanlarında sınıflandırma ve duygu analizine yönelik çalışmalar gerçekleştirilmiş olup çalışmalarda sıklıkla tercih edilen ve yüksek başarımla elde edilen algoritmalar aşağıda listelenmiştir [39], [44], [48], [61], [99], [127], [128], [129];

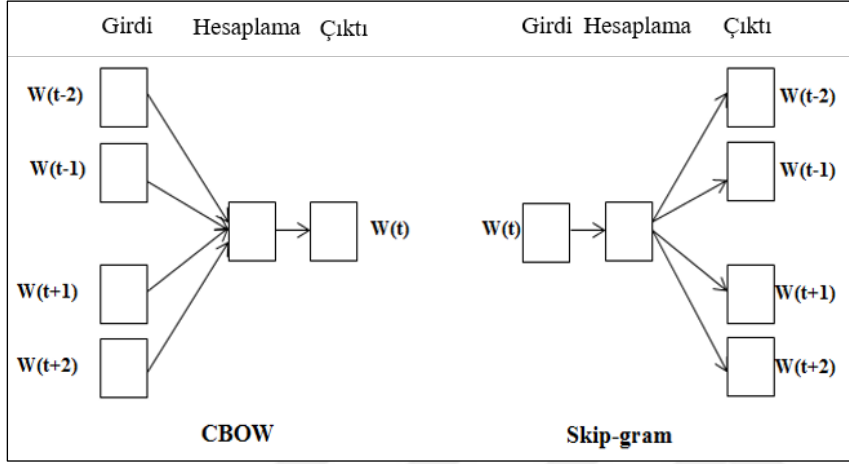
- Naive Bayes,
- K-Nearest Neighbours,
- Random Forest Classifier,
- Logistic Regression,
- LDA,
- CRP,
- Support Vector Machine,
- Ensemble Voted Classifier.

Geleneksel makine öğrenmesi ve derin öğrenme algoritmaları ile gerçekleştirilen çalışmalar daha çok istatistiksel yöntemlere dayanmakta anlamsal ve içeriksel değerler göz ardı edilmektedir. Aynı zamanda geleneksel yöntemler ile gerçekleştirilen çalışmalarda kaynak tüketimi çok yüksek olmakta, özellikle büyük boyutlu veri setleri ile gerçekleştirilen çalışmalarda performans ve hız konularında sıkıntılar yaşanmaktadır. Bu çalışma kapsamında söz konusu dezavantajların ortadan kaldırılmasına yönelik geliştirilen fastText ve BERT transformer modelleri ile eğitim ve test işlemleri gerçekleştirilmiş olup söz konusu modellerin mimarileri, modellerin değerlendirilmesinde kullanılan test metrikleri ve elde edilen modellerin test sonuçları detaylı olarak sunulmuştur.

5.1. fastText

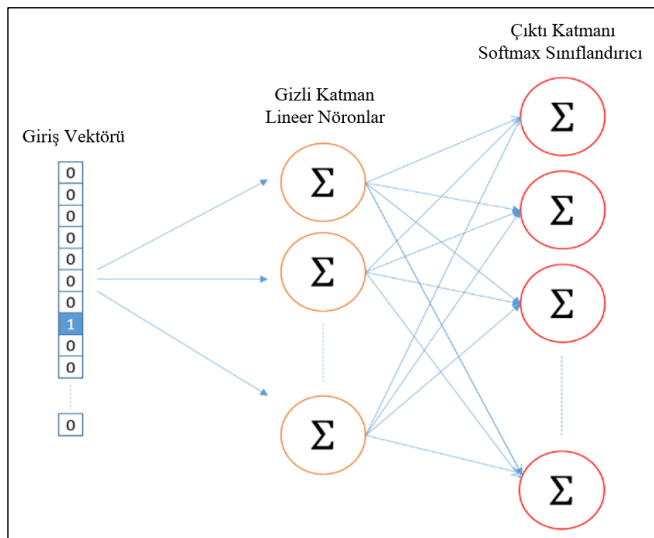
Geleneksel makine öğrenmesi yöntemlerinde karşılaşılan dezavantajların ortadan kaldırılmasına yönelik yapılan çalışmalarda kelime gömme ve kelime temsili yöntemleri

geliştirilmiştir [130]. Kelime temsili yöntemi benzer anlamlı kelimelerin birbirilerine yakın olarak gösterilmesi yöntemi olup 2013 yılında geliştirilmiştir. Geliştirilen tahmin temelli bu model [131], büyük miktarda yapılandırılmamış metin verisinden kelimelerin vektör temsillerinin yüksek verimlilikle öğrenilmesi için etkili bir yöntem olan CBOW ve Skip-gram modellerini önermektedir. Model mimarisi Şekil 5.1’de görsel olarak sunulmuştur [130].



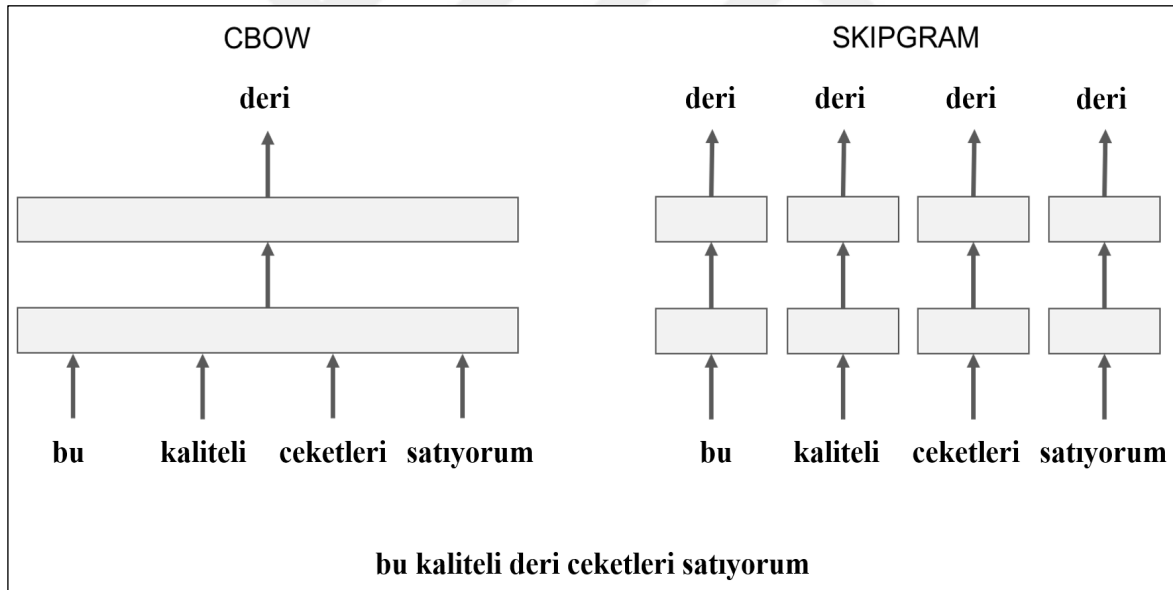
Şekil 5.1. CBOW ve Skip-gram model mimarisi (Türkçeleştirilmiştir) [130]

CBOW modelinde merkezdeki kelimeyi bulmak için çevreleyen kelimeler kullanılırken Skip-gram modelinde cümle ya da dokümandaki çevreleyen kelimeleri tahmin etmek için merkez kelime kullanılmaktadır. Yapay sinir ağı temelli bir model olan word2vec için örnek gösterim Şekil 5.2’de sunulmuştur.



Şekil 5.2. Yapay sinir ağı temelli word2vec mimarisi (Türkçeleştirilmiştir) [154]

fastText ise Facebook araştırma ekibi tarafından 2016 yılında Word2Vec modelinin eklentisi olarak geliştirilmiştir [132], [133]. fastText, metin sınıflandırma ve kelime temsili için geliştirilmiş bir kütüphanedir. Metni, daha sonra dille ilgili herhangi bir görevde kullanılabilecek sürekli vektörlere dönüştürür. Word2Vec modeline benzer olarak kelime gösterimlerinin hesaplanması amacıyla CBOW ve Skip-gram modelleri kullanılmıştır [133]. Word2vec modeline temel katkı alt kelime bilgilerini dikkate alarak gerçekleştirilmiştir [134]. Bu yöntemde kelimeler karakter n-gramlar olarak öğrenilmekte olup kelimeler belirlenen karakter n-gramların toplamı olarak gösterilmektedir. Doğrudan kelimeler yerine karakter n-gramlar ile oluşturulan bu alt kelime bilgileri yapay sinir ağına girdi olarak verilmektedir. fastText'in mimarisi Word2Vec modelinde önerilen CBOW modeline benzemektedir. Ancak, cümle içerisinde yer alan kelimelerin sırasının da sınıflandırma sürecinde kullanılabilmesi amacıyla n-gram özelliklerini de kullanmaktadır [129]. Bahsedilen 2 modelin farklılıkları Şekil 5.3'te örnek olarak sunulmaktadır.



Şekil 5.3. CBOW ve Skip-gram modelleri örneği (Türkçeleştirilmiştir) [133]

fastText modeli 3 katmandan oluşmaktadır: giriş katmanı, gizli katman ve çıktı katmanı. Girdi katmanında kelime sayısı ve n-gram özellikleri kullanılır, gizli katman maksimum olasılığı hesaplar ve çıktı olarak ağırlıklara ve model parametrelerine dayalı bir Huffman ağacı oluşturulur [135]. Önceden tanımlanmış sınıflar üzerindeki olasılık dağılımını hesaplamak için kullanılır Softmax fonksiyonu kullanılır [129].

Literatürde yer alan çalışmalar ve temel mimarisi değerlendirildiğinde fastText'in metin sınıflandırma işlemlerinde birçok avantaj sağladığı görülmektedir. Bunlar;

- fastText kütüphanesi, yüksek performanslı, hızlı ve kaynak tüketiminin az olması ile beraber derin öğrenme yöntemleri ile karşılaştırılabilecek düzeyde başarımlar elde edilmesi [129], [136],
- Türkçe gibi morfolojik açıdan zengin dillerde başarımları arttıran alt kelime bilgisini kullanması [134], [137],
- Veri setinde yer almayan kelimeleri karakter n-gram yöntemini kullanması nedeniyle tanınması ve literatürde Türkçe metinler ile gerçekleştirilen sınıflandırma çalışmalarda yüksek başarılı dil modellerinin [137], [138], [139], [140], oluşturulmasına imkân sağlaması,

olarak özetlenebilir.

Söz konusu avantajların tez çalışması kapsamında ele alınan problemin çözümüne katkı sağlayacağı değerlendirildiğinden çalışma kapsamında gerçekleştirilecek sınıflandırma işleminde fastText modeli tercih edilmiştir. Model eğitim sürecinde 2 ve daha fazla kelime kullanılarak gerçekleştirilen eğitimlerde daha iyi sonuçlar elde edilen Skip-gram modeli kullanılarak sınıflandırma işlemleri gerçekleştirilmiştir.

fastText ile model eğitimlerini gerçekleştirirken 2 farklı yöntem kullanılmıştır. İlk olarak, en iyi eğitim ve test sonuçlarını elde edebilmek ve uygulamaya entegre edilecek modeli oluşturabilmek için Çizelge 5.1'de sunulan parametreler belirtilen değer aralıklarında birçok farklı kombinasyonla çalıştırılarak elde edilen en iyi sonuçlar tespit edilmiştir.

Çizelge 5.1. Model eğitimlerinde kullanılan parametreler

Parametreler	Değer/Aralık	Standart Değer
dim (Dimension)	50-300	100
lr (Learning rate)	0,1-0,6	0,1
Epoch size	5-75	5
ws (Windows size)	3-5	5
wordNgrams	3-6	1

İkinci olarak fastText'in belirlenen bir süre içerisinde en iyi parametrelerin otomatik olarak bulunabilmesi amacıyla geliştirilmiş "Autotune" özelliği kullanılmıştır. Modellerin her 2 yöntemle gerçekleştirilen eğitim ve test süreçlerinde daha önceki bölümlerde detayları açıklandığı şekilde 10 katlamalı çapraz doğrulama için tabakalı örnekleme yöntemi ile hazırlanan veri setleri kullanılmıştır.

Oluşturulan modellerin performanslarının ölçülebilmesi için sıklıkla kullanılan metrikler tercih edilmiştir. Modellerin performanslarının ölçülmesinde; doğruluk, kesinlik, geri çağırma ve F1 skorları kullanılmıştır. Bu metrikler hesaplanırken 4 parametreye ihtiyaç duyulmaktadır. Bahse konu parametreler ve açıklamaları aşağıda sunulmuştur.

- TP (True Positive) : Doğru tahmin edilmiş pozitif sınıf.
- TN (True Negative) : Doğru tahmin edilmiş negatif sınıf.
- FP (False Positive) : Yanlış tahmin edilmiş pozitif sınıf.
- FN (False Negative) : Yanlış tahmin edilmiş negatif sınıf.

Model performansının ölçülmesinde kullanılan metrikler ve hesaplamalarda kullanılan formüller Çizelge 5.2'de sunulmuştur [141].

Çizelge 5.2. En sık kullanılan model performans metrikleri

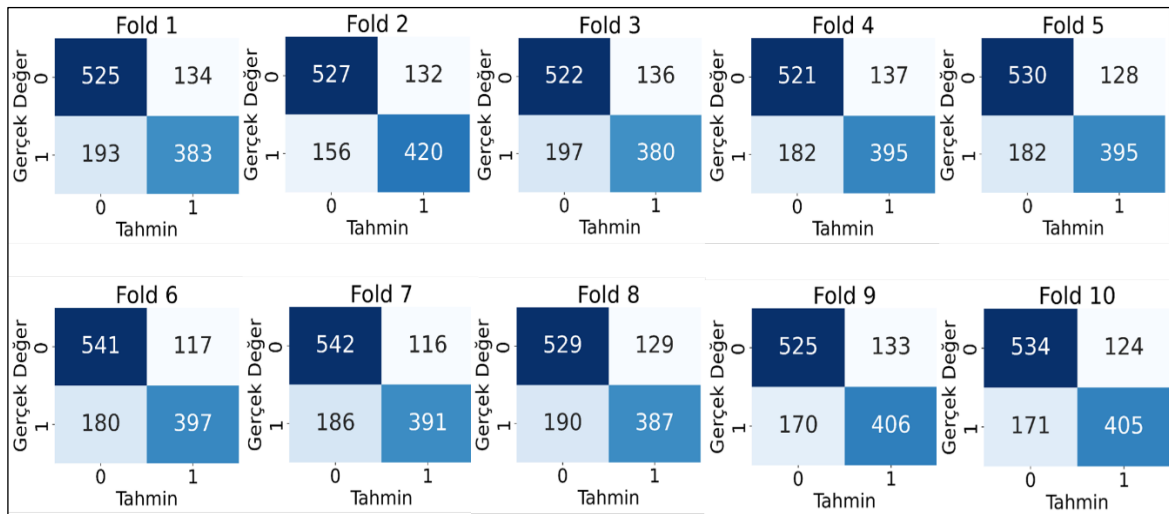
Metrik	Formül	Açıklama
Doğruluk	$\frac{TP + TN}{TP + TN + FP + FN}$	Modelin genel performansı
Kesinlik	$\frac{TP}{TP + FP}$	Doğru tahminlerin kesinliği
Geri Çağırma	$\frac{TP}{TP + FN}$	Gerçek pozitif örneklerin oranı
F1 Skoru	$\frac{2TP}{2TP + FP + FN}$	Dengesiz sınıflar için yaratılan hibrit metrik

fastText ikili metin sınıflandırma işlemlerinde doğruluk, kesinlik, geri çağırma ve F1 skoru gibi metrikleri doğrudan hesaplamamaktadır. Bu nedenle, söz konusu metriklerin hesaplanmasına imkân sağlayan Scikit-Learn kütüphanesinin [126] fonksiyonları kullanılarak yazılan kod parçacığı ile performans metrikleri hesaplanmıştır. Elde edilen sonuçlar Çizelge 5.3.-5.10'da, karmaşıklık matrisleri Şekil 5.4 - 5.11'de sunulmuştur.

Çizelge 5.3. Temel Bilgiler sınıfı model performansı

Temel Bilgiler	Etiket	Kelime Sayısı	Ort. Kayıp	Kesinlik	Geri Çağırma	F-1 Skoru	Doğruluk	Örnek Sayısı
Katlama 1	Kvkk_u	8 973	0,062	0,741	0,665	0,701	0,735	576
	Kvkk_ud			0,731	0,797	0,763		659
Katlama 2	Kvkk_u	8 979	0,053	0,761	0,729	0,745	0,767	576
	Kvkk_ud			0,772	0,800	0,785		659
Katlama 3	Kvkk_u	8 932	0,05	0,736	0,659	0,695	0,730	577
	Kvkk_ud			0,730	0,793	0,758		658
Katlama 4	Kvkk_u	8 988	0,051	0,742	0,685	0,712	0,742	577
	Kvkk_ud			0,741	0,792	0,766		658
Katlama 5	Kvkk_u	8 980	0,052	0,755	0,685	0,718	0,749	577
	Kvkk_ud			0,744	0,805	0,774		658
Katlama 6	Kvkk_u	8 980	0,053	0,772	0,688	0,728	0,760	577
	Kvkk_ud			0,750	0,822	0,785		658
Katlama 7	Kvkk_u	9 012	0,055	0,771	0,678	0,721	0,755	577
	Kvkk_ud			0,745	0,824	0,782		658
Katlama 8	Kvkk_u	9 020	0,053	0,750	0,671	0,708	0,742	577
	Kvkk_ud			0,736	0,804	0,768		658
Katlama 9	Kvkk_u	8 999	0,054	0,753	0,705	0,728	0,754	576
	Kvkk_ud			0,755	0,798	0,776		658
Katlama 10	Kvkk_u	8 984	0,054	0,766	0,703	0,733	0,761	576
	Kvkk_ud			0,757	0,812	0,784		658
Ortalama		8 985	0,054	0,750	0,690	0,720	0,750	577
				0,750	0,800	0,770		658

Temel Bilgiler sınıfına ilişkin hazırlanan her bir katlama için gerçekleştirilen testler sonucunda elde edilen karmaşıklık matrislerine ilişkin ekran görüntüleri Şekil 5.4'te sunulmuştur.

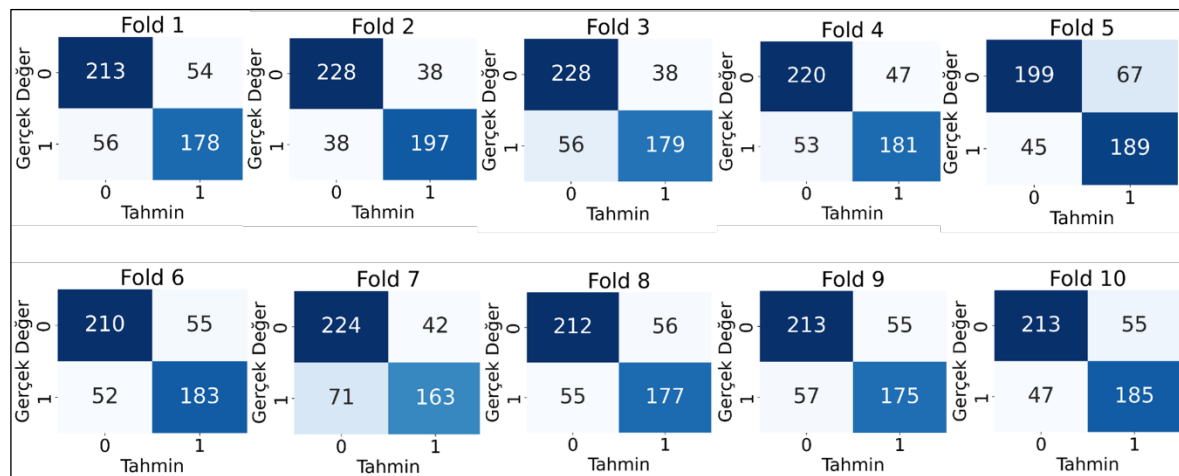


Şekil 5.4. Temel bilgiler sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları

Çizelge 5.4. Siyasi Görüş/Düşünce sınıfı model performansı

Siyasi Görüş	Etiket	Kelime Sayısı	Ort. Kayıp	Kesinlik	Geri Çağırma	F-1 Skoru	Doğruluk	Örnek Sayısı
Katlama 1	Kvkk_u	6 092	0,024	0,767	0,761	0,764	0,780	234
	Kvkk_ud			0,791	0,797	0,794		266
Katlama 2	Kvkk_u	6 086	0,056	0,838	0,838	0,838	0,848	235
	Kvkk_ud			0,857	0,857	0,857		266
Katlama 3	Kvkk_u	6 099	0,055	0,825	0,762	0,792	0,812	235
	Kvkk_ud			0,803	0,857	0,829		266
Katlama 4	Kvkk_u	6 080	0,024	0,794	0,774	0,784	0,800	234
	Kvkk_ud			0,806	0,824	0,815		267
Katlama 5	Kvkk_u	6 102	0,035	0,738	0,808	0,771	0,776	234
	Kvkk_ud			0,816	0,748	0,780		266
Katlama 6	Kvkk_u	6 130	0,054	0,769	0,779	0,774	0,786	235
	Kvkk_ud			0,802	0,792	0,797		265
Katlama 7	Kvkk_u	6 123	0,057	0,795	0,697	0,743	0,774	234
	Kvkk_ud			0,759	0,842	0,799		266
Katlama 8	Kvkk_u	6 099	0,055	0,760	0,763	0,761	0,778	232
	Kvkk_ud			0,794	0,791	0,793		268
Katlama 9	Kvkk_u	6 089	0,044	0,761	0,754	0,758	0,776	232
	Kvkk_ud			0,789	0,795	0,792		268
Katlama 10	Kvkk_u	6 073	0,025	0,771	0,797	0,784	0,796	232
	Kvkk_ud			0,819	0,795	0,807		268
Ortalama		6 097	0,043	0,780	0,770	0,780	0,790	234
				0,800	0,810	0,810		267

Siyasi Görüş/Düşünce sınıfına ilişkin hazırlanan her bir katlama için gerçekleştirilen testler sonucunda elde edilen karmaşıklık matrislerine ilişkin ekran görüntüleri Şekil 5.5'te sunulmuştur.

