Management and Political Sciences Review
Volume: 2 Issue: 2 Year: 2019 pp: 75-95

ULUSAL GÜVENLİK VE SOSYAL MEDYA: FIRSATLAR VE TEHDİTLER[1]

Arş. Gör. Ahmet KURNAZ[2], Arş. Gör. İsmail KAYAR[3],
Arş. Gör. Mustafa GÜNGÖR[4], Prof. Dr. Mustafa GÖRÜN[5]

ÖZET

Akıllı telefonun icat edilmesinden sonra kişisel verilerin paylaşılmasıyla sanal ortamda üretilen veri çok büyük boyutlara ulaşmıştır. Twitter, Facebook ve Youtube gibi uygulamalar aracıları ortadan kaldırarak vatandaşların seslerini daha kolay duyurmasına yardımcı olmakta ve kitlelerin hareketlendirilmesini sağlayarak siyasal katılımı artırmaktadır. Ayrıca bu uygulamalar kriz durumlarına acil müdahalede, kamu politikası süreçlerinde taleplerin duyurulmasında ve kurumların kamuoyu gözündeki imajlarının iyileştirmelerinde kullanılmaktadırlar. Buna karşın sosyal medya üzerinden yapılan bilgi savaşları ulusal güvenliği ve istikrarı etkileyecek son derece önemli sonuçlara yol açmaktadır. Sosyal medya uygulamalarının kamu yönetimine faydaları ve tehditleri gün geçtikçe artmaktadır. Kamu bürokrasisinin geleneksel dikey yapılanmasıyla çelişkili de olsa resmî kurumların sosyal medya stratejisine sahip olması fırsatları değerlendirmek ve tehditlerin farkına varıp onlardan kaçınmak için önemlidir.

Bu çalışmada öncelikle kamu yönetiminde büyük veri madenciliği, öğrenen makineler ve sosyal medyayla ilgili temel kavramlar açıklanmıştır. Kamu yönetiminde sosyal medya araçlarının ve bu platformlar üzerinden üretilen verinin kullanımına ilişkin tehditler, bu araçların ve verinin getirdiği fırsatlar incelenmiştir. Bu amaçla Emniyet Genel Müdürlüğü'ne ait resmi Twitter hesabı incelenmiştir. Veriler Twitter Public API üzerinden R programlama dili kullanılarak derlenmiştir. Verilerin çözümlenmesinde R programlama dilinden yararlanılmıştır. Çözümlemeler sonucunda ulusal güvenliğin ve istikrarın sağlanması için alınabilecek önlemler hakkında önerilerde bulunulmuştur.

1- Bu çalışma, 17-20 Nisan 2019 tarihleri arasında Gaziantep'te düzenlenen KAYSEM13'te özet bildiri olarak sunulmuştur.

2- Çanakkale Onsekiz Mart Üniversitesi Siyasal Bilgiler Fakültesi, SBKY Bölümü, ahmetkurnaz@comu.edu.tr, Orcid No: 0000-0001-5628-328X

3- Çanakkale Onsekiz Mart Üniversitesi Siyasal Bilgiler Fakültesi, SBKY Bölümü, ismailkayar@comu.edu.tr, Orcid No: 0000-0001-9732-6979

4- Çanakkale Onsekiz Mart Üniversitesi Siyasal Bilgile rFakültesi, SBKY Bölümü, mgungor@comu.edu.tr, Orcid No: 0000-0002-8502-8103

5- Çanakkale Onsekiz Mart Üniversitesi Siyasal Bilgiler Fakültesi, SBKY Bölümü, mgorun@comu.edu.tr, Orcid No: 0000-0001-9732-6979

Anahtar Kelimeler: Sosyal Medya, Güvenlik, Twitter, Sosyal Ağ
JEL Kodları: H56, C80.