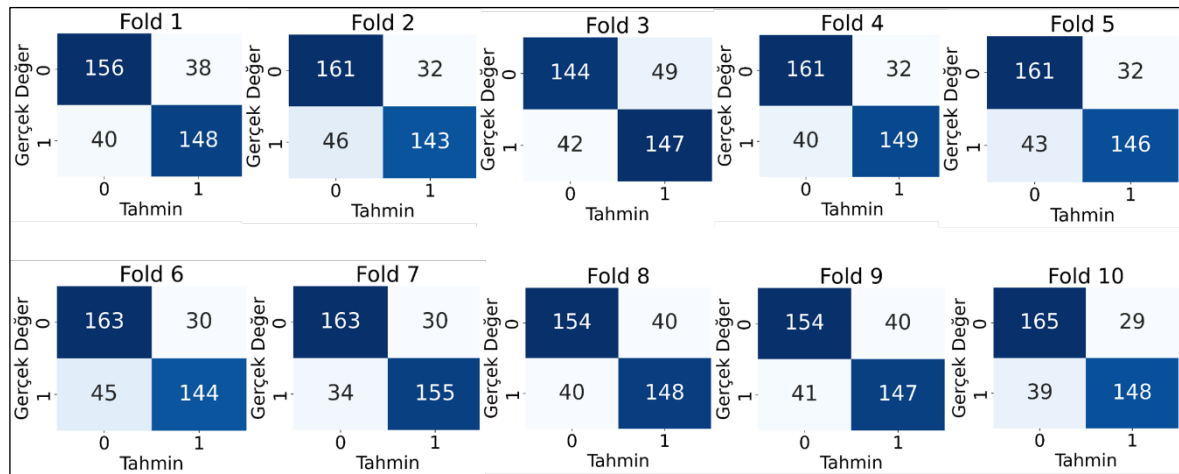


Şekil 5.5. Siyasi görüş/düşünce sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları

Çizelge 5.5. Dini Görüş/İnanç sınıfı model performansı

Dini Görüş	Etiket	Kelime Sayısı	Ort. Kayıp	Kesinlik	Geri Çağırma	F-1 Skoru	Doğruluk	Örnek Sayısı
Katlama 1	Kvkk_u	5 302	0,035	0,796	0,787	0,791	0,796	188
	Kvkk_ud			0,796	0,804	0,800		194
Katlama 2	Kvkk_u	5 268	0,033	0,817	0,757	0,786	0,796	189
	Kvkk_ud			0,778	0,834	0,805		193
Katlama 3	Kvkk_u	5 303	0,028	0,750	0,778	0,764	0,762	189
	Kvkk_ud			0,774	0,746	0,760		193
Katlama 4	Kvkk_u	5 307	0,039	0,823	0,788	0,805	0,812	189
	Kvkk_ud			0,802	0,834	0,817		193
Katlama 5	Kvkk_u	5 317	0,035	0,820	0,772	0,796	0,804	189
	Kvkk_ud			0,789	0,834	0,811		193
Katlama 6	Kvkk_u	5 287	0,066	0,828	0,762	0,793	0,804	189
	Kvkk_ud			0,784	0,845	0,813		193
Katlama 7	Kvkk_u	5 300	0,057	0,780	0,770	0,780	0,832	189
	Kvkk_ud			0,840	0,840	0,840		193
Katlama 8	Kvkk_u	5 294	0,049	0,730	0,730	0,730	0,791	188
	Kvkk_ud			0,810	0,810	0,810		194
Katlama 9	Kvkk_u	5 274	0,052	0,786	0,782	0,784	0,788	188
	Kvkk_ud			0,790	0,794	0,792		194
Katlama 10	Kvkk_u	5 289	0,052	0,836	0,791	0,813	0,822	187
	Kvkk_ud			0,809	0,851	0,829		194
Ortalama		5 294	0,045	0,800	0,770	0,780	0,800	184
				0,800	0,820	0,810		193

Dini Görüş/İnanç sınıfına ilişkin hazırlanan her bir katlama için gerçekleştirilen testler sonucunda elde edilen karmaşıklık matrislerine ilişkin ekran görüntüleri Şekil 5.6'da sunulmuştur.

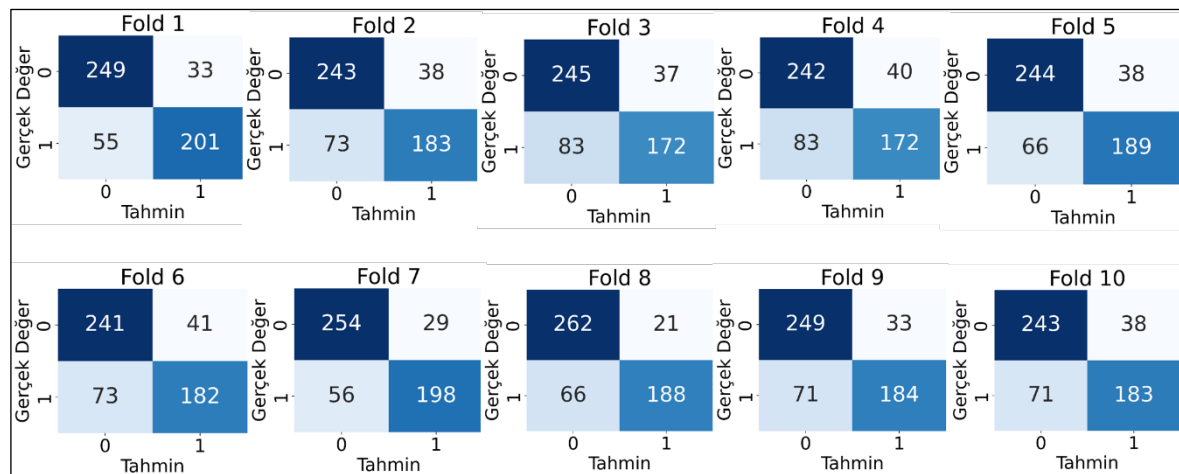


Şekil 5.6. Dini görüş/İnanç sınıfı test katlamalarına ait karışıklık matrisi sonuçları

Çizelge 5.6. Irk Köken Bilgileri sınıfı model performansı

İrk Bilgileri	Etiket	Kelime Sayısı	Ort. Kayıp	Kesinlik	Geri Çağırma	F-1 Skoru	Doğruluk	Örnek Sayısı
Katlama 1	Kvkk_u	6 654	0,035	0,859	0,788	0,822	0,838	256
	Kvkk_ud			0,822	0,883	0,851		282
Katlama 2	Kvkk_u	6 718	0,039	0,828	0,715	0,767	0,793	256
	Kvkk_ud			0,769	0,865	0,814		281
Katlama 3	Kvkk_u	6 681	0,052	0,823	0,740	0,780	0,777	255
	Kvkk_ud			0,747	0,869	0,803		282
Katlama 4	Kvkk_u	6 662	0,053	0,811	0,675	0,737	0,771	255
	Kvkk_ud			0,745	0,858	0,797		282
Katlama 5	Kvkk_u	6 657	0,053	0,833	0,741	0,784	0,806	255
	Kvkk_ud			0,787	0,865	0,824		282
Katlama 6	Kvkk_u	6 670	0,047	0,816	0,714	0,762	0,788	255
	Kvkk_ud			0,768	0,855	0,809		282
Katlama 7	Kvkk_u	6 669	0,033	0,869	0,783	0,824	0,842	254
	Kvkk_ud			0,821	0,894	0,856		283
Katlama 8	Kvkk_u	6 665	0,040	0,900	0,740	0,812	0,838	254
	Kvkk_ud			0,799	0,926	0,858		283
Katlama 9	Kvkk_u	6 654	0,036	0,848	0,722	0,780	0,806	255
	Kvkk_ud			0,722	0,883	0,827		282
Katlama 10	Kvkk_u	6 699	0,039	0,828	0,720	0,771	0,796	254
	Kvkk_ud			0,774	0,865	0,817		281
Ortalama		6 673	0,043	0,840	0,730	0,780	0,810	255
				0,780	0,880	0,830		282

İrk Bilgileri sınıfına ilişkin hazırlanan her bir katlama için gerçekleştirilen testler sonucunda elde edilen karmaşıklık matrislerine ilişkin ekran görüntüleri Şekil 5.7’de sunulmuştur.

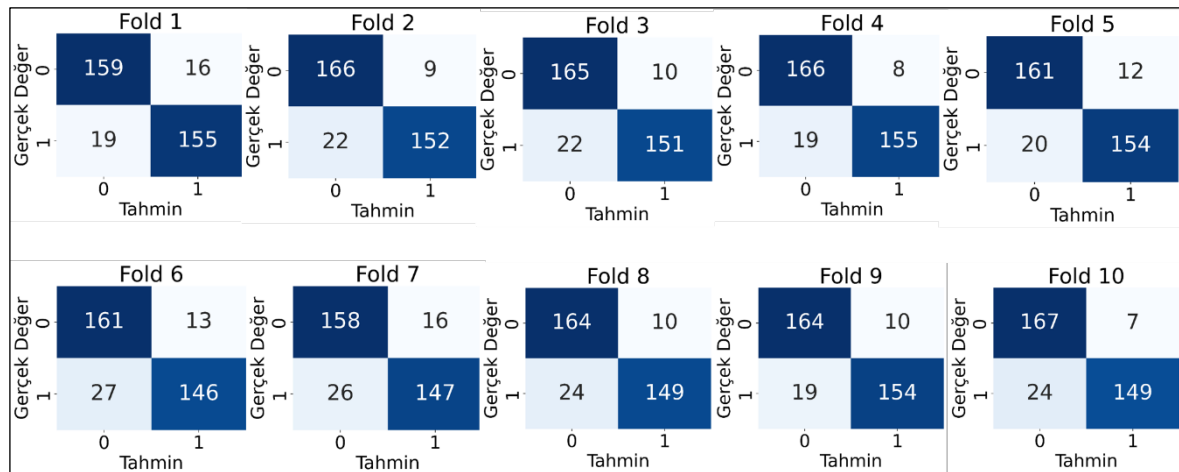


Şekil 5.7. Irk köken bilgisi sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları

Çizelge 5.7. Cinsel Yönelim sınıfı model performansı

Cinsel Yönelim	Etiket	Kelime Sayısı	Ort. Kayıp	Kesinlik	Geri Çağırma	F-1 Skoru	Doğruluk	Örnek Sayısı
Katlama 1	Kvkk_u	4 685	0,047	0,906	0,891	0,899	0,900	174
	Kvkk_ud			0,893	0,909	0,901		175
Katlama 2	Kvkk_u	4 699	0,046	0,944	0,874	0,907	0,911	174
	Kvkk_ud			0,883	0,949	0,915		175
Katlama 3	Kvkk_u	4 622	0,044	0,938	0,873	0,904	0,908	174
	Kvkk_ud			0,882	0,943	0,912		174
Katlama 4	Kvkk_u	4 658	0,042	0,951	0,891	0,920	0,922	174
	Kvkk_ud			0,897	0,954	0,925		174
Katlama 5	Kvkk_u	4 684	0,040	0,928	0,885	0,906	0,908	173
	Kvkk_ud			0,890	0,931	0,910		174
Katlama 6	Kvkk_u	4 636	0,045	0,918	0,844	0,880	0,885	173
	Kvkk_ud			0,856	0,925	0,890		174
Katlama 7	Kvkk_u	4 666	0,045	0,902	0,850	0,875	0,879	173
	Kvkk_ud			0,859	0,908	0,883		174
Katlama 8	Kvkk_u	4 651	0,040	0,937	0,861	0,898	0,902	173
	Kvkk_ud			0,872	0,943	0,906		174
Katlama 9	Kvkk_u	4 653	0,045	0,939	0,890	0,914	0,916	173
	Kvkk_ud			0,896	0,943	0,919		174
Katlama 10	Kvkk_u	4 652	0,045	0,955	0,861	0,906	0,911	173
	Kvkk_ud			0,874	0,960	0,915		174
Ortalama		4 661	0,044	0,930	0,870	0,900	0,900	173
				0,880	0,940	0,910		174

Cinsel Yönelim sınıfına ilişkin hazırlanan her bir katlama için gerçekleştirilen testler sonucunda elde edilen karmaşıklık matrislerine ilişkin ekran görüntüleri Şekil 5.8’de sunulmuştur.

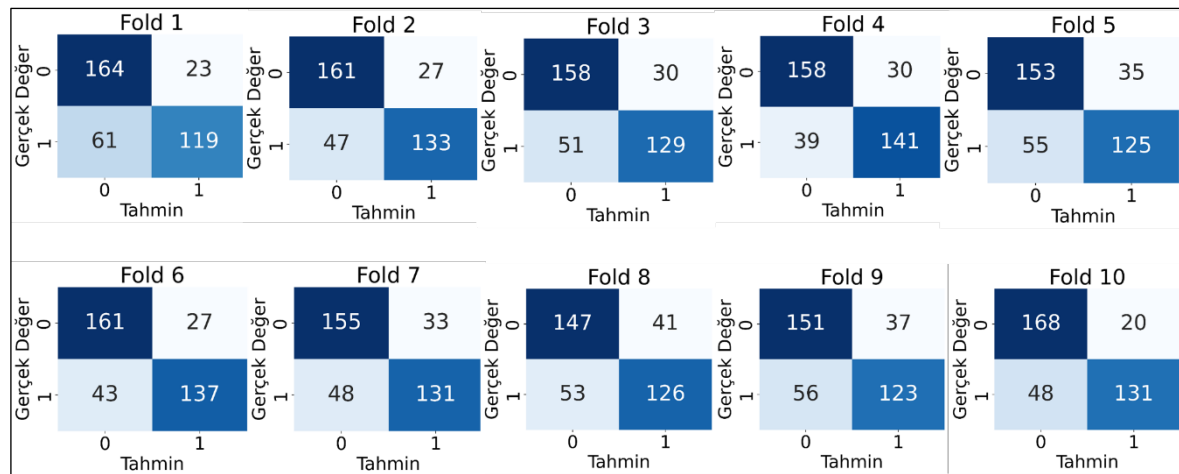


Şekil 5.8. Cinsel yönelim sınıfı test katlamalarına ait karışıklık matrisi sonuçları

Çizelge 5.8. Ceza/Mahkûmiyet Bilgileri sınıfı model performansı

Ceza Bilgileri	Etiket	Kelime Sayısı	Ort. Kayıp	Kesinlik	Geri Çağırma	F-1 Skoru	Doğruluk	Örnek Sayısı
Katlama 1	Kvkk_u	5 794	0,030	0,838	0,661	0,739	0,771	180
	Kvkk_ud			0,729	0,877	0,796		187
Katlama 2	Kvkk_u	5 743	0,042	0,833	0,750	0,789	0,799	180
	Kvkk_ud			0,782	0,856	0,817		188
Katlama 3	Kvkk_u	5 741	0,046	0,811	0,717	0,761	0,780	180
	Kvkk_ud			0,756	0,840	0,796		188
Katlama 4	Kvkk_u	5 756	0,050	0,824	0,782	0,802	0,812	180
	Kvkk_ud			0,802	0,840	0,821		188
Katlama 5	Kvkk_u	5 776	0,031	0,781	0,698	0,737	0,757	180
	Kvkk_ud			0,739	0,814	0,775		188
Katlama 6	Kvkk_u	5 768	0,037	0,835	0,761	0,797	0,810	180
	Kvkk_ud			0,789	0,856	0,821		188
Katlama 7	Kvkk_u	5 725	0,045	0,799	0,732	0,764	0,779	179
	Kvkk_ud			0,764	0,824	0,793		188
Katlama 8	Kvkk_u	5 729	0,036	0,754	0,704	0,728	0,744	179
	Kvkk_ud			0,735	0,782	0,758		188
Katlama 9	Kvkk_u	5 724	0,049	0,769	0,687	0,726	0,747	179
	Kvkk_ud			0,729	0,803	0,765		188
Katlama 10	Kvkk_u	5 723	0,037	0,868	0,732	0,794	0,815	179
	Kvkk_ud			0,778	0,894	0,832		188
Ortalama		5 748	0,040	0,810	0,720	0,760	0,780	180
				0,760	0,840	0,800		188

Ceza Bilgileri sınıfına ilişkin hazırlanan her bir katlama için gerçekleştirilen testler sonucunda elde edilen karmaşıklık matrislerine ilişkin ekran görüntüleri Şekil 5.9’da sunulmuştur.

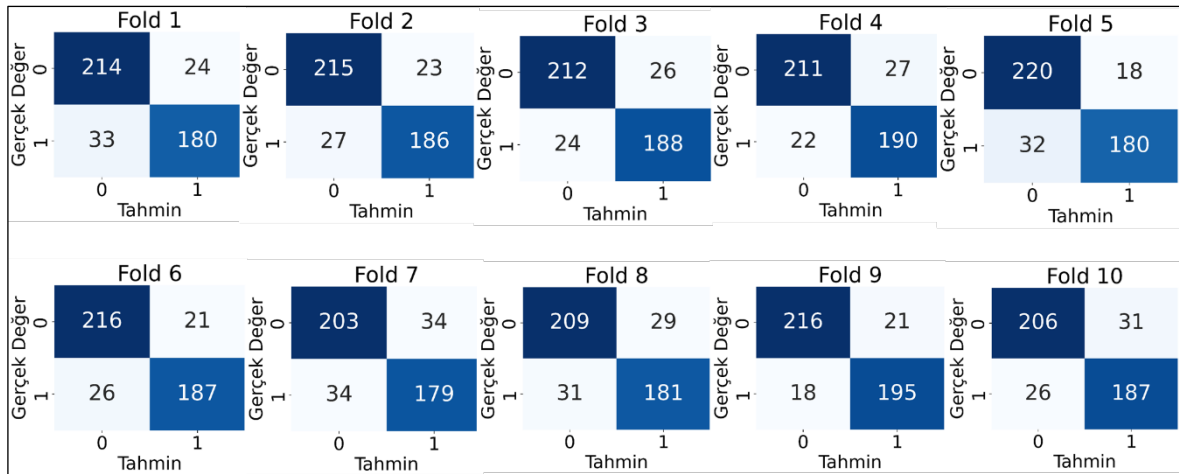


Şekil 5.9. Ceza/Mahkûmiyet bilgileri sınıfı test katlamalarına ait karışıklık matrisi sonuçları

Çizelge 5.9. Sağlık Bilgileri sınıfı model performansı

Sağlık Bilgileri	Etiket	Kelime Sayısı	Ort. Kayıp	Kesinlik	Geri Çağırma	F-1 Skoru	Doğruluk	Örnek Sayısı
Katlama 1	Kvkk_u	5 538	0,026	0,882	0,845	0,863	0,874	213
	Kvkk_ud			0,866	0,899	0,882		238
Katlama 2	Kvkk_u	5 572	0,025	0,890	0,873	0,882	0,889	213
	Kvkk_ud			0,888	0,903	0,896		238
Katlama 3	Kvkk_u	5 570	0,026	0,879	0,887	0,883	0,889	212
	Kvkk_ud			0,898	0,891	0,895		238
Katlama 4	Kvkk_u	5 499	0,043	0,876	0,896	0,886	0,891	212
	Kvkk_ud			0,906	0,887	0,896		238
Katlama 5	Kvkk_u	5 543	0,029	0,909	0,849	0,878	0,889	212
	Kvkk_ud			0,873	0,924	0,898		238
Katlama 6	Kvkk_u	5 500	0,036	0,899	0,878	0,888	0,896	213
	Kvkk_ud			0,893	0,911	0,902		237
Katlama 7	Kvkk_u	5 502	0,033	0,840	0,840	0,840	0,849	213
	Kvkk_ud			0,857	0,857	0,857		237
Katlama 8	Kvkk_u	5 574	0,038	0,862	0,854	0,858	0,862	212
	Kvkk_ud			0,871	0,878	0,874		238
Katlama 9	Kvkk_u	5 508	0,039	0,903	0,915	0,909	0,913	213
	Kvkk_ud			0,923	0,911	0,917		237
Katlama 10	Kvkk_u	5 497	0,038	0,865	0,873	0,869	0,876	213
	Kvkk_ud			0,885	0,878	0,881		237
Ortalama		5 530	0,033	0,880	0,870	0,880	0,880	213
				0,890	0,890	0,890		238

Sağlık Bilgileri sınıfına ilişkin hazırlanan her bir katlama için gerçekleştirilen testler sonucunda elde edilen karmaşıklık matrislerine ilişkin ekran görüntüleri Şekil 5.10’da sunulmuştur.