NATIONAL SECURITY AND SOCIAL MEDIA: OPPORTUNITIES AND THREATS

ABSTRACT

The amount of online data grew dramatically only after the invention of smartphones. social media platforms, such as Facebook, Twitter and Youtube, eliminate all other communication means for citizens to voice their inclinations and expand political participation by mobilising the public. Besides, these applications not only help the government to take necessary measures in emergencies but also to polish their public images. In addition to government, these platforms empower citizens by disseminating their demands, so they are included in public policy processes. On the other hand, information warfare via social media stands as a significant peril to national security and stability. As a result, the opportunities and threats created by social media for public administration are gradually raising. Although it is contradictory to the traditional public bureaucracy organisation, possessing a social media strategy is vital to utilise the opportunities and evade the threats.

In this study, firstly, essential concepts of big data mining, machine learning and social media in public administration are defined. Secondly, the threats and the opportunities created by social media and citizens' personal data on these platforms are discussed. To exemplify the discussion Turkish Security General Directorate Twitter account is selected as the sample. The data scraped and analysed by using the R programming language and Twitter Public API. possible precautions to establish national security and stability are discussed.

Keywords: Socialmedia, Security, Twitter, Social Network
JEL Codes: H56, C80.

1. GİRİŞ

Güvenlik kavramı tarihin farklı dönemlerinde toplumsal, siyasal, ekonomik ve teknolojik gelişmelere bağlı olarak farklı anlamlandırılan, algılanan ve tanımlanan bir kavramdır (Torun, 2012). Bu kavram insanlığın ilk dönemlerinde dış tehditlerden korunmak amacıyla basit yollarla gerçekleştirilirken daha sonraki süreçte özellikle yerleşik hayata geçilmesi, sosyal hayatın başlaması,

teknolojideki ilerlemeler ve savaşlarla değişik anlamlar kazanmıştır (Bakan ve Şahin, 2018).

Güvenlik kavramı, öncelerde geleneksel olarak sadece askeri ve savaş ile ilgili konuları kapsayan bir kavram sayılırken günümüzde insanların tüm hayatına girmiştir. Toplumların hayatında yaşanan değişim ve dönüşümler ile meydana gelen tehlikeler ve ihtiyaçlar güvenlik kavramının sürekli yenilenmesini, güncellenmesini gerekli kılmaktadır (Tirab, 2017). Bu kapsamda Soğuk Savaş'ın bitmesiyle birlikte önemi artan güvenlik boyutlarından biri de siber güvenliktir.

Teknolojinin hızla gelişmesi insanlara bir yandan önemli kolaylıklar sağlarken, diğer yandan da bir dizi tehditler oluşturmaktadır. Bu tehditler ulusal kritik altyapıya, ekonomiye ve ulusal güvenliğe ciddi zararlar verebilecek kabiliyetlere sahiptir. Siber saldırıların geleneksel şekli olarak tehditler virüs, truva atı, hizmet dışı bırakma, aldatma, mahremiyet ve gizlilik ihlali, yetkisiz giriş, yemleme, spam sayılabilir (Yılmaz ve Salcan, 2008). Bunların yanı sıra kişisel veriler biyolojik, ekonomik ve siyasal boyutlarıyla günümüzde bir ulusal güvenlik sorunu haline gelmiştir.

Üretilen verinin artması yapay zekâ gelişimini sanayi devriminden daha önemli bir sosyal dönüşüm haline getirmiştir. Günümüzde en fazla veri üretilen alan sosyal medya platformlarıdır. Sosyal medya yarattığı fırsat ve tehditlerle günlük yaşamın önemli bir parçası haline gelmiştir.

Sosyal medya siyasal eylemleri dönüştürmüştür. Beğenme (like), yeniden paylaşma (retweet) veya bahsetme (mention) gibi hareketlerin eski düzende bir karşılığı yoktur. 20 yıl önce siyasete katılmanın tek yolu bir siyasal partiye ya da derneğe üye olmaktan geçmekte iken; günümüzde bir cep telefonundan başka hiçbir kaynağa ihtiyaç duymadan insanlar siyasal etkileşimde bulunabilmektedirler. İnternet aktivizmi gibi küçük eylemler hükümetleri şoka sokabilecek sürpriz siyasal eylemlere neden olabilmektedir (Margetts, 2019).