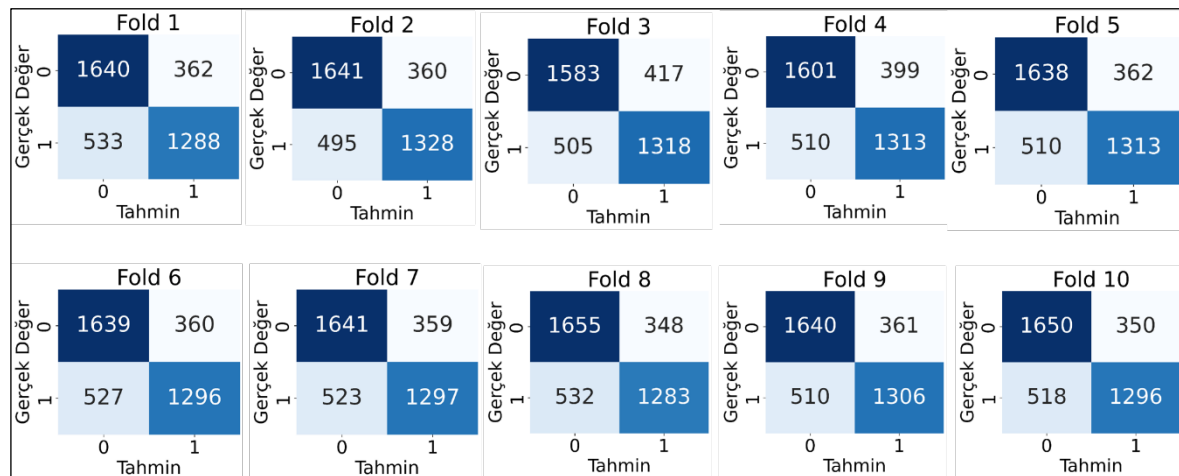


Şekil 5.10. Sağlık bilgileri sınıfı test katlamalarına ait karmaşıklık matrisi sonuçları

Çizelge 5.10. Tüm Bilgiler sınıfı model performansı

Tüm Bilgiler	Etiket	Kelime Sayısı	Ort. Kayıp	Kesinlik	Geri Çağırma	F-1 Skoru	Doğruluk	Örnek Sayısı
Katlama 1	Kvkk_u	15 445	0,043	0,781	0,707	0,742	0,766	1 821
	Kvkk_ud			0,755	0,819	0,786		2 002
Katlama 2	Kvkk_u	15 419	0,041	0,787	0,728	0,756	0,776	1 823
	Kvkk_ud			0,768	0,82	0,793		2 001
Katlama 3	Kvkk_u	15 352	0,042	0,760	0,723	0,741	0,759	1 823
	Kvkk_ud			0,758	0,791	0,774		2 000
Katlama 4	Kvkk_u	15 380	0,041	0,767	0,720	0,743	0,762	1 823
	Kvkk_ud			0,758	0,800	0,779		2 000
Katlama 5	Kvkk_u	15 390	0,041	0,784	0,720	0,751	0,772	1 823
	Kvkk_ud			0,763	0,819	0,790		2 000
Katlama 6	Kvkk_u	15 407	0,043	0,783	0,711	0,745	0,768	1 823
	Kvkk_ud			0,757	0,820	0,787		1 999
Katlama 7	Kvkk_u	15 365	0,042	0,783	0,713	0,746	0,769	1 820
	Kvkk_ud			0,758	0,821	0,788		2 000
Katlama 8	Kvkk_u	15 427	0,043	0,787	0,707	0,745	0,770	1 815
	Kvkk_ud			0,757	0,826	0,790		2 003
Katlama 9	Kvkk_u	15 371	0,045	0,783	0,719	0,750	0,772	1 816
	Kvkk_ud			0,763	0,820	0,790		2 001
Katlama 10	Kvkk_u	15 373	0,045	0,787	0,714	0,749	0,772	1 814
	Kvkk_ud			0,761	0,825	0,792		2 000
Ortalama		15 393	0,043	0,780	0,720	0,750	0,770	1 820
				0,760	0,820	0,790		2 001

Tüm sınıfların birleştirilmesi ile elde edilen Tüm Bilgiler sınıfına ilişkin hazırlanan her bir katlama için gerçekleştirilen testler sonucunda elde edilen karmaşıklık matrislerine ilişkin ekran görüntüleri Şekil 5.11’de sunulmuştur.



Şekil 5.11. Tüm kişisel bilgiler sınıfı test katlamalarına ait karışıklık matrisi sonuçları

Tez çalışması kapsamında geliştirilen modellerin boyutları 1,56-2,35 GB arası büyüklüklere sahip oldukları göz önüne alındığında modellerden elde edilecek sonuçların gösterilmesinin planlandığı uygulamada olası işlem süresi ve performans problemlerinin önüne geçilebilmesi maksadıyla modellerin sıkıştırılmasına ihtiyaç duyulmuştur. fastText kütüphanesinde yer alan model sıkıştırma işlemi ile düşük bir miktar performans kaybıyla ciddi oranda boyutların küçültülebileceği belirtilmiştir [142]. Söz konusu model sıkıştırma işlemi her bir sınıfın en iyi sonuç elde edilen katlama seçilerek uygulanmış ve sıkıştırılan modellerden elde edilen performanslar ve model boyutları karşılaştırmalı olarak Çizelge 5.11’de sunulmuştur. Elde edilen sıkıştırılmış modellerin en fazla %2,6’lık kayıp ile 196-295 MB arası boyutlara düşürüldüğü görülmektedir.

Çizelge 5.11. Modeller sıkıştırıldıktan sonra elde edilen sonuçlar

Model Adı	Kesinlik	Geri Çağırma	F-1 Skoru	Doğruluk	Size
Tüm Bilgiler (Katlama 2)	0,787	0,728	0,756	0,776	2,36 GB
	0,768	0,820	0,793		
Quantized	0,790	0,722	0,755	0,776	295 MB
	0,765	0,825	0,794		
Temel Bilgiler (Katlama 2)	0,761	0,729	0,745	0,767	1,56 GB
	0,772	0,800	0,785		
Quantized	0,759	0,700	0,728	0,756	196 MB
	0,754	0,806	0,779		
Siyasi Görüş (Katlama 2)	0,838	0,838	0,838	0,848	1,56 GB
	0,857	0,857	0,857		
Quantized	0,803	0,834	0,818	0,827	196 MB
	0,849	0,820	0,834		
Dini Görüş (Katlama10)	0,836	0,791	0,813	0,822	1,56 GB
	0,809	0,851	0,829		
Quantized	0,857	0,706	0,774	0,798	196 MB
	0,758	0,887	0,817		
Sağlık Bilgileri (Katlama9)	0,903	0,915	0,909	0,913	2,35 GB
	0,923	0,911	0,917		
Quantized	0,851	0,939	0,893	0,893	294 MB
	0,940	0,852	0,894		
İrk Bilgileri (Katlama7)	0,869	0,783	0,824	0,842	1,56 GB
	0,821	0,894	0,856		
Quantized	0,868	0,722	0,788	0,816	196 MB
	0,782	0,901	0,837		
Cinsel Yönelim (Katlama4)	0,951	0,891	0,920	0,922	2,34 GB
	0,897	0,954	0,925		
Quantized	0,945	0,891	0,917	0,920	294 MB
	0,897	0,948	0,922		
Ceza Bilgileri	0,868	0,732	0,794	0,815	1,56 GB
	0,778	0,894	0,832		
Quantized	0,787	0,804	0,796	0,798	196 MB
	0,810	0,793	0,801		

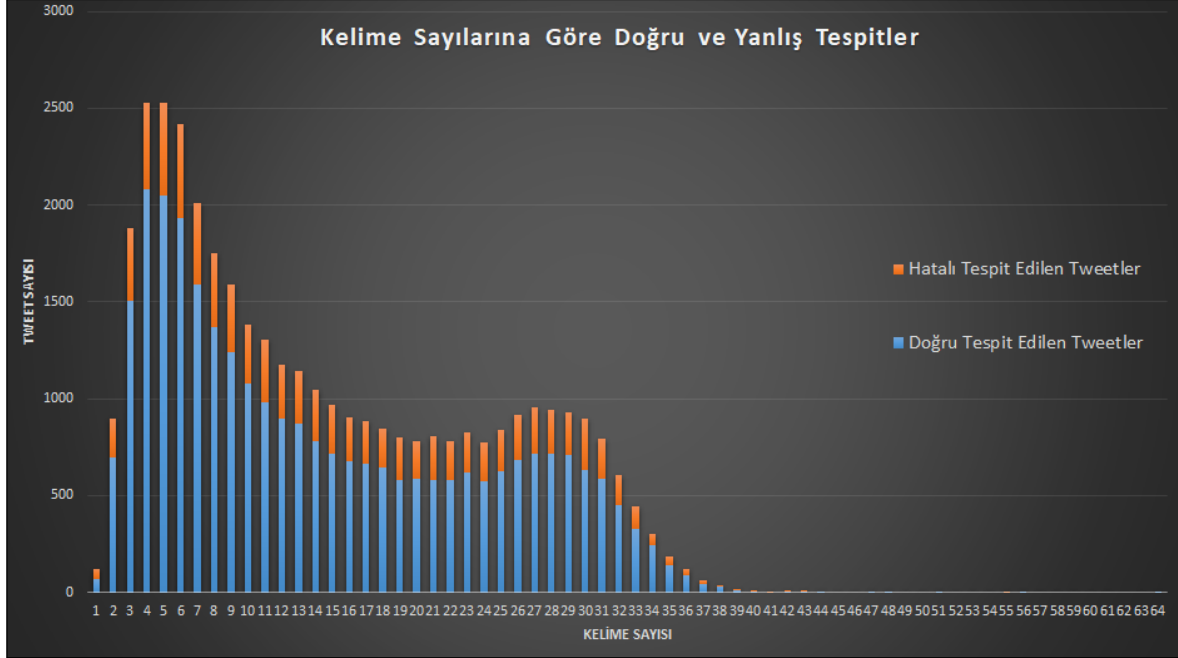
Modellerden elde edilen sonuçlar doğrultusunda ön işlemlerden geçirilmiş tivitlerin kelime sayılarının testlerden elde edilen sonuçlara bir etkisi olup olmadığı araştırılmıştır. Söz konusu işlemi gerçekleştirmek için tüm kişisel verilerden oluşturulan modele ait test sonuçları kelime sayılarına göre doğru ve hatalı tespit sayılarına göre ayrıştırılmıştır. Çizelge 5.12’de sunulan detaylar doğrultusunda yapılan incelemede kelime sayıları için ortalama hata yüzdesinin 24,4 olduğu, en yüksek hata yüzdesi ile (%41) tek kelime içeren tivitlerde karşılaşıldığı, en düşük hata oranına sahip tespitlerin 4-5 kelimelik tivitlerde (%18-19) sağlandığı görülmektedir. Genel olarak oluşturulan model doğrultusunda tek kelimeli paylaşımlar dışında kelime sayısının tespitlerin doğruluklarında çok büyük etkiye sahip olmadığı değerlendirilmektedir.

Çizelge 5.12. Tüm Bilgiler modeli ile elde edilen sonuçların kelime sayısı analizi

Kelime Sayısı	Doğru Tespit Tekrar Sayısı	Hatalı Tespit Tekrar Sayısı	Toplam Sayı	Hatalı Tespit Yüzdesi
1	69	48	117	41
2	699	199	898	22
3	1 505	375	1 880	20
4	2 082	444	2 526	18
5	2 048	479	2 527	19
6	1 931	488	2 419	20
7	1 592	421	2 013	21
8	1 370	383	1 753	22
9	1 243	347	1 590	22
10	1 080	301	1 381	22
11	984	321	1 305	25
12	897	279	1 176	24
13	874	269	1 143	24
14	777	269	1 046	26
15	713	254	967	26
16	674	229	903	25
17	666	215	881	24
18	643	203	846	24
19	577	223	800	28
20	585	198	783	25
* 40 kelimedenden sonraki sınıflandırma için doğru ve hatalı tespit sayıları çok az olduğu için tabloya eklenmemiştir. Ancak, ortalama hatalı tespit yüzdesi hesabında dikkate alınmıştır.				

Kelime Sayısı	Doğru Tespit Tekrar Sayısı	Hatalı Tespit Tekrar Sayısı	Toplam Sayı	Hatalı Tespit Yüzdesi
21	579	228	807	28
22	581	202	783	26
23	620	206	826	25
24	574	200	774	26
25	623	216	839	26
26	680	234	914	26
27	715	241	956	25
28	713	230	943	24
29	707	225	932	24
30	634	262	896	29
31	587	209	796	26
32	448	158	606	26
33	329	116	445	26
34	243	61	304	20
35	141	46	187	25
36	90	27	117	23
37	44	15	59	25
38	26	7	33	21
39	11	6	17	35
40	1	3	4	75
Ortalama Hatalı Tespit Yüzdesi				24,44

Kelime sayılarına ilişkin yapılan analiz doğrultusunda hatalı ve doğru tespit sayıları grafik olarak Şekil 5.12’de sunulmuştur.



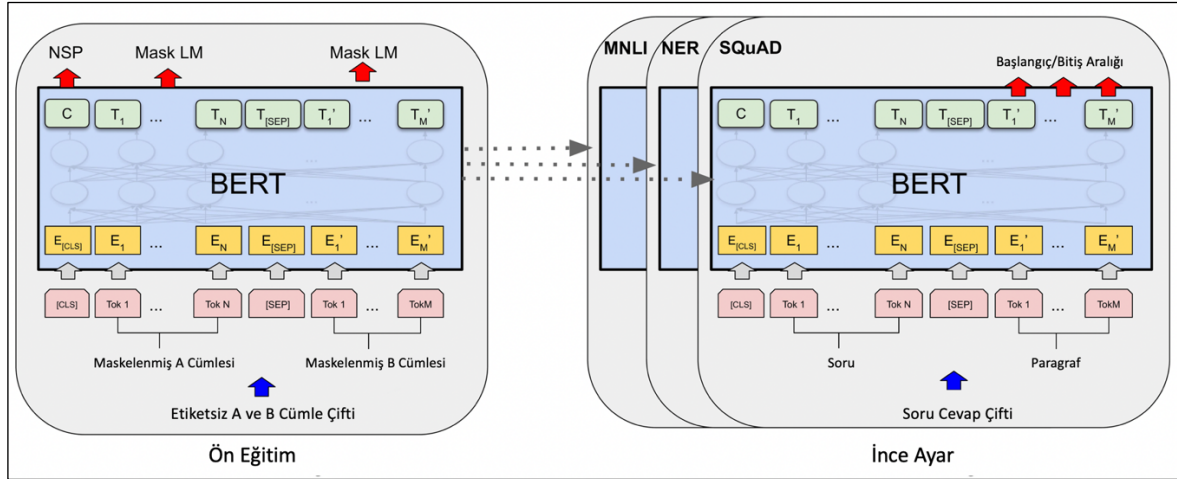
Şekil 5.12. Kelime sayılarına göre doğru ve hatalı tivit tespit grafiği

5.2. BERT (Bidirectional Encoder Representations from Transformer)

2018 yılında tanıtılan BERT, tasarım olarak basit ancak güçlü bir dil temsil modelidir [143]. Güncel dil temsil modellerinin aksine etiketlenmemiş verileri kullanarak soldan sağa ve sağdan sola çift yönlü olacak şekilde ön eğitimleri tüm katmanlarda aynı anda gerçekleştirecek şekilde tasarlanmıştır [143]. Oluşturulan ön eğitilmiş modele sadece bir çıktı katmanı ilave edilerek soru cevaplama, dil tanıma gibi birçok farklı görev için state of the art modellerin elde edilmesine imkân sağlamaktadır [143]. Gerçekleştirilen çalışmalarda BERT modeli ile 11 doğal dil işleme görevinde state of the art sonuçlar elde edilmiştir.

BERT modelinde ön eğitim ve ince ayar olarak adlandırılan iki adım bulunmaktadır. Ön eğitim sürecinde model etiketsiz veriler ile farklı ön eğitilmiş görevler için eğitilir [143]. Ön eğitim gerçekleştirilen modelden özellik çıkarımları gerçekleştirilir ve bu özellikler sabit tutularak çözülmek istenen görevde kullanılacak sınıflandırıcıya aktarılır [144]. İnce ayar yapılırken ise BERT modeli ön eğitilmiş parametreler ile başlatılır gerçekleştirilecek çalışmaya ilişkin hazırlanan etiketli veri kullanılarak parametreler güncellenir. Ön eğitim

işlemine göre ince ayar işlemi daha maliyetsizdir [143]. Çıkış katmanları haricinde ön eğitim ve ince ayar için aynı mimari kullanılmaktadır. BERT modelinin ön eğitim ve ince ayar mimarisi Şekil 5.13'te sunulmuştur.



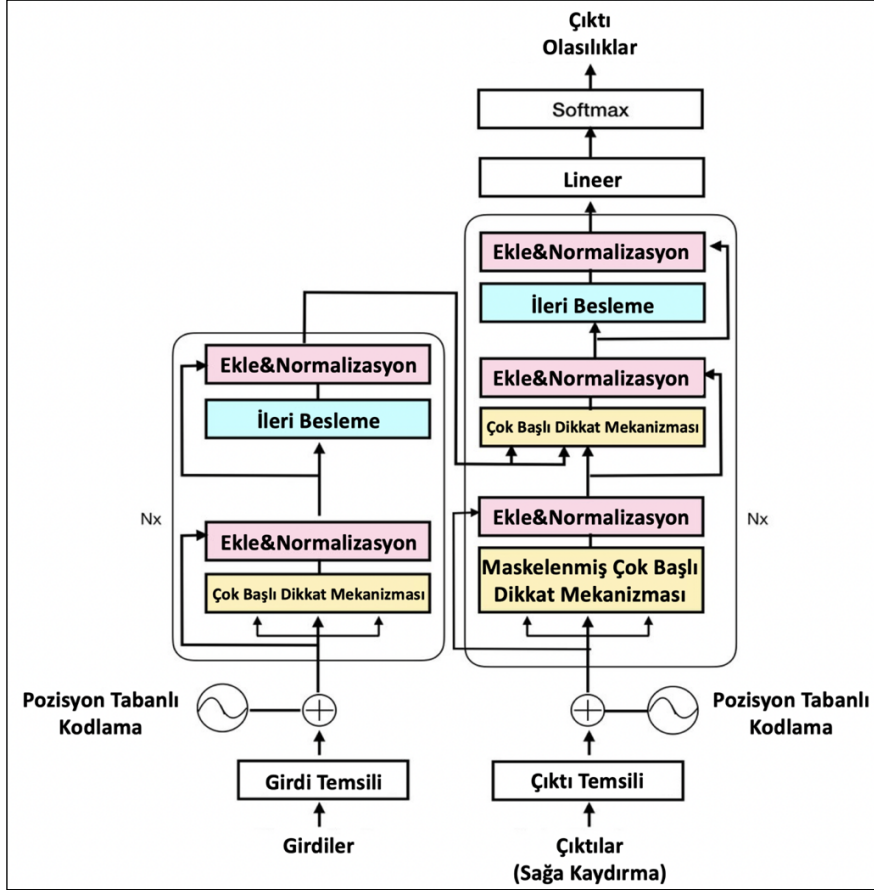
Şekil 5.13. BERT için genel ön eğitim ve ince ayar işlemleri (Türkçeleştirilmiştir) [143]

BERT modeli, Şekil 5.13'te sunulan mimaride de görüleceği gibi Maskeli Dil Modelleme (MLM-Masked Language Modelling) ve Sonraki Cümle Tahmini (NSP-Next Sentence Prediction) yöntemlerinin danışmansız olarak uygulanması ile eğitilmektedir. Bu yöntemler şu şekilde açıklanabilir [143];

- **MLM:** Derin çift yönlü kelime temsilini eğitebilmek için belirli bir oranda giriş tokeni [MASK] belirteci ile rastgele maskelenir ve bu maskelenmiş tokenlar cümleden elde edilen bağlam doğrultusunda tahmin edilmeye çalışılır. Bu yöntem Maskelenmiş LM (MLM) olarak adlandırılır.
- **NSP:** Cümle ilişkilerini anlayabilen bir model eğitebilmek için ön eğitim sürecinde, model cümle çiftlerini girdi olarak alır. A ve B cümleleri her bir ön eğitim örneğinde seçilirken, örneklerin %50'sinde B cümlesi A cümlesinden sonra gelen cümle, kalan %50'sinde ise veri seti içerisinde rastgele bir cümle olarak belirlenir. Model eğitiminde ikinci cümle gerçekten sonraki cümle olup olmadığı tahmin edilir.

BERT'nin model mimarisi, çok katmanlı çift yönlü bir Transformer kodlayıcı tabanlı olup orijinal uygulamaya dayandırılmıştır [143]. Transformer ile ortaya konulan basit ağ mimarisi

yalnızca dikkat mekanizmalarına dayanmakta olup tekrarlama ve kıvrımlardan tamamen vazgeçilmiştir [145]. Bir dikkat işlevi, bir sorguyu ve bir dizi anahtar-değer çiftini, sorgunun, anahtarların, değerlerin ve çıktının tümünün vektör olduğu bir çıktıya eşlemek olarak tanımlanabilir. Çıktı, değerlerin ağırlıklı bir toplamı olarak hesaplanır; burada her bir değere atanan ağırlık, sorgunun karşılık gelen anahtarla bir uyumluluk fonksiyonu tarafından hesaplanır [145]. Transformer mimarisi Şekil 5.14'te sunulmuştur.



Şekil 5.14. Transformer model mimarisi (Türkçeleştirilmiştir) [145]

BERT modeli Şekil 5.14'te sunulan mimari doğrultusunda girdi metninin sözcükleri arasındaki bağlamsal ilişkileri öğrenen bir dikkat bölümünden oluşur. Girdi metnini okumak ve kelime gösterimlerini oluşturmak için bir kodlayıcı ve sonucu tahmin etmek için bir kod çözücü kullanır [146]. Bu sayede vektörler kelimelerin anlamsal bağlamına uygun üretildiği için dil daha iyi anlaşılmakta ve farklı amaçlarla kullanılmış sesteş kelimeler de ayırt edilebilmektedir [147].

Bu tez çalışması kapsamında Bölüm 4.2.8'de detayları açıklanan tüm verinin birleştirilmesi sonucunda elde edilen veri seti;

- Türkçe karakterler hariç tüm karakterlerin silinmesi,
- Türkçe karakterler hariç tüm karakterlerin silinmesi + durak kelimelerin silinmesi,
- Türkçe karakterler hariç tüm karakterlerin silinmesi + normalizasyon,
- Türkçe karakterler hariç tüm karakterlerin silinmesi + normalizasyon + durak kelimelerin silinmesi,

işlemlerinden geçirilerek 4 farklı veri setine dönüştürülmüştür. Bu sayede uygulanan veri ön işleme adımlarının oluşturulacak BERT dil modellerine etkilerinin görülmesi amaçlanmıştır.

Hazırlanan 4 farklı veri seti;

- Turkish BERT-Base [148],
- BERTurk (128K) [149],
- ConvBERTurk [150],

ön eğitilmiş modellerine finetune işlemi uygulanması amacıyla kullanılmış, her bir set için farklı dil modelleri oluşturulmuştur. Dil modelleri oluşturulurken kullanılan parametreler Çizelge 5.13'te sunulmuştur.

Çizelge 5.13. Model eğitimlerinde kullanılan parametreler

	Turkish BERT-Base	BERTurk (128K)	ConvBERTurk
Batch size	256	256	256
Learning rate	1e-5	1e-5	1e-5
Optimization Algorithm	AdamW	AdamW	AdamW
Epoch	25	25	25
Weight decay	0,01	0,01	0,01
Vocabulary size	32000	128000	32000

Gerçekleştirilen finetune işleminin sonucunda oluşturulan dil modellerinin performansları Çizelge 5.2'de belirtilen metrikler doğrultusunda değerlendirilmiş olup Çizelge 5.14'te elde edilen sonuçlar karşılaştırmalı olarak sunulmuştur.