Sosyal medyadan örgütlenen Arap Baharı benzeri toplumsal hareketler yerini seçimlerin sosyal medyayla manipüle edilmesine bırakmıştır. ABD'de 2016 başkanlık seçimlerine ve Birleşik Krallık'ta Brexit referandumuna Twitter ve Facebook gibi sosyal medya platformları kullanılarak müdahale edildiği ortaya çıkmıştır(Cadwalladr, 2017; Nielsen, 2018; Twitter Public Policy, 2017). Ayrıca Cambridge Analytica skandalının patlak vermesi veri etiği konusunda tartışmaları alevlendirmiş sonuçta Avrupa'da, internette kişisel verilerin korunması konusunda, geniş çaplı bir reform olan Genel Veri Koruma Düzenlemesinin (General Data Protection Regulation- GDPR) kabul edilmesine neden olmuştur

(European Commission, 2018).

Yukarıda ifade etmiş olduğumuz olaylar, milyarlarca insanı online olarak birbirine bağlayan sosyal medyanın yarattığı tehditlerin gündeme gelebilmiş kısmıdır. Bu alanda çalışan bilgisayar ve sosyal bilimciler buzdağının görünmeyen kısmına dikkatlerini vermiş durumdalar. Gelecekte günlük ortalama bireyin gündelik yaşantısının merkezine girecek olan veri teknolojilerinin olası etkileri henüz bilinmemektedir. Kredi kartı hizmet sunucuları, medya merkezleri, sosyal medya platformları ve online mağaza devleri gibi şirketlerin insanların verilerini etik olmayan biçimlerde kullanıyor olmaları sosyal yaşama ilişkin büyük tehditler içermektedir.

Bu çalışmada öncelikle online olarak elde edilen verilerin sosyal medya araçları ile bireylere ve uluslara sağladığı faydalar ve yarattığı tehditler incelenmiştir. Çalışmanın ikinci kısmında online veri dinleme yoluyla vatandaşların güvenlik noktasında talep ve istekleri Twitter üzerinden nasıl dile getirildiği çözümlenmiştir. Çözümlemede öncelikle Türkiye Cumhuriyeti Emniyet Genel Müdürlüğü resmi Twitter hesabına gönderilen tweetlerin içerik analizi yapılmıştır. Daha sonra içerik analiziyle ortaya çıkartılan gruplarla eğitilen yapay zekâ ile ihbarların bilgisayar tarafından otomatik sınıflandırması yapılmıştır.

2. FIRSATLAR VE TEHDİTLER

İnsanoğlunun yüzyıllardır acı ve gözyaşı ile kazandığı sosyal ve siyasal hakları, kişisel verileri kullanılarak yapay zekâ algoritmaları aracılığıyla ellerinden alındığı araştırmacılar tarafından dile getirilmektedir. Vatandaşlar birey olmaktan bir veri noktası olmaya, insanlıktan bir laboratuvar deneğine dönüşme tehlikesiyle karşı karşıyadır. Sonuçta bütün insanlık, kötü niyetli istihbarat servislerinin ve teknoloji şirketlerinin kölesi olma tehlikesi ile karşı karşıyadır (Askonas, 2019). Buna ek olarak devletler de uluslararası doğa durumunun yarattığı asimetrik güç dengesi yüzünden daha güçlü devletlerin güdümüne girmeye zorlanmaktadır.

Fırsatlar ve tehditler bu bölümde değerlendirilirken öncelikle online ortamlarda üretilen verinin hangi biçimlerde kullanıldığına ilişkin açıklamalar yapılacaktır. Daha sonra verinin korunmasına yönelik Türkiye ve Avrupa'da yasal düzenlemeler kısaca değinilecektir. Ardından sosyal medya üzerinden terör olayları ile ulusal güvenliği tehdit edebilecek toplumsal hareketlerin yönlendirilmesine ilişkin incelemeler yapılacaktır.

a. Verinin Değeri

Sosyal medya verilerinin siyasal kullanımı pazarlamanın her alanında olduğu gibi işlevselleştirilmektedir. Yani bir ayakkabının veya politikacının pazarlanması aynı biçimlerde gerçekleşmektedir. Hedef kitlenin bu şekilde seçilmesindeki problem bunun ne kadar etik olduğudur. Sosyal medya verilerini kullanıcıların ürettiği içerikler, kullanıcı bilgileri ve sosyal ağ verisi olarak sınıflandırmak mümkündür. Kullanıcıların ürettiği veriler metin, fotoğraf veya video gibi farklı formatlarda olabilir. Kullanıcı verileri demografik bilgiler, tercihler ve konum bilgisi gibi kişisel bilgileri içerebilir. Sosyal ğ verisi ise ilk olarak kullanıcıların birbirleri arasında kurulan bağlantıların bilgisidir. Buna ek olarak beğenme, paylaşma, yorum yapma ve mesajlaşma gibi işlemler hem içerik üretmekte hem de ağ verisi üretmektedir.

b. Verinin Elde Edilmesi

Veriler, "şirketlerin günlük yaşamı gözetlemesi" ile gönüllülerden, gözlemlerden ve çıkarımlardan elde edilir. Google, Facebook ve Amazon gibi dijital platformlar, kredi kartı servisleri, bankalar ve medya tüketici verisinin en önemli satıcılarıdır. Örneğin Spotify, dinleyicilerinin şarkı dinleme alışkanlıklarının yanı sıra günlük duygu durumlarını da pazarlamaktadır (Beres, 2019; Christl, 2017).

Sosyal medyada verilerin elde edilmesi için iki temel yöntemden bahsedilebilir. Bunlardan ilki web sayfalarının doğrudan toplanmasıdır. Bu yönteme web-scraping denilmektedir. İkinci yöntem ise ise API (application user interfaces-kullanıcı uygulama arayüzü) kullanılarak verilerin toplanmasıdır. Bu yönteme ise dijital dinleme adı verilmektedir. İlk yöntemde veri toplayanlar herhangi bir şekilde sınırlandırılmazken ikinci yöntemde platform geliştiricinin koyduğu bir takım kurallar çerçevesinde veriler toplanabilir.

Dijital dinleme kişinin sosyal medyada yapmış olduğu hareketlerin üçüncü taraf tarafından derlenmesini anlatan bir kavramdır (Varga, 2018). Bunlar bir mesaj paylaşma, beğenme, yorum yapma, yeniden paylaşma (retweet etme), başlık (hashtag) veya bahsetme (mention) gibi araçlarla elde edilirler ve kişinin siyasi duygu durumunu, tutumunu, yaklaşımını, beklentilerini ve tarafını ortaya koymak için gelişmiş analizlerde kullanılırlar. Yeterli teknik beceriyle birlikte günümüzde muazzam miktarda veriyi toplayıp analiz edilebilmektedirler. NLP (natural language processing) adı verilen tekniklerle bu veriler yapay zekâ ile desteklediğinde zaman içerisinde daha fazla veri ile daha isabetli analiz yapar hale gelmektedirler.

Dijital dinleme, bireylerin gözlendiği hissini ortadan kaldırarak farklı davranma durumunu aşmaya yardımcı olup gerçek niyetleri/ihtiyaçları ortaya çıkarabilir. Kamu karar alıcılarının fark etmedikleri sorunların ortaya çıkmasına yardımcı bir araç olarak kullanılabilir. Buna karşın kişilerin gerçek kimlikleriyle ilişkilendirilerek yerel veya uluslararası istihbarat servisleri tarafından kötü amaçlarla bireyin özgürlüklerinin kısıtlanması veya devletin zayıflatılması amacıyla da kullanılabilir. Ayrıca otomatik içerik üretilerek önemsiz konuların önemli olarak yansıtılması tehlikesini de barındırır (Gilani vd., 2017; Ratkiewicz vd., 2011).