Çizelge 5.14. Tüm Bilgiler sınıfı model performansı (BERT)

			Kesinlik	Geri Çağırma	F1-Skoru	Doğruluk	Örnek Sayısı
ConvBERTurk	Karakter temizleme	kvkk_u	0,93	0,93	0,93	0,93	1 871
		kvkk_ud	0,93	0,93	0,93		1 875
	Karakter temizleme + durak kelime silme	kvkk_u	0,92	0,93	0,93	0,93	1 871
		kvkk_ud	0,93	0,92	0,93		1 875
	Karakter temizleme + normalizasyon	kvkk_u	0,93	0,93	0,93	0,93	1 867
		kvkk_ud	0,93	0,93	0,93		1 873
	Karakter temizleme + normalizasyon + durak kelime silme	kvkk_u	0,91	0,92	0,92	0,92	1 859
		kvkk_ud	0,92	0,91	0,92		1 871
BERTurk (128K)	Karakter temizleme	kvkk_u	0,93	0,92	0,93	0,93	1 871
		kvkk_ud	0,92	0,93	0,93		1 875
	Karakter temizleme + durak kelime silme	kvkk_u	0,91	0,93	0,92	0,91	1 871
		kvkk_ud	0,92	0,90	0,91		1 875
	Karakter temizleme + normalizasyon	kvkk_u	0,93	0,92	0,93	0,93	1 867
		kvkk_ud	0,92	0,93	0,93		1 873
	Karakter temizleme + normalizasyon + durak kelime silme	kvkk_u	0,91	0,91	0,91	0,91	1 859
		kvkk_ud	0,91	0,91	0,91		1 871
Turkish BERT-Base	Karakter temizleme	kvkk_u	0,92	0,92	0,92	0,92	1 871
		kvkk_ud	0,92	0,92	0,92		1 875
	Karakter temizleme + durak kelime silme	kvkk_u	0,90	0,91	0,90	0,90	1 871
		kvkk_ud	0,91	0,89	0,90		1 875
	Karakter temizleme + normalizasyon	kvkk_u	0,93	0,92	0,92	0,92	1 867
		kvkk_ud	0,92	0,93	0,92		1 873
	Karakter temizleme + normalizasyon + durak kelime silme	kvkk_u	0,91	0,90	0,91	0,91	1 859
		kvkk_ud	0,90	0,91	0,91		1 871

Test sonuçları doğrultusunda ConvBERTurk ön eğitilmiş modelinin farklı ön işlemlerden geçirilerek elde edilen eğitim setleri ile finetune edilmesi ile oluşturulan dil modellerinin karmaşıklık matrisleri Şekil 5.15'te görülmektedir.

Gerçek Değer	0	1	
0	1748	123	
1	130	1745	
	0	1	Tahmin

Gerçek Değer	0	1	
0	1741	130	
1	149	1726	
	0	1	Tahmin

Gerçek Değer	0	1	
0	1740	127	
1	127	1746	
	0	1	Tahmin

Gerçek Değer	0	1	
0	1728	131	
1	164	1707	
	0	1	Tahmin

Şekil 5.15. Karakter temizleme, karakter temizleme + durak kelime silme, karakter temizleme + normalizasyon, karakter temizleme + normalizasyon + durak kelime silme işlemlerinden geçirilerek hazırlanan setlerle elde edilen karmaşıklık matrisleri (Sırasıyla)

Test sonuçları doğrultusunda BERTurk (128K) ön eğitilmiş modelinin farklı ön işlemlerden geçirilerek elde edilen eğitim setleri ile finetune edilmesi ile oluşturulan dil modellerinin karmaşıklık matrisleri Şekil 5.16’da görülmektedir.

Gerçek Değer	0	1	
0	1721	150	
1	124	1751	
	0	1	Tahmin

Gerçek Değer	0	1	
0	1732	139	
1	180	1695	
	0	1	Tahmin

Gerçek Değer	0	1	
0	1724	143	
1	135	1738	
	0	1	Tahmin

Gerçek Değer	0	1	
0	1707	152	
1	161	1710	
	0	1	Tahmin

Şekil 5.16. Karakter temizleme, karakter temizleme + durak kelime silme, karakter temizleme + normalizasyon, karakter temizleme + normalizasyon + durak kelime silme işlemlerinden geçirilerek hazırlanan setlerle elde edilen karmaşıklık matrisleri (Sırasıyla)

Test sonuçları doğrultusunda Turkish BERT-Base ön eğitilmiş modelinin farklı ön işlemlerden geçirilerek elde edilen eğitim setleri ile finetune edilmesi ile oluşturulan dil modellerinin karmaşıklık matrisleri Şekil 5.17’de görülmektedir.

Gerçek Değer	0	1	
0	1731	140	
1	143	1732	
	0	1	Tahmin

Gerçek Değer	0	1	
0	1720	151	
1	191	1684	
	0	1	Tahmin

Gerçek Değer	0	1	
0	1710	157	
1	133	1740	
	0	1	Tahmin

Gerçek Değer	0	1	
0	1690	169	
1	164	1707	
	0	1	Tahmin

Şekil 5.17. Karakter temizleme, karakter temizleme + durak kelime silme, karakter temizleme + normalizasyon, karakter temizleme + normalizasyon + durak kelime silme işlemlerinden geçirilerek hazırlanan setlerle elde edilen karmaşıklık matrisleri (Sırasıyla)

Gerçekleştirilen model performans değerlendirmeleri sonucunda en yüksek başarımların %93 doğruluk değeri ile ConvBERTurk ön eğitilmiş modeline ince ayar yapılması ile elde edildiği görülmektedir. Yapılan test işlemlerinde veri seti içerisinde yer alan durak kelimelerin silinmesinin sonuçları olumsuz etkilediği, en düşük başarımın %90 ile Turkish BERT-Base ön eğitilmiş modelinin karakter temizleme ve durak kelime silme işlemleri gerçekleştirilmiş veri seti ile finetune edilmesi ile elde edildiği görülmektedir. Bunun yanı sıra, normalizasyon işleminin sonuçlara olumlu anlamda bir katkı sağlamadığı görülmektedir. Dolayısıyla BERT modelinin metinlerin anlamsız karakterlerin ve rakamların silinmesi dışında ön işlem adımlarından geçirilmeden de kullanılabilmesine imkan sağladığı, normalizasyon, kök alma gibi doğal dil işleme süreçlerine ihtiyaç duyulmaması nedeniyle tasarım ve uygulama yönünden de kolaylıklar sağladığı değerlendirilmektedir.

Söz konusu model eğitimleri ile ilgili gerçekleştirilen çalışmalarda ön eğitilmiş modellerin belirtilen 4 farklı veri seti ile finetune edilmesi yaklaşık 3 günlük bir çalışma sonucunda gerçekleştirilebilmiştir. BERT modelinin eğitim sürecinin, kaynak tüketimi ve eğitim süreleri açısından her ne kadar ince ayar işleminin maliyetsiz olduğu belirtilse de dezavantajlı olduğu görülmektedir.

Tüm kişisel verilere ilişkin hazırlanan veri seti kullanılarak fastText ile gerçekleştirilen eğitim ve test işlemlerinde elde edilen %77'lik başarımlar BERT modeli ile %16'lık bir artış ile %93'e çıkarılmıştır.

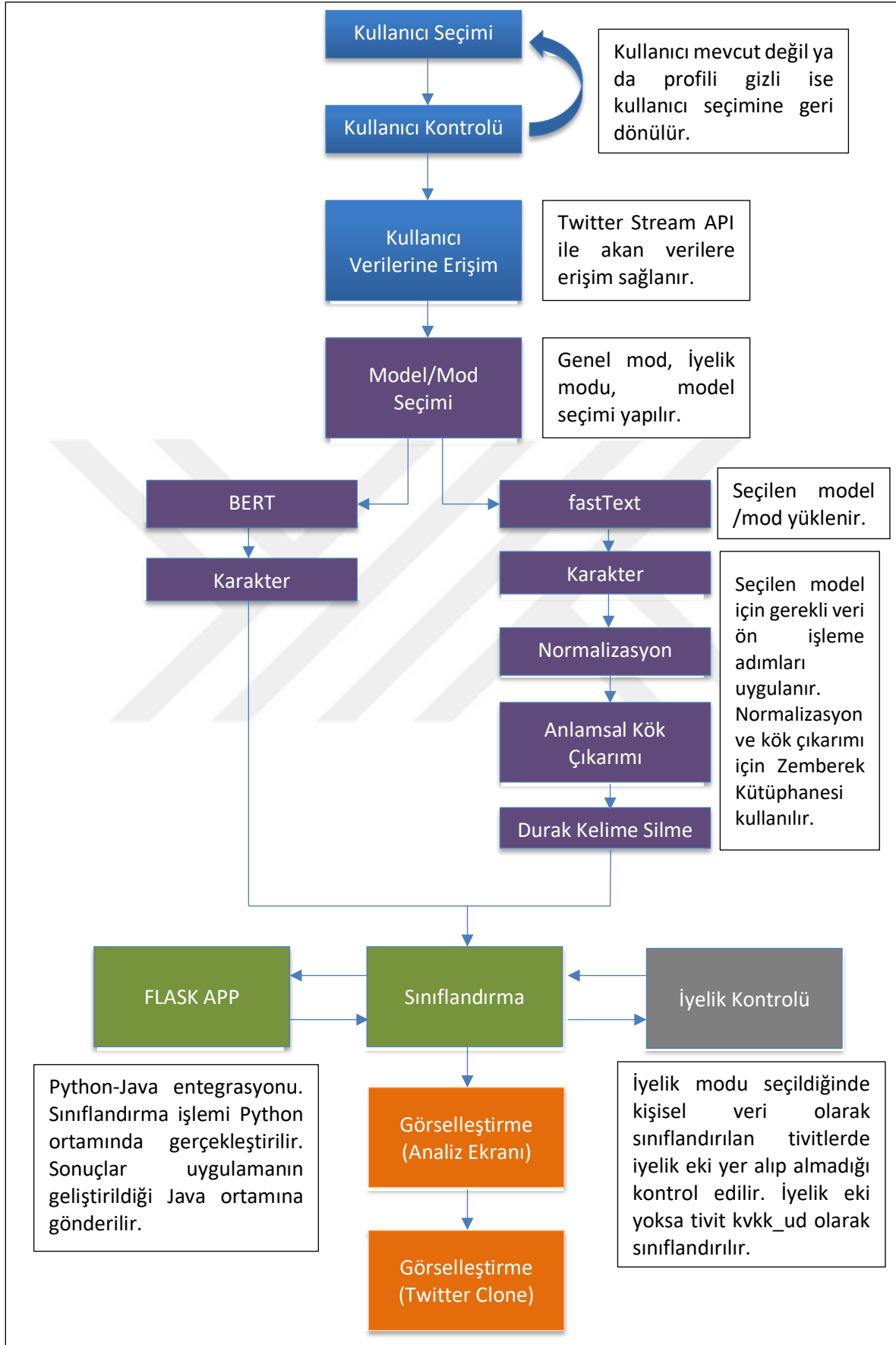
6. GELİŞTİRİLEN GERÇEK ZAMANLI T-PII HUNTER SİSTEMİ

Literatürde yer alan çalışmalarda [18], [22] farkındalığın artırılması amacıyla geliştirilen uygulamalarda etkileşimli sistemlerin kullanıcı davranışlarında değişiklik yarattığı görülmektedir. Kullanıcılara yapacakları paylaşımın kimler tarafından görüleceğinin gösterilmesi ya da kullanıcıların yazdıkları metinde gizlilik ifşası içeren bir paylaşıma ilişkin onay istenmesi gibi durumlarda kullanıcıların daha kısıtlayıcı davrandıkları tespit edilmiştir. Bu kapsamda tez çalışması kapsamında hazırlanan ve testleri yapılan modellerin bir prototip uygulama ile kullanıcı analizi ve görselleştirme yapacak şekilde geliştirilmesine karar verilmiştir.

T-PII Hunter (Türkçe Kişisel Veri Avcısı) adı verilen sistem ile Twitter platformunda kullanıcılar tarafından atılan tivitlerin toplanarak Zemberek kütüphanesi ile doğal dil işleme süreçlerinden geçirilmesi ve çalışma kapsamında fastText ve BERT transformer yaklaşımları ile hazırlanan dil modelleri kullanılarak kişisel veri ifşası içerip içermediğinin tespit edilmesi amaçlanmıştır. Söz konusu tespitler kişinin sosyal ağlarda mahremiyet ve gizlilik farkındalığının ölçülmesine imkân sağlayacaktır.

Sistemin farklı bilgi ve teknolojik okur yazarlık seviyesine sahip sosyal ağ kullanıcıları tarafından rahatlıkla kullanılabilecek şekilde tasarlanmasına dikkat edilmiştir. Bu nedenle basit, sade arayüzlere sahip olacak ve zincirleme çalışacak şekilde tasarlanmıştır. Geliştirme sürecinde arayüzün oluşturulması, veri toplama, veri ön işleme ve görselleştirme süreçlerinde Java programlama dili kullanılmıştır.

fastText ve BERT transformer dil modelleri Python programlama dilinde geliştirildiğinden yaşanabilecek muhtemel uyumsuzluk süreçlerinden dolayı Python üzerinden model yükleme ve tahmin işlemleri gerçekleştirilmeye devam edilmiştir. Python programlama dili üzerinde fastText ve BERT transformer kütüphaneleri kullanılarak oluşturulan dil modellerine FLASK kütüphanesi ile entegrasyon sağlanmış ve Java programlama dili içerisinde tahmin sonuçlarına erişim sağlanmasına yönelik geliştirmeler tamamlanmıştır. Kullanıcı farkındalığının artırılması maksadıyla, Twitter Clone [142] adı verilen açık kaynak projeden faydalanılarak hazırlanan ekranda Geliştirilen T-PII Hunter ile elde edilen sonuçlar renklendirilerek gösterilmiştir. Sisteme ait diyagram Şekil 6.1’de sunulmuştur.

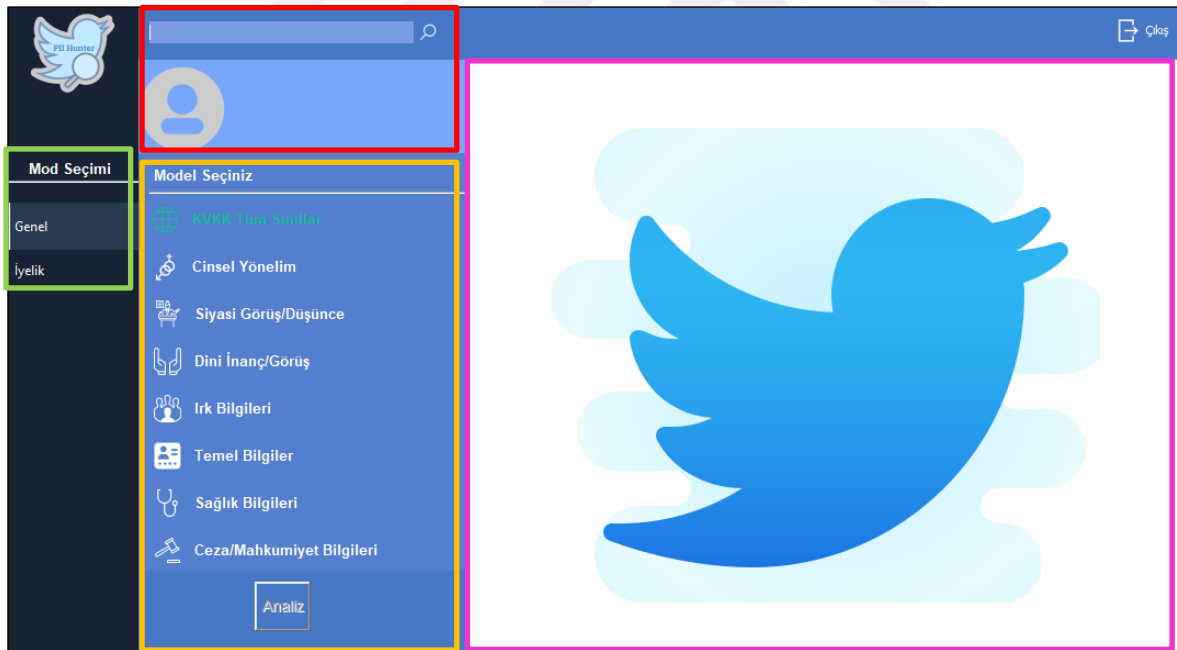


Şekil 6.1. T-PII Hunter uygulaması akış diyagramı

Geliştirilen uygulama ana ekranında 4 bölüm bulunmaktadır. Bunlar;

- 1- Kullanıcı adı sorgulama ve kullanıcının adı, takip ve takipçi sayılarının gösterildiği özet bilgileri alanı,
- 2- Sınıflandırma sürecinde tivitlerin doğrudan sınıflandırıldığı “Genel” ya da kişisel veri ifşa riski içeren tivitlerin iyelik eki kontrolünden geçirilerek nihai sınıfının belirlendiği “İyelik” modunda gerçekleştirilmesine yönelik seçim ekranı,
- 3- Tez çalışması kapsamında oluşturulan 8 adet sınıflandırmaya yönelik hazırlanan dil modellerinden seçim ekranı ve
- 4- Süreç bilgilendirme (Model yüklendi, analiz tamamlandı, riskli tivit tespit edildi gibi) ve grafik ekranların (Analiz sonuçlarına ilişkin) gösterileceği alandan oluşmaktadır.

T-Pii Hunter uygulamasının ana ekran görüntüsü ve bölümleri Şekil 6.2’de sunulmuştur.



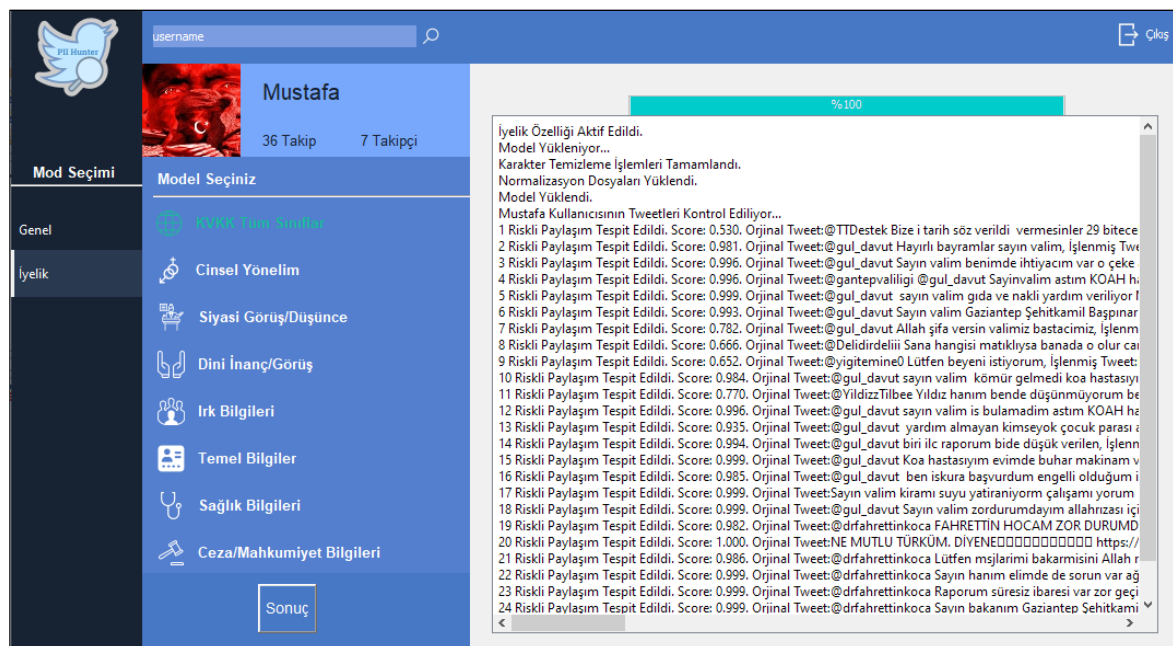
Şekil 6.2. T-Pii Hunter ana ekran görüntüsü

Çalışma kapsamında sosyal ağlarda gizlilik ayarı bulunmayan kullanıcıların ifşa riski içeren paylaşımlarının tespiti amaçlanmaktadır. Bu nedenle kullanıcı adı ile gerçekleştirilen aramalarda kullanıcı adı ile ilişkili hesap bulunmaması durumunda kullanıcı özet ekranında “Kullanıcı Bulunamadı!” şeklinde yazı ile ya da söz konusu hesabın gizli olması durumunda

süreç bilgilendirme ve grafik ekranların gösterildiği bölümde kilit işareti görseli ve “Kullanıcı Hesabı Kilitlidir!” şeklinde ikaz verilmektedir.

Kişisel veri ifşa riski bulunan tivitlerin tespit edilmesi amacıyla kullanıcı adı yazılarak arama butonuna basıldığında öncelikle kullanıcı özet bilgileri güncellenmektedir. Söz konusu bilgilerin ilgili hesaba ait olduğu kontrol edildikten sonra kullanıcı analizinin başlatılması maksadıyla “Analiz” butonuna tıklanması gerekmektedir. Söz konusu butona tıklandıktan sonra Java programlama dili ile geliştirilen uygulama ile Twitter platformuna bağlanılmakta ve ilgili kullanıcının paylaşımlarına erişim sağlanmaktadır. Uygulama daha önceden elde edilmiş veriler ile değil Twitter üzerinde akan veri ile çalışmaktadır. Dolayısı ile mevcut uygulama ile daha önceden elde edilerek depolanan verilerle analiz yapılamamaktadır. Analiz sürecinde uygulamanın ekran görüntüsü Şekil 6.3’te sunulmuştur.

Daha önceki bölümlerde açıklandığı şekilde kullanıcının retivitleri kapsam dışı bırakılmış tivitler ve kullanıcının başka paylaşımlara yazdığı cevaplar elde edilmiştir. Söz konusu veri elde etme süreci Twitter’ın gün ve sayı sınırları ile sınırlandırılmaktadır. Bu nedenle kullanıcının son 200 paylaşımına erişim sağlanarak analiz edilebilmektedir. Analiz işlemi süresince seçilen model doğrultusunda kişisel veri ifşa riski içerdiği tespit edilen tivitlerin orijinal hali, veri ön işleme süreçlerinden geçirildikten sonraki hali, sınıflandırma skoru gibi özet bilgileri içerecek şekilde sunulmaktadır.