Yukarıda bahsedilen yöntemlere ek olarak mobil ve/ya yerleşik cihazlar üzerinden farklı tekniklerle kişisel verilere erişilmektedir. Mobil uygulamalar üzerinden kişilerin sağladıkları iletişim verilerinin yanı sıra sosyal medya adreslerini ve/veya seçmen tercihlerini kısa soru formları/anketler yoluyla elde edebilir. Örneğin, Cambridge Analytica, Facebook üzerinden benzeri bir uygulama geliştirerek milyonlarca insanın psikometrik profilini çıkartmıştır(Levin, 2018). Ayrıca kişilerin oy tercihlerini anket ve mini testlerle ortaya koyan pek çok platform mevcuttur (I Side With; Who Should You Vote For, 2017).

Psikomeetrik profil temelde beş büyük olarak adlandırılan açıklık (openness), insaflılık (conscientiousness), dışa dönüklük (extraversion), uyumluluk (agreeleness) ve nevrotiklik (neuroticism) duygu durumları ile insanları etiketlemektir. Alanyazında beş büyük (big five) İngilizce akrostiş olarak üretilen OCEAN kelimesiyle geçmektedir (Adrews, 2018).

Kurabiyeler (çerezler) aracılığıyla webde yapılan her hareket, gps verileri, ekran takibi, internet kapalıyken yapılan hareketler gibi pek çok yolla kişiler takip edilmektedirler. Kurabiyeler temelde uygun reklam içeriğinin web sitesinde gösterilmesi ve yanı sıra kişilerin kategorize edilmesi amacına da hizmet eder. En tehlikeli takip biçimi üçüncü parti kurabiye takibidir. Süper kurabiye ve parmak izi (web tarayıcınıza atanan tekil bir sayı) olmak üzere iki biçimde sürekli olarak internet kullanıcılarını gözetlerler (Bashyakarla, 2018; Mayer ve Mitchell, 2012). GDPR kurabiyeler için kullanıcının rızasını şart koşmuştur (Cookiebot, 2019; Wachter, 2018). Bu takibin etik olmayan kullanımını engellemek amacıyla çıkarılan yasalar etkisiz kalmaktadırlar. Çevrim içi platformla kullanıcıya kısaca veri toplamamıza izin veriyor musunuz şeklinde bir soru sorup eski düzenlerinde devam etmektedirler. Genellikle etik olmayan biçimlerde kullanılsalar bile kurabiye takibi bireyleri oy vermeye yönlendirerek demokrasinin güçlenmesine yardımcı olabilir (Cookie Central, 2019).

Dijital dinleme veya web scraping yöntemleri kullanılarak kişilerin konum verileri de elde edilmektedir. Böylece bireylerin alışveriş tercihlerini, egzersiz düzenlerini, iş yerlerini, gittiği sosyal mekânları ve daha pek çok şeyi açığa çıkaracak bir değişkedir. Böylece siyasi veya ekonomik casusluktan kürtaj karşıtı mesajların hedefi haline gelmeye kadar pek çok alanda kullanılabilirler.

Pek çok sosyal medya platformu meta verileri (yaş, cinsiyet, konum, tercihler vs.) kullanıcılarında istemektedir. Kullanıcıların bazıları bu bilgileri açıkça paylaşırken birçoğu bunları açıkça paylaşmamayı tercih etmektedirler. Bu gizli kalmış değişkenleri yapay zekâ algoritmalarıyla birlikte ortaya çıkartılabilmektedir. Kullanıcılara benzer hayat görüşü, beğenileri, paylaşımları olan diğer kişilerin verileri kullanılarak bir kişinin yaşı, konumu, cinsiyeti, siyasi eğilimi tahmin edilebilmektedir (Chen vd., 2015; Li vd., 2019; Liu vd., 2019; Nguyen vd., 2013; Rao ve Yarowsky, 2010; Sap vd., 2014; Wang vd., 2019; Zhang vd., 2016).