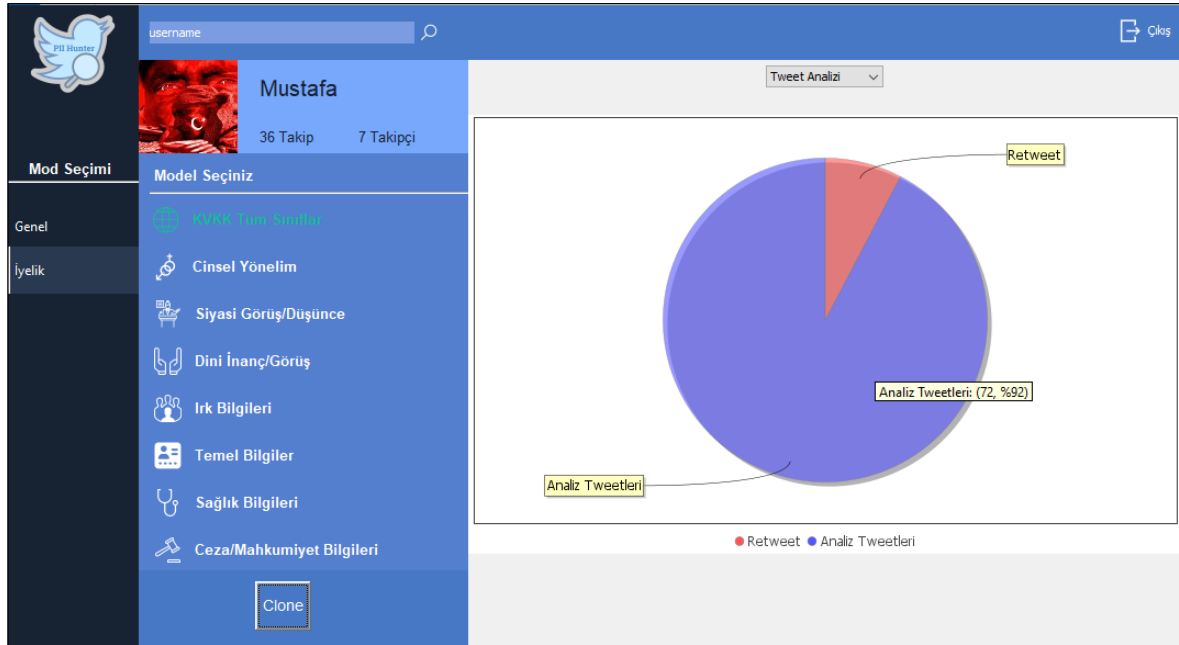


Şekil 6.3. Analiz sürecinde ekran görüntüsü

Analiz tamamlandıktan sonra “Sonuç” butonu aktif hale gelmektedir. Sonuç butonuna basıldığında 4 farklı grafik ekrana ilişkin hesaplamalar yapılarak kullanıcının erişimine açılmaktadır. Bunlar;

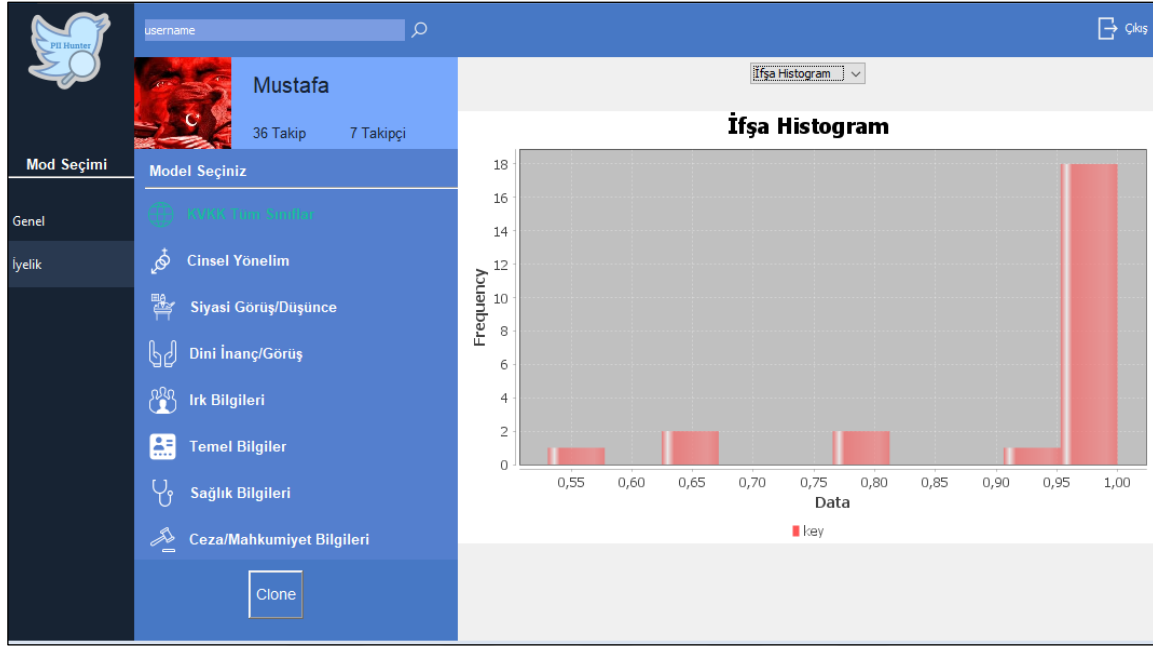
- 1- Kullanıcının elde edilen paylaşımlarından analiz edilen ve kapsam dışı bırakılan (retivit) miktarların görselleştirildiği “Tivit Analiz” ekranı,
- 2- İfşa riski içeren paylaşımlara ilişkin skor ve adetlerin görselleştirildiği “İfşa Histogram” ekranı,
- 3- İfşa riski içermediği değerlendirilen paylaşımlara ilişkin skor ve adetlerin görselleştirildiği “Tivit Histogram” ekranı ve
- 4- İfşa riski içeren tespitlere ilişkin güvenilirliğinin belirlenebilmesi maksadıyla hesaplanan skorun gösterildiği “Güvenirlik Analizi” ekranıdır.

Çalışma kapsamında önceki bölümlerde açıklanan sebeplerle retivitler kapsam dışı bırakılmıştır. Kullanıcının analiz edilen ve kapsam dışı bırakılan paylaşım sayılarının anlaşılabilmesi maksadıyla geliştirilen grafik arayüzün ekran görüntüsü Şekil 6.4’te sunulmuştur.



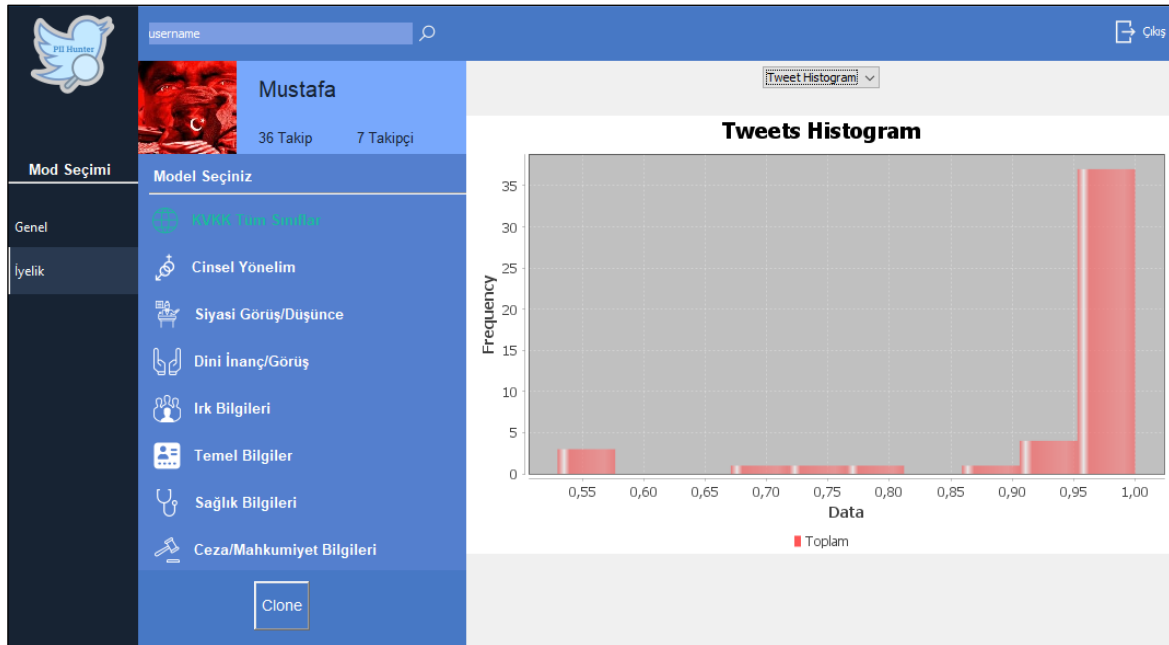
Şekil 6.4. Tivit analizi ekranı

Kullanıcının kişisel veri ifşa riski içeren tivit sayılarının ve skorlarının gösterildiği grafik arayüzün ekran görüntüsü Şekil 6.5'te sunulmuştur.



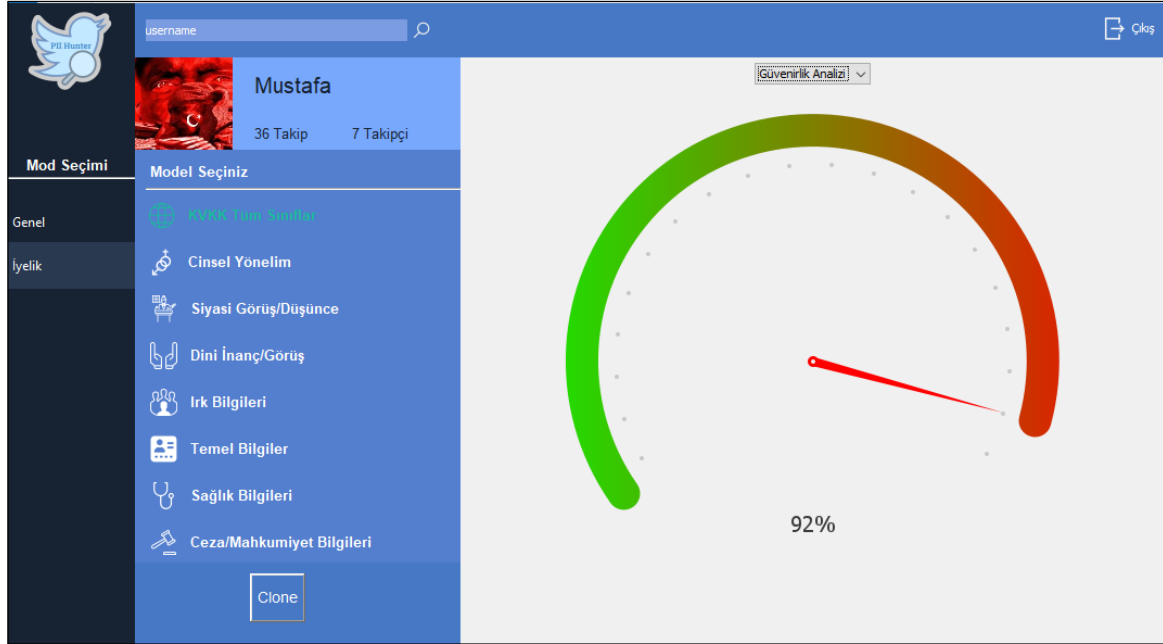
Şekil 6.5. İfşa histogram ekranı

Kullanıcının kişisel veri ifşa riski içermediği değerlendirilen tivit sayılarının ve skorlarının gösterildiği grafik arayüzün ekran görüntüsü Şekil 6.6'da sunulmuştur.



Şekil 6.6. Tivit histogram ekranı

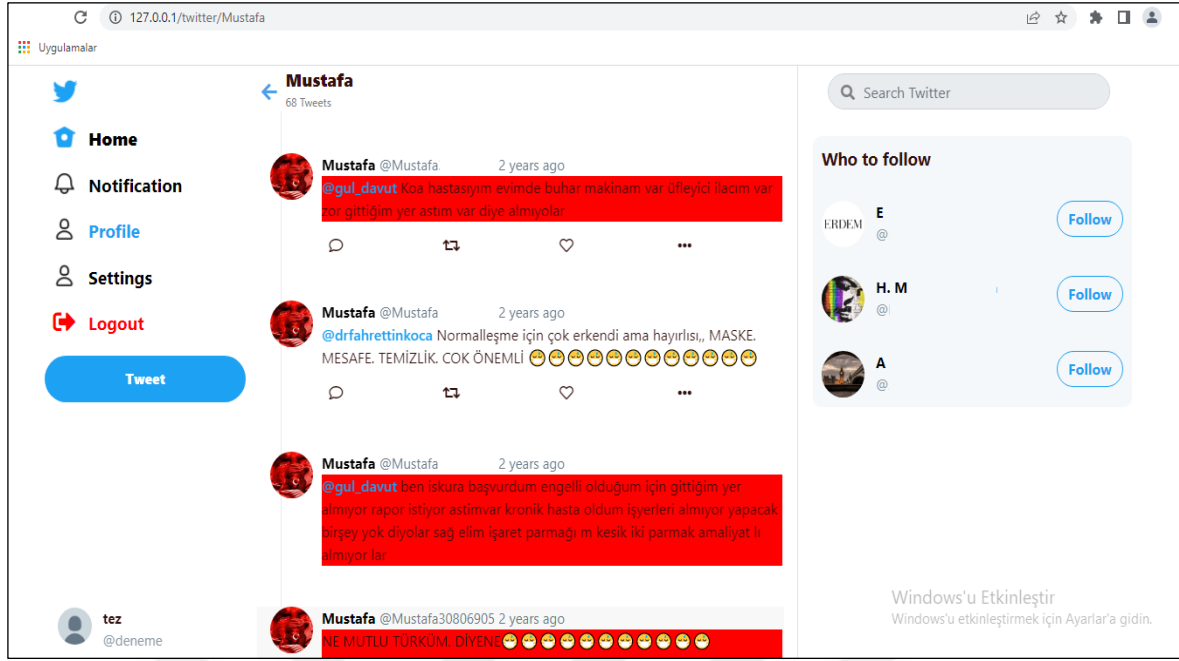
Kişisel veri ifşa riski içeren tivit skorlarının ortalamaları alınarak hesaplanan güvenirlilik skorunun görüntülediği arayüze ilişkin ekran görüntüsü Şekil 6.7’de sunulmuştur.



Şekil 6.7. Güvenirlilik analizi ekranı

Açıklanan ve görselleri sunulan analiz ekranlarının yanı sıra kullanıcıların alışkın olduğu ekranlar üzerinden kişisel veri ifşa riski içeren paylaşımlarının dikkat çekici şekilde sunulması ve bilinçsizce yapılan paylaşımlardan riskli olanlara dikkat çekilebilmesi amacıyla Twitter Clone [142] uygulaması çalışmaya entegre edilmiş ve söz konusu farkındalık ekranının hazırlanabilmesi için kişisel veri ifşa riski içeren tivitlerin renklendirilmesine yönelik düzenlemeler yapılmıştır. Analiz ekranlarında gerekli incelemeler tamamlandıktan sonra “Clone” butonuna tıklandığında kullanıcının sınıflandırma sürecinde ele alınan paylaşımları Twitter web sayfasının birebir kopyası üzerinde renklendirilerek görselleştirilmektedir. Söz konusu uygulamaya ilişkin ekran görüntüsü Şekil 6.8’de sunulmuştur.

Ekran görüntülerinin sunulabilmesi amacıyla Twitter ortamından gerçek bir kullanıcıya ilişkin analizler gerçekleştirilmiş olup kişisel verilerin gizliliği kapsamında kullanıcı adı ve tanımlanmasına sebep olabilecek bazı bilgiler görsellerden silinmiştir.



Şekil 6.8. Twitter clone üzerinde ifşa riski içerdiği tespit edilen paylaşımların gösterilmesi

Tez çalışması kapsamında;

- Birden fazla sınıfa (Sağlık bilgileri, Irk Köken Bilgileri ve Temel bilgiler) ilişkin kişisel veri ifşa riski barındıran tivitler içermesi,
- Yazım yanlışlarının ve yarım bırakılmış cümlelerin tivitler içerisinde yoğun olarak bulunması,
- Türkçe dilinde karşılığı olmayan ifadelerin sıklıkla kullanılması,
- Karakter temizleme adımıyla ele alınan hashtag, mention gibi ifadeler ile emojilerin tivitler içerisinde sıklıkla yer alması,
- Metinler içerisinde URL adreslerinin bulunması,
- Rakamsal ifadelerin sıklıkla metin içerisinde geçmesi,

gibi nedenlerle sınıflandırma açısından model başarımlarını zorlayacağı değerlendirilen bir canlı kullanıcı seçilerek geliştirilen dil modellerinin başarımlarına yönelik testler gerçekleştirilmiştir. T-PH Hunter sistemi ile fastText ve BERT transformer yaklaşımları kullanılarak elde edilen Tüm Bilgi modelleri ile gerçekleştirilen analiz sonuçları karşılaştırmalı olarak Çizelge 6.1’de sunulmuştur. Hatalı tespitler kırmızı ile renklendirilmiştir.

Çizelge 6.1. Genel mod ile Tüm Bilgiler modeli için gerçek veri ile fastText ve BERT modelleri ile gerçekleştirilen sınıflandırma sonuçları

Tivit	Etiket	fastText	BERT
@TTDestek Elemanlar ınız geldi üstüne fırça atıp dalga geçiyor lar ekipler	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek Ya arkadaş verdiğini gün sözü nu bile turmadiniz ayıp değil mi 3ay old yazık gerçek yazık fatura gecikse hemen kesiyorsunuz hala internet yokkkkkk	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek Tarih verdiği halde yapmıyor yazık vallahi yazı söz verdiler söz nedemek cimere atıyorum resimlerw kadarre	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek Yav çalışma NERDE geli bakın burayı kablolar yerde ayıp nasi bı ülkede yaşıyoruz gelip bakmazah metinde bulunmuyorsun ,3ayoldu 4cu ayagirecez Allah'tan korkun. 👍👍👍👍👍	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek Neicelemesi çalışılıyor diyorsunuz. Kimse gelmiyor tüketici hakları şikayet edicemmmm	kvkk_ud	kvkk_ud	kvkk_ud
@unidenduygu @TurkTelekom Vallahi YAZIKLAR OLSUNNNN 3ay elviđannnn internet yok bikabloyu bağlamadunuz çoğu yerde arabalar gelip geçiyor üstünden alsana türk Telekom 🙄🙄🙄🙄🙄 tovbeeeew	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek Kardeşim çalışma falan yok burda kablo gözümün önünde necalismasiilleti kandırma yın okadar kişi magdur	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek @swietrusso Doğru 3ay oldu interneti yavaksinizzz yazikkkkk	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek 3aydır dönüş yapılacak msj geliyo aynı. Boşa laffff	kvkk_ud	kvkk_u	kvkk_ud
@TTDestek Vallah ben hizmet göremedim gelen giden yokkkk 3aydır aynı kelime ,,,,	kvkk_ud	kvkk_u	kvkk_ud
@TTDestek 3aydır bu boyleeeeeee bi kaployu bağlamadılar https://t.co/jC7t4NdjRk	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek İnşaat var bahanesiyle gelmiyorlar Allah bildiği gibi yapsın 3ay yaaaa okul dersveriyorlar cikaramiyoruz vebali sizin boyunuza	kvkk_ud	kvkk_u	kvkk_ud
@TTDestek Vallah hiç bişey yapılmıyor	kvkk_ud	kvkk_ud	kvkk_ud
TÜRK Telekom NERDE 3AY OLDU YAZIKLAR OLSUNNNN https://t.co/Vi2XmhM1i5	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek 3aydır bu böyle teknik servis türk Telekom nerdeeeee yazıklar olsunnnn https://t.co/EVkaUcmecqo	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek Yazikkkk ya söz vermesinler 29 dediler gelen yok 9desiler yok 18 dediler yok sayimmi. Yalanları yazıklar sunnn nn	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek 3ay oldu elviđannnn bugün gectini nasıl kesiyorsunuzzzzz	kvkk_ud	kvkk_u	kvkk_ud
@TTDestek Vallah hiç bi hizmet dahi yok boşa bubu söylemeyin ayıptır ya çalış ma yapılyor diye msj geliyor gözümün onu allahin bı Kulu gelmiyor yazıklar olsun tük Telekom,,, 3 ay oldu elviđannnn	kvkk_ud	kvkk_u	kvkk_ud
@TTDestek Tamamda burda kablo duvar dibinde de ama gelip bakan yokkkk her yerde var 4.. 5 evde yok bunasil oluyor kablo yolumun üstü köpük duru yor ne alt yapisi	kvkk_ud	kvkk_u	kvkk_ud
@TurkTelekom Birtane ekip gelmiyor gaski Tedaş buralarda geziyor türk Telekom yokkkk	kvkk_ud	kvkk_ud	kvkk_ud

Çizelge 6.1. (devam) Genel mod ile Tüm Bilgiler modeli için gerçek veri ile fastText ve BERT modelleri ile gerçekleştirilen sınıflandırma sonuçları