Bu şekilde açık kaynaklardan elde edilen veriler siyasal eğilimlerin tahmin edilmesinde kullanılabilmektedirler. Örneğin Stanford Üniversitesi yapay zeka araştırmacıları Google haritalar servisini kullanarak yerleşim yerindeki araç tiplerine göre seçimi kimin kazanacağını tahmin etmişlerdir (Gebru vd., 2017).

c. Verinin Kullanılması

Yukarıda açıklandığı şekilde elde edilen veriler siyasal pazarlama amaçlı tutumların ölçülmesi ve kamuoyunun yönlendirilmesi gibi iki temel motivasyonla kullanılmaktadır. Öncelikle tutumların ölçülmesi için temel değişkenler elde edildikten sonra A/B testi denilen uygulamalarla bireylerin tercihleri ortaya konulmaktadır. A/B testi; iki ya da daha fazla değişkenin tercih edilme oranlarını ölçen bir araçtır. Sosyal medyada paylaşılan içeriklere gelen yorum ve beğenilerle kişilerin siyasal eğilimleri yaşam tarzları veya ideolojileri hakkında veri elde edilebilir. Kişi bunlara oy vermese dahi ilgisizliği üzerinden veri derlenebilir (Christian, 2012; Hootsuite, 2017; Jiang vd., 2019; Segal, 2017).

İkinci olarak toplanan metinler üzerinde duygu analizi çeşitli kütüphaneler yardımıyla yapılabilmektedir. Bu kütüphanelerin başında LIWC gelmektedir ("LIWC | Linguistic Inquiry and Word Count", 2018). Uzmanlar tarafından oluşturulan bu kütüphanelerde yer alan hedeflenmiş anahtar kelimeler sosyal medyadan toplanan verilerde aratılarak içeriği üretenin duygu durumu, amacı, ideolojisi gibi veriler ortaya çıkarılmaktadır.

Kamuoyunun yönlendirilmesinde kullanılan yalan haber kavramı ya da daha geleneksel terimle ifade edilirse dezenformasyon sosyal medya tartışmalarının

merkezinde yer almaktadır. Günümüzde sosyal medya aracılığıyla sahte/yalan içerik bireyin ve toplumun gerçeklik algısını bozulmasına ilişkin, gerçeklik sonrası sosyal düzen ile ilgili araştırmalar yapılmaktadır (Corner, 2017). Bu dönemde artık doğru ve yanlış, gerçek ve yalan, teknolojik araçlarla insan beyni aldatılarak inşa edilir hale gelmiştir.

Sosyal medya kullanımı ile tembelleşen bireyler bilginin kaynağı hakkında araştırma yapmaz hale gelmiştir. Bilişsel psikologlar yalan habere inanmanın nedenleri üzerine yaptıkları çalışmalarda en büyük nedeni eleştirel tembellik olarak ortaya koymuşlardır (Pennycook ve Rand, 2019). Yalan içeriklerle mücadele etmenin henüz verimli bir çözümü bulunmuş değildir. Facebook, Twitter, Google ve YouTube gibi büyük platformlar her gün yeni bir çözüm önerisi ile birlikte gelseler de yalan haber üreten troller ve botlar daha sofistikehale gelmektedir (Condliffe, 2017; Google, 2019; Hern, 2019; Matney, 2019; Vanian, 2018; Whittaker, 2018).

Kamuoyunun yönlendirilmesinde otomatik içerik üreten botlar kullanılmaktadır. Bot olarak adlandırılan uygulamalar istenilen işlemlerin bilgisayar kodları tarafından otomatik olarak yapılmasını ifade etmektedir. Günümüzde yapay zekanın ulaştığı seviye botların gerçek kişileri ikna etmek için argüman üretmelerine imkan vermektedir. Bu botlar seçmeni ikna etmek için kullanılabileceği gibi aşırılıkçı grupları tahrik etmek veya toplumdan bu türde gruplar devşirmek için de kullanılabilirler.

d. Sosyal Medya ve Terör

Sosyal medya aşırı hareketler için mükemmel bir araç haline gelmiştir. Özellikle aşırı dinci ve aşırı sağ ırkçı gruplar, sosyal medyayı etkin biçimde kullanarak toplumları terörize etmektedirler. Sosyal medya propaganda aracı olmasının yanı sıra sınırlar ötesi benzer ideolojilere sahip grupların örgütlenmesi ve organize eylemlerde bulunmasına yardımcı olabilirler ve yalnız kurt denilen saldırı emirlerinin verilmesi amacıyla da kullanılabilmektedir (Froio ve Ganesh, 2018).