Tivitler	Etiket	fastText	BERT
@TurkTelekom Şimdide 18 diyolar abi okulla sorun yaşıyorum hocalarımız ders veriyor cikaramıyoruz yazıktıryaaaa	kvkk_ud	kvkk_ud	kvkk_ud
@emrahildiz55 @gul_davut Telefon dan bakıyor lar faturada yüksek geldi durumumda yok zor durumdayım saygılarımla arz ederim	kvkk_ud	kvkk_u	kvkk_ud
@trthabercanli @ceyhuntoker1453 Maşallah maşallah Allah güc kuvvet versin sayın cumhurbaşkanımız	kvkk_ud	kvkk_u	kvkk_ud
@gul_davut sayın valim Öğüm Söğüt köyü öğüm Söğüt mahallesi Şehitkamil Gaziantep no 36 tıda koblo böyle bırakılmış Inter net yok cogukisi mağdur okuldan çocuk larımızdan yazı istiyorlar okul hocalarımız ders çıkaramıyor uz lütfen gereği bin yapılması ni arz ederim saygılarımla https://t.co/KGF7o0TrPW	kvkk_ud	kvkk_u	kvkk_u
@TTDestek Buhalde kopuk ayhanbey böyle bırakılır mı. 🤔🤔🤔 https://t.co/PYIIxUFFYu	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek 05348659775ayhanbey ararsanız sevinirim teşekkürler	kvkk_u	kvkk_u	kvkk_ud
@TTDestek Yok abi hiç iletişime geçilmiyor 2ay olmuş ne iletişimi yüzümüze kapanıyor ayıptır müdürlüğü dediler çarşı ya türk Telekom ma gittik Bayan gelecekler dediler gelen yok kaployu öyle bağlayıp gitmişler kimisi yerdeeee ayıppyaaaaa	kvkk_ud	kvkk_u	kvkk_ud
@TurkTelekom 9oldu gelmediler 29desiler gelmediler 4..5..ev mağdur yazık tır günü geldiğinde yatırıldımı kesiliyor yazık magduruzzz....	kvkk_ud	kvkk_ud	kvkk_ud
@TurkTelekom Gaziantep Şehitkamil Başpınar öğüm Söğüt köyü öğüm Söğüt mahallesi no 136 ikametgah etmekteyim 2ay oldu bikabluyu bağlamaya gelmesinin ayıp tırya müşteri hizmetleri nu aramaktan nihal oldu ayıp vallahi dalga gecergibi gün verip söz verildi bu BUKADAR olmaz	kvkk_u	kvkk_u	kvkk_u
@TTDestek Bize i tarih söz verildi vermesinler 29 bitecek dediler oda yok şimdi 9 dediler bekledik oda yok dalgagecergibi kablolar yerde gelin bibakin cokmuzor biz kaldırdık inşaat var ya gaski çalış ti bı ekibi bile gelmedi bir ay oldu ayıp gerçek bidaha tovbeeee	kvkk_ud	kvkk_u	kvkk_ud
@TTDestek @YiitMer22964248 Birtirli iletişime geçmediler malesefff	kvkk_ud	kvkk_ud	kvkk_ud
BİRAKİP GİDİLEN KOBLOLAR İNTERNET YOK MAGDUR OLANLAR	kvkk_ud	kvkk_ud	kvkk_ud
@TDaligunes Maşallah maşallah 🌸 mutlu bayramlar dileriz	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek Duvarda duruyor demek istedi. Kablolar	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek Kablolar	kvkk_ud	kvkk_ud	kvkk_ud
@TTDestek Vallahi mağdur durumda lar kanla duvarda duru yor gelip bibakan yok aramanıza rağmen yazık yani	kvkk_ud	kvkk_u	kvkk_ud
@gul_davut Hayırlı bayramlar sayın valim	kvkk_ud	kvkk_u	kvkk_ud
@gul_davut Bilgilendirme mi rica ettiler	kvkk_ud	kvkk_ud	kvkk_ud
@emineozcelik Mutaga ege hadiii	kvkk_ud	kvkk_ud	kvkk_ud
@mrymdst Sensi hayat yerin dibine batsın 🌸🌸🌸	kvkk_ud	kvkk_u	Kvkk_ud

Çizelge 6.1. (devam) Genel mod ile Tüm Bilgiler modeli için gerçek veri ile fastText ve BERT modelleri ile gerçekleştirilen sınıflandırma sonuçları

Tivitler	Etiket	fastText	BERT
@gul_davut Sayın valim benimde ihtiyacım var o çeke astım KOAH hastasıyım kirada oturuyorum çalışmıyorum sagelim parmaklarım dikimi işaret parmağım kesik faprikalar almıyor ilaç alamıyorum neyapacağımı bilemiyorum öğüm Söğüt köyü öğüm Söğüt mahallesi no 136	kvkk_u	kvkk_u	kvkk_u
@cikolatlikayisi Tehlikelisinnnn dikkat etmeklazımmmm 🌹🌹🌹	kvkk_ud	kvkk_ud	kvkk_ud
@ganteptvaliligi @gul_davut Öğüm Söğüt köyü öğüm Söğüt mahallesi no 136	kvkk_u	kvkk_u	kvkk_ud
@ganteptvaliligi @gul_davut Sayınvalim astım KOAH hastasıyım kirada oturuyorum çalışmıyorum sagelimde 1 parmak kesik faprikalar almıyo çalışmıyorum Allah rızası için yardım bekliyor arzederim	kvkk_u	kvkk_u	kvkk_u
@lcansukorkmaz Sağol günahına ortak etme bariiiii 🤔🤔🤔🤔🤔🤔	kvkk_ud	kvkk_ud	kvkk_ud
@gul_davut sayın valim gıda ve nakli yardım veriliyor Muş baş vurduğum hala bi sonuç alamadım astım KOAH hastasıyım kirada oturuyorum çalışmıyorum zor durumdayım saygılarımla arz ederim	kvkk_u	kvkk_u	kvkk_u
SENİ YAZDIM KALBİME,👉👉👉👉👉👉 https://t.co/7V5TBXcyB5	kvkk_ud	kvkk_ud	kvkk_ud
@mervecimbirdur Cumhurbaşkanı mizin bilafi var sen ne kadar gerizakilisin 😊😊😊😊😊😊	kvkk_ud	kvkk_u	kvkk_ud
@BlackSwan_BW @gazatr Doğru dur budun ya iyi olmayanların dünyası 🤔🤔🤔🤔	kvkk_ud	kvkk_ud	kvkk_ud
@gul_davut Yardım fan faydalanmak istiyorum saygılarımla	kvkk_u	kvkk_ud	kvkk_ud
@gul_davut Sayın valim Gaziantep Şehitkamil Başpınar öğüm Söğüt köyünde ikametgah etmekteyim astım KOAH hastasıyım kirada oturuyorum çalışmıyorum hiç bir işyeri almıyor sağ elimde parmakmagim kesik faprikalar almıyor ilaç alamıyorum neyapacağımı bilemiyorum saygılarımla arz ederim	kvkk_u	kvkk_u	kvkk_u
@mrymdst Marifetmiş gibi soruyor pis ilet o 🤔🤔🤔	kvkk_ud	kvkk_ud	kvkk_ud
Stayla paket kaynımın acil satlık 0530 929 09 92 https://t.co/KrJWhosAGz	kvkk_ud	kvkk_ud	kvkk_ud
Stayla paket kaybının acil satlık https://t.co/yQ1f75ihHR	kvkk_ud	kvkk_ud	kvkk_ud
MEKANIN CENNET OLSUN 🤔🤔🤔🤔🤔🤔 https://t.co/5DqHEyCgoP	kvkk_ud	kvkk_ud	kvkk_ud
ALLAH rahmet eylesin mekanı cennet olsun inşaallah 🤔🤔🤔🤔🤔🤔🤔🤔🤔🤔🤔🤔 https://t.co/VqKJKEiwsM	kvkk_ud	kvkk_ud	kvkk_ud
@gul_davut Allah şifa versin valimiz bastacımız	kvkk_ud	kvkk_ud	kvkk_ud
@kubraniziim Senin yüksek heralde taktına göre	kvkk_ud	kvkk_ud	kvkk_ud
@emrelncc2 Hadi hayırlısıyla gelbi	kvkk_ud	kvkk_ud	kvkk_ud
@Delidirdeliii Sana hangisi matıklıysa banada o olur canım 😊😊😊😊😊😊😊😊😊😊😊😊😊😊😊😊	kvkk_ud	kvkk_u	kvkk_ud
@haluklevent abi Gaziantep hiç yardım edilmedi şehit Kamil öğüm Söğüt köyü öğüm Söğüt mahallesi no 51 5358659775 tlf	kvkk_u	kvkk_u	kvkk_u

Çizelge 6.1. (devam) Genel mod ile Tüm Bilgiler modeli için gerçek veri ile fastText ve BERT modelleri ile gerçekleştirilen sınıflandırma sonuçları

Tivitler	Etiket	fastText	BERT
@drfahrettinkoca Fakirin oturduğu nerde görülüşkü	kvkk_ud	kvkk_ud	kvkk_ud
@BedihaGs @yigitemine0 Bedia 23 nisan çektik beyeni yap	kvkk_ud	kvkk_ud	kvkk_ud
@yigitemine0 Emine. Yigite	kvkk_ud	kvkk_ud	kvkk_ud
@yigitemine0 Lütfen beyeni istiyorum	kvkk_ud	kvkk_ud	kvkk_ud
AnTEPLİ OLSAKTA. GS AŞKI https://t.co/3ZNqDEebyL	kvkk_u	kvkk_u	kvkk_u
@gul_davut sayın valim kömür gelmedi koa hastasıyım kirada oturuyorum ödeyemiyor zor durumdayım çalışanı yorum engelliyim 40 raporum vardı 20 düş tü heyete girmem gerekiyor 6ay beklemek zorunda kaldım iskura gitt işlere yönlendiri tırlar almıyorlar rahatsızlığın neyapacağım	kvkk_u	kvkk_u	kvkk_u
MEKANI CENNET OLSUN https://t.co/SnbWxP2iNp	kvkk_ud	kvkk_ud	kvkk_ud
Aile, Çalışma ve Sosyal Hizmetler Bakanlığı Pandemi Sosyal Destek Ön Başvurusu https://t.co/ALnfvcW6tk @ekapi aracılığıyla	kvkk_ud	kvkk_ud	kvkk_ud
@gul_davut sayın bakanım heryere kömür dağıtılmış amabize hala gelmedi cikti halde koa hastasıyım calisamiyoeymmm	kvkk_u	kvkk_u	kvkk_u
@YildizzTilbee Yıldız hanım bende düşünmüyorum bende vurulmaya ağı m	kvkk_ud	kvkk_ud	kvkk_ud
@gul_davut sayın valim is bulamadım astım KOAH hastası olduğu m için almıyor lar neyapacağı bilmiyorum 40 enlim vardı 24dusti 6ay bekliycem tekrardan heyete giricem yardım aldım 6bekliyeceksin dediler daha önce size yazmıştım işkur gönderi yor almıyorlar köyde oturuyorum	kvkk_u	kvkk_u	kvkk_u
EFE MUSTAFA  https://t.co/RHg08e0cuh	kvkk_ud	kvkk_ud	kvkk_ud
@gul_davut yardım almayan kimseyok çocuk parası almıyor um iki adım da nefesim kesiliyor oturduğum yer iki oda sadece ehleytsizlikten ceza yemiştım zorbyatırdım engelli otobus kartım iptal olukmu bilmiyorum yoldakimse almıyorlar köyde oturuyorum öğüm Söğüt köyü	kvkk_u	kvkk_u	kvkk_u
@gul_davut biri ilc raporum bide düşük verilen	kvkk_u	kvkk_u	kvkk_u
@gul_davut Koa hastasıyım evimde buhar makinam var üfleyci ilacım var zor gittiğim yer astım var diye almıyorlar	kvkk_u	kvkk_u	kvkk_u
Bel fitiği var roparum vardı 40 24 dustu tekrardan 6 sonra diyorlar https://t.co/KUTMmURo4L	kvkk_u	kvkk_u	kvkk_u
@gul_davut ben iskura başvurdum engelli olduğum için gittiğim yer almıyor rapor istiyor astımvar kronik hasta oldum işyerleri almıyor yapacak birşey yok diyorlar sağ elim işaret parmağı m kesik iki parmak amaliyat lı almıyor lar	kvkk_u	kvkk_u	kvkk_u
Sayın valim kiramı suyu yatıranıyorm çalışamı yorum yardımcı olursanız sevinirim saygılarımla arz ederim https://t.co/PfSh2Hzpgg	kvkk_u	kvkk_u	kvkk_u
@gul_davut Sayın valim zordurumdayım allahrızası için yardım istiyorum 2 çocuğum var okul eşyasını zor aldım r var dolmuş 40 engellim var dı düşük verdiler astımım buronsit koa hastasıyım istifa ettirdiler zordurumdayım sosyal yardımlaşma pandemi 2 kere yardım aldım şimdi yok yakacağım yok	kvkk_u	kvkk_u	kvkk_u

Çizelge 6.1. (devam) Genel mod ile Tüm Bilgiler modeli için gerçek veri ile fastText ve BERT modelleri ile gerçekleştirilen sınıflandırma sonuçları

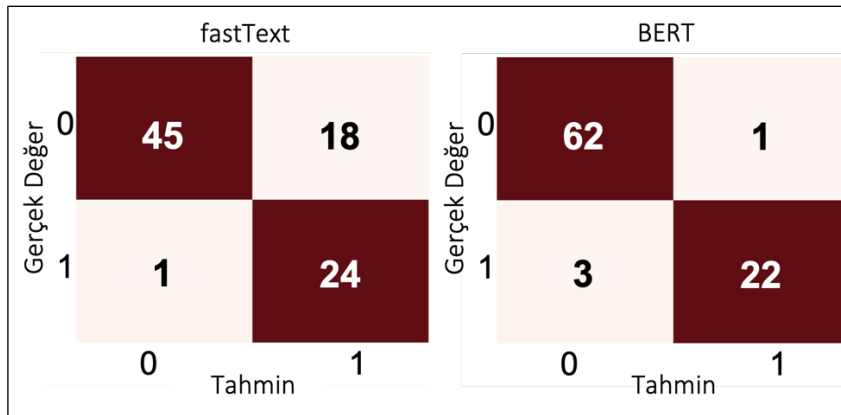
Tivitler	Etiket	fastText	BERT
@drfahrettinkoca FAHRETTİN HOCAM ZOR DURUMDAYIM LÜTFEN YARDİMCİOLUN SAĞLIK ÇALIŞA Nİ İDİ İSTİFA Ettirdiler VE ALMADILAR 40 ENGELLİ M VARDİ ODA GİTTİ ÇALIŞAMIYOR ASTİM KOA HASTA SİYİM KİRA EVİM GECİNE MIYORUM 5348659775 LÜTFEN YARDİMCİ OLUN	kvkk_u	kvkk_u	kvkk_u
NE MUTLU TÜRKÜM. DİYENE🙏🙏🙏🙏🙏🙏🙏🙏🙏🙏 https://t.co/NIWDRStY9e	kvkk_u	kvkk_u	kvkk_u
@drfahrettinkoca Normalleşme için çok erkendi ama hayırlısı,, MASKE. MESAFE. TEMİZLİK. COK ÖNEMLİ 🙏🙏🙏🙏🙏🙏🙏🙏🙏🙏	kvkk_ud	kvkk_u	kvkk_ud
@_lostlife1 Dedi kodusuda çok olur amanhaaaaaa🙏🙏🙏🙏🙏🙏🙏🙏	kvkk_ud	kvkk_ud	kvkk_ud
@drfahrettinkoca Lütfen msjlarimi bakarmisini Allah rızası için yardım istiyorum	kvkk_ud	kvkk_u	kvkk_ud
@drfahrettinkoca Sayın hanım elimde de sorun var ağır işte çalışamaz roporum var astım sonradan oldum bel Didim var amaliyat dediler olmadım zor duruyor ağır işte çalışamaz hale geldi m allahrızası için yardım	kvkk_u	kvkk_u	kvkk_u
@drfahrettinkoca Raporum süresiz ibaresi var zor geçiniyor um cocugum lsinifa gidiyor okul eşyasını zor aldım raporum olmadan işyerleri almıyor temizlik personeli idim astımım buronsitten doloyi istifa ettirdiler zordurumdayım allahrızası için yardım istiyorum senialirizdedi hastane şefi almadı	kvkk_u	kvkk_u	kvkk_u
@drfahrettinkoca Sayın bakanım Gaziantep Şehitkamil ilçesinde ikamet etmekteyi 40engelim vardı 24dusurduler astımım var işten istifa ettirdiler zordurumdayım allahrızası için yardım istiyorum itiraz ettim rapora 6ay beklediyolar ev kira zorgeciniyorum 2 kez girdim	kvkk_u	kvkk_u	kvkk_u

Gerçekleştirilen sınıflandırma işlemleri sonucunda analiz edilen 88 tivitten fastText ile oluşturulan model ile 13, BERT transformer (En yüksek test performansı elde edilen ConvBERTurk ön eğitilmiş modelinin finetune edilmesi ile oluşturulan model kullanılmıştır) modeli ile 4 adet tivit hatalı olarak sınıflandırılmış olup performans metrikleri karşılaştırmalı olarak Çizelge 6.2’de sunulmuştur.

Çizelge 6.2. fastText ve BERT modelleri performans metrikleri

	Etiket	Kesinlik	Geri Çağırma	F1-Skoru	Doğruluk	Örnek
fastText	kvkk_u	0,57	0,96	0,71	0,78	25
	kvkk_ud	0,97	0,71	0,82		63
BERT	kvkk_u	0,88	0,95	0,91	0,95	25
	kvkk_ud	0,98	0,95	0,96		63

Gerçekleştirilen testler sonucunda fastText ve BERT transformer modelleri ile elde edilen sonuçlara ilişkin oluşan karmaşıklık matrisleri Şekil 6.9’da sunulmuştur.



Şekil 6.9. fastText ve BERT modeli karmaşıklık matrisleri

Canlı kullanıcı ile gerçekleştirilen testler sonucunda elde edilen doğruluk değerlerinin fastText için Çizelge 5.10’da sunulan 0,77’lik doğruluk oranı, BERT için elde edilen değerin Çizelge 5.14’te sunulan 0,93’lük doğruluk oranı ile uyumlu olduğu görülmektedir. BERT transformer modeli ile oluşturulan dil modeli kullanılarak yapılan testlerde, karakter temizleme dışında herhangi bir ön işlemden geçirilmemesine rağmen fastText’e göre ciddi seviyede yüksek başarıma sahip sonuçlar elde edilmiştir.

fastText ile gerçekleştirilen sınıflandırma sonucunda elde edilen 0,78 doğruluk oranının iyileştirilmesi maksadıyla çalışma kapsamında geliştirilen “İyelik” modu seçilerek tekrar sınıflandırma yapılarak sonuçlar karşılaştırılmıştır. Riskli tespitler içerisinde çıkarılan paylaşımlar Çizelge 6.3’te sunulmuştur.

Çizelge 6.3. İyelik modu ile yapılan sınıflandırmada düzeltilen hatalı tespitler

Titviter
@TTDestek 3aydır dönüş yapılacak msj geliyo aynı. Boşa laffff
@TTDestek 3ay oldu elvijdannnn bugün gectini nasıl kesiyorsunuzzzzz
@TTDestek Vallahi mağdur durumda lar kanla duvarda duru yor gelip bibakan yok aramanıza rağmen yazık yani
@mrymdst Sensi hayat yerin dibine batsın 🌹🌹🌹🌹
@mervecimbirdur Cumhurbaşkanı mizin bilafi var sen ne kadar gerizakilisiz😏😏😏😏
@drfahrettinkoca Normalleşme için çok erkendi ama hayırlısı,, MASKE. MESAFE. TEMİZLİK. COK ÖNEMLİ 🙏🙏🙏🙏🙏🙏🙏🙏🙏🙏🙏🙏🙏🙏🙏🙏

Uygulama iyelik modunda çalıştırıldığında 13 adet hatalı tespit içerisinde 5 tanesinde herhangi bir iyelik eki (Ben, biz) bulunmaması nedeniyle, 1 tanesinde ise “Cumhurbaşkanı mizin” şeklinde yazım hatası ile ifade edildiğinden dolayı iyelik eki tespit edilemediğinden toplam 6 tivit kişisel veri içermediği değerlendirilerek riskli tespitler içerisinde çıkarılmıştır.

İyelik modu uygulandıktan sonra oluşan yeni TP (24), TN (51), FP (12) ve FN (1) değerleri doğrultusunda hesaplanan performans metrikleri Çizelge 6.4’te sunulmuştur. Çizelge 6.2’de sunulan değerler ile karşılaştırıldığında doğruluk değerinin %78’den %85’e yükseldiği, söz konusu iyelik kontrolünün sınıflandırma sonuçlarına olumlu katkı sağladığı görülmektedir.

Çizelge 6.4. İyelik modu performans metrikleri

	Kesinlik	Geri Çağırma	F1-Skoru	Doğruluk	Örnek
fastText + iyelik modu	0,66	0,96	0,78	0,85	88



7. SONUÇ VE ÖNERİLER

Bu çalışmada; sosyal ağlarda kullanıcılar tarafından bilinçsizce paylaşılan ve kişisel veri ifşa riski içeren tivitlerin otomatik olarak tespit edilerek gizlilik ve mahremiyet farkındalığının tespiti ve ölçümüne yönelik modeller ve bu çalışmanın gerçek zamanlı olarak gerçekleştirilebileceği bir sistem geliştirilmiş ve başarı ile test edilmiştir.

Yapılan çalışmalarda; ilk olarak, sosyal veri kavramı ve gizlilik kavramına yönelik bir literatür incelemesi gerçekleştirilerek sosyal ağlarda gizlilik, mahremiyet kavramları ile kişisel veri ihlalleri ve farkındalık arasındaki ilişki derinlemesine ele alınmış ve yeni bir çözüm sunulmuştur.

İkinci olarak, sosyal ağlardan elde edilen veriler kullanılarak gerçekleştirilen ve uygulama içeren çalışmalar detaylı olarak incelenmiş ve tez çalışması kapsamında kullanılabilecek yöntem, metodoloji, veri kaynakları gibi hususlar belirlenerek yeni çözüm önerileri geliştirilmiştir. Bu kapsamda;

- Belirlenen metodoloji doğrultusunda Türkçe veri setlerinin elde edilmesine yönelik çalışmalar gerçekleştirilmiş, Kişisel Verilerin Korunması Kanunu kapsamında ele alınan temel ve hassas bilgiler bütüncül bir yaklaşımla ele alınmış, toplam 284 farklı arama kelimesi ile kişisel veri sınıflarına ilişkin arama sözlükleri içeren Türkçe korpus ilk kez oluşturulmuş ve araştırmacıların kullanımına sunulmuştur. Bu korpus; 3 aylık süre boyunca Twitter ortamından veriler elde edilerek toplam 39.888 adet tivit 109 farklı etiket ile 7 farklı sınıf altında etiketlenmiş, kişisel veri ifşa riski barındıran tivitlerin tespitine yönelik Türkçe dilinde ilk kez hazırlanan özgün veri seti literatüre kazandırılmıştır. Gerçekleştirilecek çalışmalara referans olacağı değerlendirilen bu veri setinin farklı dillerde yapılan çalışmalar da göz önüne alındığında kişisel veri tespitine yönelik hazırlanmış en kapsamlı veri seti olduğu değerlendirilmektedir.
- Verilerin elde edilmesi ve etiketlenmesini takiben doğal dil işleme süreçlerine yönelik Zemberek kütüphanesi kullanılarak veri ön işleme adımları gerçekleştirilmiş, hatalı yazım düzeltme (Normalizasyon) ve anlamsal kök

çıkarımı işlemleri bu verilere uygulanmış ve fastText yaklaşımı ile gerçekleştirilecek dil modeli oluşturma çalışmalarına uygun hale getirilmiştir.

- Elde edilen veri setleri kullanılarak kişisel veri ifşa riski barındıran tivitlerin tespitine yönelik Türkçe dil modelleri ilk kez oluşturulmuştur. Söz konusu modellerin oluşturulması maksadıyla fastText ve BERT transformer yaklaşımları kullanılarak oluşturulan 8 farklı sınıf için ayrı ayrı dil modelleri gerçekleştirilmiş ve bu modellerde %75-91 arası doğruluk değerleri elde edilmiştir. BERT transformer yaklaşımı ile oluşturulan dil modelleri 3 farklı ön eğitilmiş modelin ince ayar yapılması ile elde edilmiş olup %90-95 arası doğruluk değerlerine erişilmiştir.
- Elde edilen dil modelleri, Zemberek kütüphanesi kullanılarak gerçekleştirilen doğal dil işleme süreçleri, veri ön işleme süreçleri ve sınıflandırma işlemleri sosyal ağ kullanıcılarının kişisel veri ifşa riski barındıran tivitlerinin analizinin gerçekleştirilmesi maksadıyla Java programlama dilinde geliştirilen T-PII Hunter sistemine entegre edilmiştir. Söz konusu sistem Türkçe kişisel veri ifşa riski barındıran tivitlerin otomatik olarak başarılı bir şekilde tespitine imkân sağlayan ilk sistem geliştirilmiş ve başarıyla test edilmiştir.
- Bu tez kapsamında yapılan çalışmalar ve geliştirilen T-PII Hunter sistemi ile geliştirilen analiz ve otomatik tespit sisteminde elde edilen sonuçların kullanıcı farkındalığının artırılmasına imkân sağlayacak şekilde Twitter Clone uygulaması ile entegre edilmesi sağlanmış ve ifşa riski barındıran tivitlerin kolaylıkla anlaşılması için ise kırmızı renkte gösterilmesine yönelik geliştirmeler yapılmıştır. Söz konusu entegrasyon ile kişisel veri ifşa riski barındıran Türkçe tivitlere yönelik olarak ilk kez farkındalık tespit ve sunum sistemi geliştirilmiştir.

Söz konusu çalışmalar doğrultusunda geliştirilen sistem ile kullanıcıların gizlilik ve mahremiyetinin bilinçsizce ihlal edilmesine sebep olan kişisel ifşa riski barındıran tivitleri tüm bilgiler sınıfı için fastText modeli ile %77 doğrulukla sınıflandırılmış, elde edilen tespit doğruluk değerinin yükseltilmesi maksadıyla gerçekleştirilen çalışmalar kapsamında BERT transformer yaklaşımı ile en çok %95'e yükseltilmiştir. Gerçekleştirilen çalışmalar doğrultusunda canlı kullanıcı verisi ile örnek bir analiz gerçekleştirilmiş olup söz konusu çalışmada yapılan testlerde elde edilen sonuçlarla uyumlu doğruluk değerleri elde edildiği görülmüştür. Her ne kadar literatürde fastText yaklaşımı ile Türkçe için başarılı sonuçlar elde edildiği görülse de BERT transformer yaklaşımı elde edilen sonuçlar ile doğruluk değerinde %18'lik bir artış sağlanmıştır.

Yapılan çalışma sonucunda geliştirilen sistem ve elde edilen sonuçlar ile elde edilen yüksek başarımın tam olarak anlaşılabilmesi için sosyal ağ verilerinin yapısı göz önüne alınmalıdır. Kısa metin (short text) olarak adlandırılan grupta yer alan tivitler birçok dezavantajı içerisinde barındırmaktadır. Bu dezavantajlar şu şekilde özetlenebilir;

- Kelime sayılarındaki azlık ve kelime frekanslarının düşük olması [151].
- Sosyal ağların kullanım şekli ve kullanıcı alışkanlıkları doğrultusunda konuların metin içerisinde çok hızlı değişim göstermesi [151], tek bir paylaşımda birden fazla konuya ilişkin duygu ve düşüncelerin belirtilmesi.
- Sosyal ağlarda yapılan paylaşımlarda kullanılan özel tabirler, kısaltmalar, hatalı ve dil bilgisi kurallarına uygun olmayan yazımlar, alaycı ve dolaylı anlatımlar, doğal dil işleme konusunda yaşanan kayıplar [6].

Kısa metinlerin özellikleri doğrultusunda yaşanan dezavantajların yanı sıra metin sınıflandırma süreçlerinde de zorluklarla karşılaşmaktadır. Bunlar;

- Çalışmaların İngilizce üzerinde yoğunlaşması nedeniyle karakter sorunu gibi problemlerin çözülmesinin akademik çalışmalarda ortaya çıkardığı zorluklar,
- Yüksek sınıflandırma başarımı açısından en iyi sonuçlar öğreticili öğrenme yöntemleri ile elde edilirken öğreticisiz ya da yarı-öğreticili öğrenmeye dayalı yöntemlerin doğru sınıflandırma oranlarının kısmen daha düşük olması [152],
- Otomatik etiketleme yöntemlerinin mevcut çalışmalarda istenilen doğruluk seviyesinde olmaması nedeniyle etiketlenmiş veri sayılarının kısıtlı olması [118] ve örneklerin ardışık gelmesi nedeniyle veri setinde bazı benzer örnekler çok yoğun yer alırken bazı örneklerin hiç yer almaması [151],
- Yüksek doğrulukla sınıflandırma yapılması için modelin eğitiminde kullanılacak veri seti oluşturulurken farklı türde örneklerin yer almasını sağlamak gerektiğinden arama kelimelerinin belirlenmesinde yaşanan zorluklar,
- Son yıllarda fastText, BERT gibi modeller kullanılarak oluşturulan dil modellerinde yer verilmeye başlamasına rağmen Türkçe için ön eğitilmiş dil modelleri başta olmak üzere metin sınıflandırma konusunda kullanıma sunulmuş model ve uygulamaların özellikle İngilizce dili için geliştirilen modellere göre sayısal olarak oldukça az ve yetenek olarak kısıtlı olması,

- Türkçe için literatürde yapılan çalışmaların duygu analizi ve konu sınıflandırması üzerinde yoğunlaşmış olması nedeniyle kişisel veri ifşa riski bulunan paylaşımların tespitine yönelik referans çalışmalarının bulunmaması ve
- Literatürde yer alan çalışmalarda daha çok tek bir araştırma sorusu ya da belirli konular üzerinde kısıtlı bir alanı kapsayacak şekilde gerçekleştirilmesi nedeniyle bütüncül bakış açısıyla gerçekleştirilen çalışmalarda yaşanan zorluklar,

olarak özetlenebilir.

Kısa metinlerin yapısından kaynaklanan ve sınıflandırma konusunda karşılaşılan dezavantajlar nedeniyle kısıtlı miktarda veri ile gerçekleştirilen model eğitimlerinde aşırı öğrenme (over-fitting) ile ilgili sorunlar da ortaya çıkabilmektedir [153]. Tüm dezavantajlar değerlendirildiğinde Türkçe veriler ile ilk kez gerçekleştirilen ve kişisel veri ifşa riski bulunan paylaşımların tespit edilmesi amaçlanan tez çalışması kapsamında fastText modeli ile elde edilen %75-90 aralığındaki doğruluk oranları ile BERT modeli ile elde edilen %95 doğruluk oranının yüksek bir başarıyı ifade ettiği görülmektedir. Elde edilen yüksek başarımın gelecekte kişilerin gizlilik ve mahremiyetinin temelini oluşturan kişisel verilerindeki sızıntıların tespitine yönelik gerçekleştirilecek çalışmalara ciddi bir altlık ve referans oluşturacağı değerlendirilmektedir.

Literatürde yer alan çalışmalarda Türkçe veriler ile kişisel verilerin tespitine yönelik çalışma bulunmamakla beraber diğer dillerde gerçekleştirilen sınıf bazlı çalışmalarda %56-88 aralığında değişen değerlerde doğruluk oranları elde edildiği görülmektedir. Metin sınıflandırma işlemlerinde diğer dillere göre daha fazla dezavantaj barındırmasına rağmen Türkçe için bu çalışmada elde edilen sonuçların diğer diller ile gerçekleştirilen çalışmalarla benzerlik gösterdiği, birçok çalışmadan daha yüksek sonuçlar elde edildiği, BERT transformer yaklaşımı ile şu ana kadar elde edilen en yüksek başarımın elde edildiği görülmektedir. Bu açıdan eğitilen dil modellerinin gelecek çalışmalara temel ve referans sağlama açısından önemli olduğu ve farklı yöntem ve teknolojiler kullanılarak gerçekleştirilecek çalışmalarla söz konusu doğruluk değerinin arttırılmasına yönelik umut verici olduğu değerlendirilmektedir.

Çalışma kapsamında oluşturulan dil modelleri geliştirilen T-PII Hunter adlı uygulamaya entegre edilerek Twitter üzerinden elde edilen gerçek ve güncel verilerin sınıflandırılmasına imkân sağlanmıştır. Söz konusu uygulamanın bu alanda gerçekleştirilecek çalışmalara bir

referans olacağı ve kullanıcıların bilinçsizce yaptığı kişisel veri ifşalarının etkileşimli bir şekilde gösterimine imkân sağlaması nedeniyle kişisel farkındalığın arttırılmasına katkı sağlayacağı değerlendirilmektedir.

Sosyal ağ verileri kullanılarak kişisel veri ifşa risklerinin tespitine ve görselleştirilmesine yönelik gerçekleştirilen bu çalışmanın Türkçe gerçekleştirilen ilk çalışma olması, kişisel verilerin tespitine yönelik yöntem ve kriterlerin ortaya konulması, kişisel verilere ilişkin Türkçe veri seti oluşturulması maksadıyla kullanılabilecek bir veri sözlüğünün literatüre kazandırılması, söz konusu alanda kullanılabilecek Türkçe veri setinin özgün olarak hazırlanmış olması ve yüksek doğrulukla çalışan dil modellerinin oluşturulması, yönleriyle literatüre katkı sağlayacağı ve gerçekleştirilecek çalışmalara ışık tutacağı değerlendirilmektedir.

Gelecek çalışmalar olarak; geliştirilen T-PII Hunter adlı uygulama kişisel bazda kullanıcıların paylaşımlarını temel alacak şekilde geliştirilmiş olup yapılacak ilave çalışmalarla kurum/firma gibi bir topluluğa ait kişilerin toplu olarak analiz edilmesi ile kurumsal farkındalığın tespitine imkân sağlayabileceği, gündemde yer alan bir konuya ilişkin kişilerin duygu ve düşüncelerini paylaşırken bilinçsizce yaptığı kişisel veri ifşaları doğrultusunda analizler yapılmasına imkân sağlayabileceği değerlendirilmektedir. Özetle, kişisel farkındalığın arttırılması amacıyla gerçekleştirilen çalışmanın yapılacak ilave çalışmalarla kurumsal, toplumsal bazda da sonuçlar elde edilmesine yönelik yapılacak çalışmalara altlık oluşturacağı açıktır.

T-PII Hunter sistemi her ne kadar sosyal ağlar temel alınarak hazırlanmış olsa da kurumsal eposta içerikleri, web sayfalarında açık olarak paylaşılan bilgiler gibi farklı alanlarda yer alan içeriklerin de sınıflandırılmasına yönelik kullanılabileceği değerlendirilmektedir. Gelecekte bahse konu alanlarda yapılacak çalışmaların literatüre ve kişisel/kurumsal/toplumsal farkındalığın ölçülmesine ve arttırılmasına katkı sağlayacağı düşünülmektedir.

Bunlara ilave olarak; kişisel veri ifşa riski bulunan tivitlerin tespitine yönelik oluşturulan modellerde rakamsal ifadeler karakter temizleme aşamasında silinmektedir. Söz konusu rakamsal ifadeler kimi zaman telefon numarası kimi zaman doğum tarihi gibi önemli kişisel verilere karşılık gelmektedir. Gelecek çalışma olarak rakamsal verilerin silinerek

kaybedilmesi yerine sınıflandırma işlemlerinde etkin olarak kullanılabilmesi maksadıyla Varlık İsmi Tanıma (NER) ya da düzenli ifadeler (Regex) gibi yöntemlerle metin içerisinde tespit edilerek etiketlenmesi ve model eğitimlerinde etiketli hali ile kullanılarak model başarımlarının yükseltilmesi planlanmaktadır. Ayrıca, büyük veri ortamları ile uyumlu olarak çalıştırılabilir şekilde tasarlanan yapı sayesinde söz konusu uygulamanın büyük veri ortamlarına taşınmasının söz konusu çalışmaya ilave yetenekler kazandırılmasının önünü açacağı, yeni uygulamalarının geliştirilmesine altyapı oluşturacağı, geliştirilen yeteneklerin farklı platformlara entegre olabileceği ve yeni modellerin geliştirilebileceği değerlendirilmektedir.



KAYNAKLAR

1. İnternet: Facebook'a Cambridge Analytica skandalı nedeniyle 5 milyar dolar ceza kesilecek. (2019). URL: <https://www.bbc.com/turkce/haberler-dunya-48974921>, Son Erişim Tarihi: 26.12.2021.
2. İnternet: All data breaches in 2019-An alarming timeline. (2019). URL: <https://selfkey.org/data-breaches-in-2019/>, Son Erişim Tarihi: 26.12.2021.
3. Kemp, S. (2021). Digital 2021 Global Overview Report.
4. İnternet: Customer data: Designing for transparency and trust. (2015). URL: <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>, Son Erişim Tarihi: 26.12.2021.
5. İnternet: Global digital population as of January 2021. (2021). URL: <https://www.statista.com/statistics/617136/digital-population-worldwide/>, Son Erişim Tarihi: 04.07.2021.
6. Erol, S. E., Sağiroğlu, Ş. (2021). *Privacy awareness in social networks*. 2021 International Conference on Information Security and Cryptology (ISCTURKEY).
7. İnternet: Cost of a Data Breach Report. (2021). URL: <https://www.ibm.com/downloads/cas/OJDVQGRY>, Son Erişim Tarihi: 01.05.2022.
8. Alder, S. (2021). December 2021 Healthcare Data Breach Report.
9. Sohoraye, M., Gooria, V., Nundoo-Ghoorah, S., Koonjal, P. (2015). *Do you know Big Brother is watching you on Facebook? A study of the level of awareness of privacy and security issues among a selected sample of Facebook users in Mauritius*. 2015 International Conference on Computing, Communication and Security (ICCCS).
10. Morgan, S. (2019). 2019 Official Annual Cybercrime Report.
11. İnternet: Data breaches compromised 3.3 billion records in first half of 2018. (2018). URL: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/data-breaches-compromised-3-3-billion-records-in-first-half-of-2018>, Son Erişim Tarihi: 26.12.2021.
12. Zou, H. (2016). *Protection of personal information security in the age of big data*. 2016 12th International Conference on Computational Intelligence and Security (CIS).
13. İnternet: Data Breach Investigations Report. (2021). URL: <https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf>, Son Erişim Tarihi: 01.05.2022.
14. Zhao, H., Haoxin, D. (2017). Research on personal privacy protection of China in the era of big data. *Open Journal of Social Sciences*, 5 (6), 139-145.

15. Fraenkel, O. K. (1968). ALAN F. WESTIN. Privacy and Freedom. Pp. xvi. New York: Atheneum, 1967. *The ANNALS of the American Academy of Political and Social Science*, 377 (1), 196-197.
16. Aslanyürek, M., Türk, S. M. (2015). *İnternet güvenliği ve çevrimiçi gizlilik alanında yaşanan sorunlar:İnternet ve sosyal medya kullanıcılarının internet güvenliği ve çevrimiçi gizlilik ile ilgili kanaatleri ve farkındalıkları üzerine bir araştırma*, Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara.
17. Perreault, L. (2015). *Big data and privacy: Control and awareness aspects*. CONFIRM.
18. Alemany, J., del Val, E., Alberola, J., García-Fornes, A. (2019). Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms. *International Journal of Human-Computer Studies*, 129, 27-40.
19. Chen, T., Kaafar, M. A., Boreli, R. (2013). The where and when of finding new friends: Analysis of a location-based social discovery network. *Proceedings of the 7th International Conference on Weblogs and Social Media, ICWSM 2013*, 61-70.
20. Zhang, C., Sun, J., Zhu, X., Fang, Y. (2010). Privacy and security for online social networks: challenges and opportunities. *IEEE Network*, 24 (4), 13-18.
21. Çalıcı, C., İşcan, Y. (2011). *Sosyal ağlarda suç farkındalığı: Facebook örneği*, Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul.
22. Mester, Y., Yolum, P. (2015). *Negotiating privacy constraints in online social networks*, Yüksek Lisans Tezi, Boğaziçi Üniversitesi, İstanbul.
23. Nasirov, N., Albayrak, S. (2015). *Lokasyon bazlı sosyal ağlarda insan hareketliliğinin modellenmesi*, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, İstanbul.
24. Ateş, Ü., Temizel, T. T. (2014). *Inference of personality using social media profiles*, Yüksek Lisans Tezi, Ortadoğu Teknik Üniversitesi, Ankara.
25. Abubaker, F. R., Bölük, P. S. (2016). *An intelligent model for vulnerability analysis of social media user*, Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, İstanbul.
26. Çetinkal, Y., Şahin, S. (2016). *Matching of social media accounts by using public information*, Yüksek Lisans Tezi, İzmir Teknoloji Üniversitesi, İzmir.
27. Kaplan, İ., Yüksel, H. A. (2017). *Üniversite öğrencisi sosyal medya kullanıcılarının mahremiyet algısı*, Yüksek Lisans Tezi, Anadolu Üniversitesi, Eskişehir.
28. Hekimoğlu, H., Akgül, M. (2019). *Sosyal ağlarda mahremiyetin dönüşümü: Instagram örneği*, Yüksek Lisans Tezi, Erciyes Üniversitesi, Kayseri.
29. Günay, A., Çarıkçı, İ. H. (2019). *Sosyal medya kişilik özelliklerini yansıtır mı? İnsan kaynakları perspektifinde Twitter üzerinden bir söylem analizi*, Doktora Tezi, Süleyman Demirel Üniversitesi, Isparta.

30. Tataroğlu, V., Tokat, S. (2019). *Derin öğrenmeye dayalı sosyal medya profillemesi*, Yüksek Lisans Tezi, Pamukkale Üniversitesi, Denizli.
31. Krämer, N. C., Schäwel, J. (2020). Mastering the challenge of balancing self-disclosure and privacy in social media. *Current Opinion in Psychology*, 31, 67-71.
32. Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L. F., Agarwal, Y. (2015). Your location has been shared 5,398 times! A field study on mobile app privacy nudging. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. Association for Computing Machinery, 787–796.
33. Sari, P. K., Prasetyo, A. (2017). *Knowledge sharing and electronic word of mouth to promote information security awareness in social network site*. 2017 International Workshop on Big Data and Information Security (IWBIS).
34. Tiganoaia, B., Cernian, A., Niculescu, A. (2017). *The use of social platforms and personal data protection — An exploratory study*. 2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet).
35. Semiz Türkoğlu, H. (2018). Sosyal medya üzerinden mahremiyet farkındalığı ve değişimin ölçülmesine yönelik bir araştırma. *Connectist: İstanbul University Journal of Communication Sciences (Online)*, 1 (54), 163-189.
36. Bang, C. C., Lee, J., Rao, H. R. (2021). The Egyptian protest movement in the twittersphere: An investigation of dual sentiment pathways of communication. *International Journal of Information Management*, 58.
37. Flesch, B., Vatrappu, R., Mukkamala, R. R. (2017). *A big social media data study of the 2017 German Federal Election based on social set analysis of political party Facebook pages with SoSeVi*. IEEE International Conference on Big Data (IEEE Big Data), Boston, MA.
38. Ch'ng, E., Chen, Z. Y., See, S. (2017). *Real-time GPU-accelerated social media sentiment processing and visualization*. 21st IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications (DS-RT), Rome, Italy.
39. Raj, J. A. S., Fernando, J. L., Raj, Y. S. (2017). *Predictive Analytics on Facebook Data*. 2017 World Congress on Computing and Communication Technologies (WCCCT).
40. Wong, F. M. F., Tan, C. W., Sen, S., Chiang, M. (2016). Quantifying political leaning from tweets, retweets, and retweeters. *IEEE Transactions on Knowledge and Data Engineering*, 28 (8), 2158-2172.
41. Boulianne, S. (2015). Social media use and participation: A meta-analysis of current research. *Information, Communication & Society*, 18 (5), 524-538.
42. Kourtiti, K., Nijkamp, P., Östh, J. (2021). My home is my castle – Assessment of city love in Sweden. *International Journal of Information Management*, 58, 102213.