Sosyal medya, toplumların teröre ve nefret suçlarının normalleştirilmesine karşı örgütlenmesi açısından önemli bir işlevi de yerine getirmektedir. Renk, din ve kimlik farklılıklarına rağmen yaşanan trajedilere verilen ortak tepki nefretin daha fazla yayılmasına engel olmaktadır.

e. Sosyal Medya ve Toplumsal Hareketler

Toplumsal hareketler ve sosyal medya denilince akla ilk gelen dönem Arap coğrafyasında ortaya çıkan Arap Baharı fenomenidir. Toplumların, devletlerinin başındaki zorba liderlere karşı örgütlenmesi ve diktatörlere karşı kamuoyu yaratmaları sosyal medya aracılığı ile gerçekleşmiştir. Buna karşın sosyal medya üzerinden örgütlenip devrim yapılarak demokrasi getirilen ülkelerde kan ve gözyaşı dinmemiştir. Başta Mısır olmak üzere bazı ülkelerde ise askeri darbelerle devrim etkisizleştirilmiştir.

Türkiye'de Gezi Olayları sırasında ve 15 Temmuz kalkışmasına karşı direnişte Twitter ve Facebook etkin biçimde kullanılmıştır. 15 Temmuz'da başta Cumhurbaşkanı Recep Tayyip Erdoğan'ın FaceTime uygulamasıyla halka seslenişi, iktidar ve muhalefetten önde gelen siyasetçilerin ve kalkışmanın karşısında yer alarak devlete ihanete karşı çıkan generallerin demeçleri kısa sürede Twitter'da yayılmış halkın direnişe daha geniş kitleler halinde katılmasında önemli belirleyici olmuştur.

3. EMNİYET GENEL MÜDÜRLÜĞÜ TWITTER HESABINA GELEN TWEETLERİN DİNLENMESİ

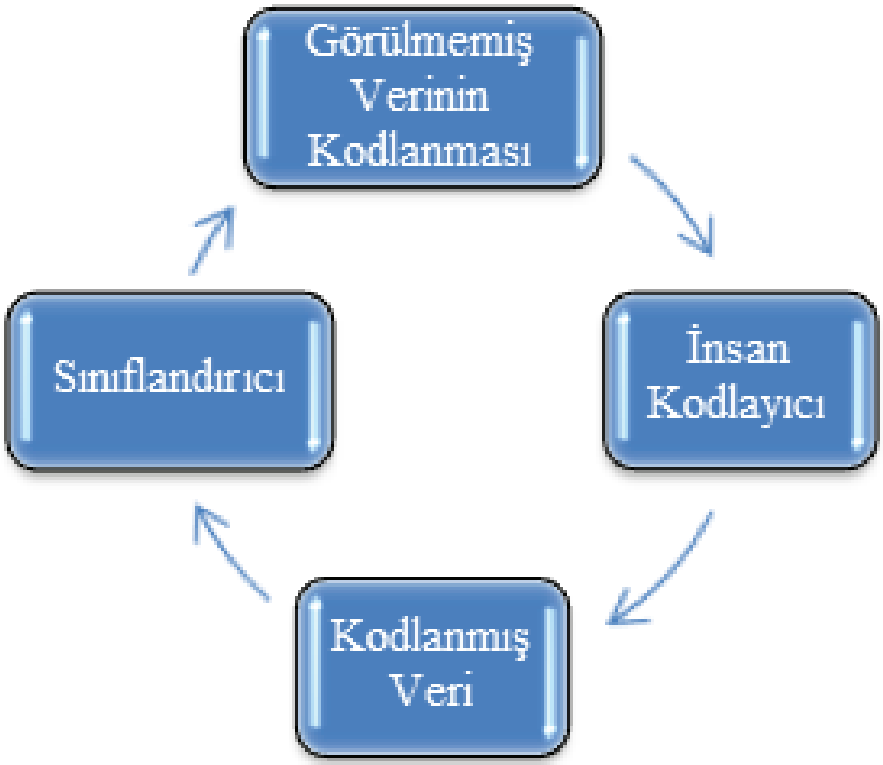
Bu çalışmada veriler 11.11.2018 – 18.02.2019 tarihleri arasında Twitter RESTful API üzerinden @EmniyetGM ve #EmniyeGManahtar terimleri takip edilerek toplanmıştır. Toplamda 44bin tekil kullanıcı tarafından atılan 107bin tweete ulaşılmıştır. Bu tweetlerin %90.1'i retweet iken %9.9'u organik olarak tespit edilmiştir. Kullanıcıların isimleri 114bin isim-cinsiyet ikilisinin olduğu bir sözlükle karşılaştırılmış ve böylece cinsiyetleri tespit edilmiştir. Buna göre kullanıcıların %76'sı erkek ve %24'ü de kadındır.