43. Zhang, S., Zhou, W. Q. (2018). Recreational visits to urban parks and factors affecting park visits: Evidence from geotagged social media data. *Landscape and Urban Planning*, 180, 27-35.
44. Stanojevic, M., Alshehri, J., Obradovic, Z. (2019). *Surveying public opinion using label prediction on social media data*. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Vancouver, Canada.
45. Li, Z. L., Li, X. M., Porter, D., Zhang, J. J., Jiang, Y. Q., Olatosi, B., Weissman, S. (2020). Monitoring the spatial spread of COVID-19 and effectiveness of control measures through human movement data: Proposal for a predictive model using big data analytics. *Jmir Research Protocols*, 9 (12), 10.
46. Eichstaedt, J. C., Smith, R. J., Merchant, R. M., Ungar, L. H., Crutchley, P., Preotiuc-Pietro, D., Asch, D. A., Schwartz, H. A. (2018). Facebook language predicts depression in medical records. *Proceedings of the National Academy of Sciences of the United States of America*, 115 (44), 11203-11208.
47. Thorstad, R., Wolff, P. (2019). Predicting future mental illness from social media: A big-data approach. *Behavior Research Methods*, 51 (4), 1586-1600.
48. Alkouz, B., Aghbari, Z. A., Abawajy, J. H. (2019). Tweetluenza: Predicting flu trends from Twitter data. *Big Data Mining and Analytics*, 2 (4), 273-287.
49. Moise, I. (2016). *The Technical Hashtag in Twitter Data: a Hadoop experience*. 4th IEEE International Conference on Big Data, Washington, DC.
50. Khatua, A., Khatua, A., Cambria, E. (2019). A tale of two epidemics: Contextual Word2Vec for classifying twitter streams during outbreaks. *Information Processing & Management*, 56 (1), 247-257.
51. Giglio, S., Bertacchini, F., Bilotta, E., Pantano, P. (2019). Using social media to identify tourism attractiveness in six Italian cities. *Tourism Management*, 72, 306-312.
52. Jaidka, K., Giorgi, S., Schwartz, H. A., Kern, M. L., Ungar, L. H., Eichstaedt, J. C. (2020). Estimating geographic subjective well-being from Twitter: A comparison of dictionary and data-driven language methods. *Proceedings of the National Academy of Sciences of the United States of America*, 117 (19), 10165-10171.
53. Salas-Olmedo, M. H., Moya-Gómez, B., García-Palomares, J. C., Gutiérrez, J. (2018). Tourists' digital footprint in cities: Comparing big data sources. *Tourism Management*, 66, 13-25.
54. Miah, S. J., Vu, H. Q., Gammack, J., McGrath, M. (2017). A big data analytics method for tourist behaviour analysis. *Information & Management*, 54 (6), 771-785.
55. Li, Z. M., Zhang, Q., Du, X. Y., Ma, Y. F., Wang, S. H. (2021). Social media rumor refutation effectiveness: Evaluation, modelling and enhancement. *Information Processing & Management*, 58 (1), 102420.
56. O'Halloran, K. L., Pal, G., Jin, M. (2021). Multimodal approach to analysing big social and news media data. *Discourse, Context & Media*, 40, 100467.

57. Harrigan, P., Daly, T. M., Coussement, K., Lee, J. A., Soutar, G. N., Evers, U. (2021). Identifying influencers on social media. *International Journal of Information Management*, 56, 102246.
58. Amato, F., Moscato, V., Picariello, A., Piccialli, F. (2019). SOS: A multimedia recommender system for online social networks. *Future Generation Computer Systems*, 93, 914-923.
59. Nallaperuma, D., Nawaratne, R., Bandaragoda, T., Adikari, A., Nguyen, S., Kempitiya, T., Silva, D. D., Alahakoon, D., Pothuhera, D. (2019). Online incremental machine learning platform for big data-driven smart traffic management. *IEEE Transactions on Intelligent Transportation Systems*, 20 (12), 4679-4690.
60. Dingli, A., Engerer, B. (2019). *Big social data - Predicting users' interests from their social networking activities*. International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), Univ Oxford, Dept Comp Sci, Oxford, England.
61. Zhang, Y. H., Mao, W. J., Lin, J. J. (2017). *Modeling topic evolution in social media short texts*. IEEE International Conference on Big Knowledge (IEEE ICBK), Hefei, Peoples R China.
62. Egebjerg, N. H., Hedegaard, N., Kuem, G., Mukkamala, R. R., Vatrappu, R. (2017). *Big social data analytics in football: Predicting spectators and TV ratings from Facebook data*. IEEE 6th International Congress on Big Data (BigData Congress), Honolulu, HI.
63. Barnaghi, P., Ghaffari, P., Breslin, J. G. (2016). *Opinion mining and sentiment polarity on Twitter and correlation between events and sentiment*. 2016 IEEE Second International Conference on Big Data Computing Service and Applications (BigDataService).
64. Minanovic, A., Gabelica, H., Krstic, Z. (2014). *Big data and sentiment analysis using KNIME: Online reviews vs. social media*. 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).
65. Iftikhar, R., Khan, M. S. (2020). Social media big data analytics for demand forecasting: Development and case implementation of an innovative framework. *Journal of Global Information Management*, 28 (1), 103-120.
66. Shirdastian, H., Laroche, M., Richard, M. O. (2019). Using big data analytics to study brand authenticity sentiments: The case of Starbucks on Twitter. *International Journal of Information Management*, 48, 291-307.
67. Li, B., Chan, K. C. C., Ou, C., Ruifeng, S. (2017). Discovering public sentiment in social media for predicting stock movement of publicly listed companies. *Information Systems*, 69, 81-92.
68. Liu, P., Teng, F. (2019). Probabilistic linguistic TODIM method for selecting products through online product reviews. *Information Sciences*, 485, 441-455.

69. Sternberg, F., Pedersen, K. H., Ryelund, N. K., Mukkamala, R. R., Vatrappu, R. (2018). *Analyzing customer engagement of Turkish Airlines using big social data*. IEEE International Congress on Big Data (IEEE BigData) Part of the IEEE World Congress on Services, San Francisco, CA.
70. Kumar, M., Bala, A. (2016). *Analyzing Twitter sentiments through big data*. 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India.
71. Lassen, N. B., Madsen, R., Vatrappu, R. (2014). *Predicting iPhone sales from iPhone tweets*. 18th IEEE International Enterprise Distributed Object Computing Conference (EDOC), Ulm Univ, Ulm, Germany.
72. Shah, S. A., Seker, D. Z., Rathore, M. M., Hameed, S., Ben Yahia, S., Draheim, D. (2019). Towards disaster resilient smart cities: Can internet of things and big data analytics be the game changers? *IEEE Access*, 7, 91885-91903.
73. Kankanamge, N., Yigitcanlar, T., Goonetilleke, A., Kamruzzaman, M. (2020). Determining disaster severity through social media analysis: Testing the methodology with South East Queensland Flood tweets. *International Journal of Disaster Risk Reduction*, 42, 101360.
74. Xu, Z., Liu, Y. H., Yen, N. Y., Mei, L., Luo, X. F., Wei, X., Hu, C. P. (2020). Crowdsourcing based description of urban emergency events using social media big data. *IEEE Transactions on Cloud Computing*, 8 (2), 387-397.
75. Wu, X., Cao, Y., Xiao, Y., Guo, J. (2020). Finding of urban rainstorm and waterlogging disasters based on microblogging data and the location-routing problem model of urban emergency logistics. *Annals of Operations Research*, 290 (1), 865-896.
76. Ragini, J. R., Anand, P. M. R., Bhaskar, V. (2018). Big data analytics for disaster response and recovery through sentiment analysis. *International Journal of Information Management*, 42, 13-24.
77. Negara, E. S., Andryani, R., Erlansyah, D., Syaputra, R. (2020). Analysis of Indonesian motorcycle gang with social network approach. *International Journal of Advanced Computer Science and Applications*, 11 (12), 193-198.
78. Alhalabi, W., Jussila, J., Jambi, K., Visvizi, A., Qureshi, H., Lytras, M., Malibari, A., Adham, R. S. (2021). Social mining for terroristic behavior detection through Arabic tweets characterization. *Future Generation Computer Systems*, 116, 132-144.
79. Williams, M. L., Burnap, P., Javed, A., Liu, H., Ozalp, S. (2020). Hate in the machine: Anti-black and anti-muslim social media posts as predictors of offline racially and religiously aggravated crime. *British Journal of Criminology*, 60 (1), 93-117.
80. Camargo, J. E., Torres, C. A., Martínez, O. H., Gómez, F. A. (2016). *A big data analytics system to analyze citizens' perception of security*. 2016 IEEE International Smart Cities Conference (ISC2).

81. Xu, Q., Cai, M., Mackey, T. K. (2020). The illegal wildlife digital market: an analysis of Chinese wildlife marketing and sale on Facebook. *Environmental Conservation*, 47 (3), 206-212.
82. Alipour, J. V., Fadinger, H., Schymik, J. (2021). My home is my castle - The benefits of working from home during a pandemic crisis. *Journal of Public Economics*, 196.
83. Sun, Y., Shao, Y. W., Chan, E. H. W. (2020). Co-visitation network in tourism-driven peri-urban area based on social media analytics: A case study in Shenzhen, China. *Landscape and Urban Planning*, 204, 103934.
84. Chen, H., Zhu, Z., Qi, F., Ye, Y., Liu, Z., Sun, M., Jin, J. (2020). Country image in COVID-19 Pandemic: A Case Study of China. *IEEE Transactions on Big Data*, 7, 81-92.
85. Gunter, U., Onder, I., Gindl, S. (2019). Exploring the predictive ability of likes of posts on the Facebook pages of four major city DMOs in Austria. *Tourism Economics*, 25 (3), 375-401.
86. Geissinger, A., Laurell, C., Sandstrom, C. (2020). Digital Disruption beyond Uber and Airbnb-Tracking the long tail of the sharing economy. *Technological Forecasting and Social Change*, 155, 119323.
87. Cerchiello, P., Giudici, P., Nicola, G. (2017). Twitter data models for bank risk contagion. *Neurocomputing*, 264, 50-56.
88. Punel, A., Ermagun, A. (2018). Using Twitter network to detect market segments in the airline industry. *Journal of Air Transport Management*, 73, 67-76.
89. Martin-Domingo, L., Martín, J. C., Mandsberg, G. (2019). Social media as a resource for sentiment analysis of Airport Service Quality (ASQ). *Journal of Air Transport Management*, 78, 106-115.
90. Amirmokhtar Radi, S., Shokouhyar, S. (2021). Toward consumer perception of cellphones sustainability: A social media analytics. *Sustainable Production and Consumption*, 25, 217-233.
91. Ducange, P., Pecori, R., Mezzina, P. (2018). A glimpse on big data analytics in the framework of marketing strategies. *Soft Computing*, 22 (1), 325-342.
92. Amalina, F., Hashem, I. A. T., Azizul, Z. H., Fong, A. T., Firdaus, A., Imran, M., Anuar, N. B. (2020). Blending big data analytics: Review on challenges and a recent study. *IEEE Access*, 8, 3629-3645.
93. Ghani, N. A., Hamid, S., Hashem, I. A. T., Ahmed, E. (2019). Social media big data analytics: A survey. *Computers in Human Behavior*, 101, 417-428.
94. Schneider, D., Seelmeyer, U. (2019). Challenges in using big data to develop decision support systems for social work in Germany. *Journal of Technology in Human Services*, 37 (2-3), 113-128.

95. Mavriki, P., Karyda, M. (2020). Automated data-driven profiling: Threats for group privacy. *Information and Computer Security*, 28 (2), 183-197.
96. Abkenar, S. B., Kashani, M. H., Mahdipour, E., Jameii, S. M. (2021). Big data analytics meets social media: A systematic review of techniques, open issues, and future directions. *Telematics and Informatics*, 57, 101517.
97. Phua, J., Jin, S. V., Kim, J. (2017). Gratifications of using Facebook, Twitter, Instagram, or Snapchat to follow brands: The moderating effect of social comparison, trust, tie strength, and network homophily on brand identification, brand engagement, brand commitment, and membership intention. *Telematics and Informatics*, 34 (1), 412-424.
98. Vatrappu, R., Mukkamala, R. R., Hussain, A., Flesch, B. (2016). Social set analysis: A set theoretical approach to big data analytics. *IEEE Access*, 4, 2542-2571.
99. Shayaa, S., Jaafar, N. I., Bahri, S., Sulaiman, A., Wai, P. S., Chung, Y. W., Piprani, A. Z., Al-Garadi, M. A. (2018). Sentiment analysis of big data: Methods, applications, and open challenges. *IEEE Access*, 6, 37807-37827.
100. Komalavalli, C., Laroia, C. (2019). *Challenges in big data analytics techniques: A survey*. 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence).
101. Taleb, I., Serhani, M. A., Dssouli, R. (2018). *Big data quality: A survey*. 2018 IEEE International Congress on Big Data (BigData Congress).
102. Karajeh, O., Darweesh, D., Darwish, O., Abu-El-Rub, N., Alsinglawi, B., Alsaedi, N. (2021). A classifier to detect informational vs. non-Informational heart attack tweets. *Future Internet*, 13 (1), 1-10.
103. Tesfay, W. B., Serna, J., Rannenber, K. (2019). *PrivacyBot: Detecting privacy sensitive information in unstructured Texts*. 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS).
104. Saniei, R., Doncel, V. (2022). PHDD: Corpus of physical health data disclosure on Twitter during COVID-19 pandemic. *SN Computer Science*, 3 (3), 212.
105. Makita, M., Mas-Bleda, A., Morris, G., Thelwall, M. (2020). Mental health discourses on Twitter during Mental Health Awareness Week. *Issues in Mental Health Nursing*, 42 (5), 437-450.
106. Al-Fedaghi, S., Al-Azmi, A. (2012). Experimentation with personal identifiable information. *Intelligent Information Management*, 4, 123-133.
107. İnternet: Kişisel Verilerin Korunması Kanunu. URL: <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf>, Son Erişim Tarihi: 01.05.2022.
108. İnternet: GDPR Chapter 2 (Art. 5-11). URL: <https://gdpr.eu/tag/chapter-2/>, Son Erişim Tarihi: 01.05.2022.

109. Yin, Z., Fabbri, D., Rosenbloom, S. T., Malin, B. A. (2015). A scalable framework to detect personal health mentions on Twitter. *Journal of Medical Internet Research*, 17 (6), e138.
110. İnternet: Kişisel Verilerin Korunması Kanunu'na ilişkin uygulama rehberi. (2019). URL: <https://www.kvkk.gov.tr/Icerik/4197/Kisisel-Verilerin-Korunmasi-Kanununa-Iliskin-Uygulama-Rehberi>, Son Erişim Tarihi: 01.05.2022.
111. Geetha, R., Karthika, S., Kumaraguru, P. (2021). Tweet-scan-post: A system for analysis of sensitive private data disclosure in online social media. *Knowl. Inf. Syst.*, 63 (9), 2365–2404.
112. Geetha, R., Karthika, S., Pavithra, N., Preethi, V. (2019). Tweedle: Sensitivity check in health-related social short texts based on Regret Theory. *Procedia Comput. Sci.*, 165 (C), 663–675.
113. Karisani, P., Agichtein, E. (2018). *Did you really just have a heart attack? Towards robust detection of personal health mentions in social media*. Proceedings of the 2018 World Wide Web Conference, Lyon, France.
114. Syarif, I., Ningtias, N., Badriyah, T. (2019). *Study on mental disorder detection via social media mining*. 2019 4th International Conference on Computing, Communications and Security (ICCCS).
115. Küçükali, H., Ataç, Ö., Palteki, A. S., Tokaç, A. Z., Hayran, O. (2022). Vaccine hesitancy and anti-vaccination attitudes during the start of COVID-19 vaccination program: A content analysis on Twitter data. *Vaccines*, 10 (2), 161.
116. Tankut, Ü., Esen, M. F., Balaban, G. (2021). Analysis of tweets regarding psychological disorders before and during the COVID-19 pandemic: The case of Turkey. *Digital Scholarship in the Humanities*.
117. Wissler, L., Almasraee, M., Monett, D., Paschke, A. (2014). *The Gold Standard in corpus annotation*.
118. Tomanek, K., Wermter, J., Hahn, U. (2007). *An Approach to text corpus construction which cuts annotation costs and maintains reusability of annotated data*. EMNLP.
119. Snow, R., O'Connor, B., Jurafsky, D., Ng, A. Y. (2008). *Cheap and fast---but is it good? evaluating non-expert annotations for natural language tasks*. Proceedings of the Conference on Empirical Methods in Natural Language Processing, Honolulu, Hawaii.
120. Alqaraleh, S., Isik, F. M. (2020). Efficient Turkish tweet classification system for crisis response. *Turkish J. Electr. Eng. Comput. Sci.*, 28 (6).
121. İnternet: Zemberek-NLP. URL: <https://github.com/ahmetaa/zemberek-nlp>, Son Erişim Tarihi: 01.05.2022.
122. Camargo, J. E., Torres, C. A., Martinez, O. H., Gomez, F. A. (2016). *A big data analytics system to analyze citizens' perception of security*. 2nd IEEE International Smart Cities Conference (ISC2), Trento, Italy.

123. Elsayed, M., Abdelwahab, A., Ahdelkader, H. (2019). *A Proposed framework for improving analysis of big unstructured data in social media*. 2019 14th International Conference on Computer Engineering and Systems (ICCES).
124. Bhardwaj, P. (2019). Types of sampling in research. *Journal of the Practice of Cardiovascular Sciences*, 5 (3), 157-163.
125. İnternet: Stratified sampling in machine learning. (2019). URL: <https://www.baeldung.com/cs/ml-stratified-sampling>, Son Erişim Tarihi: 23.12.2021.
126. İnternet: Scikit-learn machine learning in Python. URL: <https://scikit-learn.org/stable/>, Son Erişim Tarihi: 01.05.2022.
127. Kawade, D., Oza, K. (2016). News classification: A data mining approach. *Indian Journal of Science and Technology*, 9 (46), 1-6.
128. Shinde, P. P., Oza, K. S., Kamat, R. K. (2017, 10-11 Feb. 2017). *Big data predictive analysis: Using R analytical tool*. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC).
129. Joulin, A., Grave, E., Bojanowski, P., Mikolov, T. (2017). *Bag of tricks for efficient text classification*. Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics.
130. Mikolov, T., Sutskever, I., Chen, K., Corrado, G., Dean, J. (2013). *Distributed representations of words and phrases and their compositionality*. Proceedings of the 26th International Conference on Neural Information Processing Systems, 2, Lake Tahoe, Nevada.
131. Mikolov, T., Chen, K., Corrado, G. S., Dean, J. (2013). Efficient estimation of word representations in vector space. *Proceedings of Workshop at ICLR*.
132. Velioglu, R., Yıldız, T., Yıldırım, S. (2018). *Sentiment analysis using learning approaches over emojis for Turkish tweets*. 2018 3rd International Conference on Computer Science and Engineering (UBMK).
133. İnternet: FastText library for efficient text classification and representation learning. URL: <https://fasttext.cc/>, Son Erişim Tarihi: 22.05.2022.
134. Bojanowski, P., Grave, E., Joulin, A., Mikolov, T. (2017). Enriching word vectors with subword information. *Transactions of the Association for Computational Linguistics*, 5, 135-146.
135. Zhou, T., Wang, Y., Zheng, X. (2020). *Chinese text classification method using FastText and Term Frequency-Inverse Document Frequency optimization*. Journal of Physics: Conference Series.
136. Wang, Z., Ji, S. (2017). *Learning convolutional text representations for visual question answering*. Proceedings of the 2018 SIAM International Conference on Data Mining (SDM).

137. Nergiz, G., Safali, Y., Avaroğlu, E., Erdoğan, S. (2019). *Classification of Turkish news content by deep learning based LSTM using Fasttext model*. 2019 International Artificial Intelligence and Data Processing Symposium (IDAP).
138. Kuyumcu, B., Aksakalli, C., Delil, S. (2019). *An automated new approach in fast text classification (fastText): A case study for Turkish text classification without pre-processing*. Proceedings of the 2019 3rd International Conference on Natural Language Processing and Information Retrieval, Tokushima, Japan.
139. Çelik, Ö., Koç, B. (2021). Classification of Turkish news text by TF-IDF, Word2vec and Fasttext vector model methods. *Deu Muhendislik Fakultesi Fen ve Muhendislik*, 23, 121-127.
140. Erdinç, H. Y., Güran, A. (2019). *Semi-supervised Turkish text categorization with Word2Vec, Doc2Vec and FastText algorithms*. 2019 27th Signal Processing and Communications Applications Conference (SIU).
141. İnternet: Makine öğrenmesi ipuçları ve püf noktaları el kitabı. URL: <https://stanford.edu/~shervine/l/tr/teaching/cs-229/cheatsheet-machine-learning-tips-and-tricks>, Son Erişim Tarihi: 01.05.2022.
142. İnternet: Yasser, A. Twitter Clone. URL: <https://github.com/aminyasser/twitter-clone/blob/master/home.php>, Son Erişim Tarihi: 01.05.2022.
143. Devlin, J., Chang, M. W., Lee, K., Toutanova, K. (2019). *BERT: Pre-training of deep bidirectional transformers for language understanding*.
144. Alammary, A. S. (2022). BERT models for Arabic text classification: A systematic review. *Applied Sciences*, 12 (11), 5720.
145. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A., Kaiser, L., Polosukhin, I. (2017). *Attention is all you need*. Proceedings of the 31st Annual Conference on Neural Information Processing Systems.
146. Mohammadi, S., Chapon, M. (2020). *Investigating the performance of fine-tuned text classification models based-on BERT*. 2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS).
147. Çelikten, A., Bulut, H. (2021). *Turkish medical text classification using BERT*. 2021 29th Signal Processing and Communications Applications Conference (SIU).
148. İnternet: Bert-Base-Turkish-Uncased URL: <https://huggingface.co/loodos/bert-base-turkish-uncased>, Son Erişim Tarihi: 22.05.2022.
149. İnternet: Bert-Base-Turkish-128k-Cased. URL: <https://huggingface.co/dbmdz/bert-base-turkish-128k-cased>, Son Erişim Tarihi: 22.05.2022.
150. İnternet: Convbert-Base-Turkish-Cased. URL: <https://huggingface.co/dbmdz/convbert-base-turkish-cased>, Son Erişim Tarihi: 22.05.2022.

151. Tommasel, A., Godoy, D. (2019). Short-text learning in social media: a review. *The Knowledge Engineering Review*, 34, e7.
152. Onan, A., Korukoğlu, S. (2016). A review of literature on the use of machine learning methods for opinion mining. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 22 (2), 111-122.
153. Kaddoura, S., Chandrasekaran, G., Popescu, D., Duraisamy, J. (2022). A systematic literature review on spam content detection and classification. *PeerJ Computer Science*, 8, e830.
154. İnternet: McCormik, C. Word2Vec Tutorial - The Skip-Gram Model. URL: <http://mccormickml.com/2016/04/19/word2vec-tutorial-the-skip-gram-model/>, Son Erişim Tarihi: 22.05.2022.





GAZİLİ OLMAK AYRICALIKTIR..