a. Veri Etiketleme

Verilerin etiketlenmesi için R programlama dili ile bir nitel kodlama aracı geliştirilmiştir. Bu araç teker teker tekil tweet metinlerini kullanıcıya gösterir. Kullanıcı okuduğu metni yalnızca bir kod altına kodlayabilir. Eğer anlamı karşılayan bir kod yoksa kullanıcı yeni bir kod oluşturabilir ya da var olan bir kodu geliştirebilir. Bu şekilde tweetler üzerinde ileri geri hareket ederek her grupta yeterli sayıda tweet kodlanmıştır. Geliştirilen araç retweetleri ve karbon kopya organik tweetleri kullanıcının belirttiği kodla işaretlemektedir.

Veriler etiketlenirken sınıflandırıcı destekli nitel analiz yöntemi kullanılmıştır. Bu yöntem King ve arkadaşlarının "Computer-Assisted Keyword and Document

Set Discovery from Unstructured Text" adlı makalesinde bahsettiği yöntemden esinlenerek geliştirilmiştir (King vd.,2017). Buna göre önce veriler belirli kategoriler altında kodlanmıştır. Daha sonra bu verilerle Naïve Bayes multinomial sınıflandırıcı eğitilmiştir. Sınıflandırıcının tespit ettiği veriler tekrar kodlayıcı tarafından uygun kategoriler altında kodlanmıştır (Şekil 1)



Şekil 1: Kodlama Yöntemi

b. Veri Temizleme

Veriler R programlama dili içerisine aktarılmıştır. Metin doküman-özellik matriksi (DFM) oluşturulurken *quanteda* R kütüphanesinin fonksiyonlarından yararlanılmıştır (Benoit, 2019). Öncelikle tweet metni içindeki bütün URL'ler silinmiştir. Ardından bütün karakterler Latin-ASCII karakter setinedönüştürülmüştür. Metinde alfabekarakterleri dışındaki bütün karakterler silinmiştir. *Regular expression (düzenli ifade)* fonksiyonlarından yararlanarak bitişik kelimeler ayrılmıştır. Bitişik kelimelerin tespitinde camelnotation tespit edilmiştir ve geriye bakma özelliği ile büyük harfler ayrılmıştır. Daha sonra bütün kelimeler küçük harfe dönüştürülmüştür. Türkçe için iyi bir *stemmer (köklere ayırıcı)* ve *lemmatizer (sözlük formu bulucu)* bulunmadığı için veriyi kirletmemek adına metin orijinal formunda bırakılmıştır.

Yukarıda anlatılan adımlar izlenerek *unigram* (tek terimli) DFM oluşturulmuştur. Buna ek olarak *trigram* (üç terimli) DFM ve retweeterların da eklendiği bir hibrit DFM de oluşturulmuştur. Ancak bahsedilen bu son iki DFM sınıflandırıcılar üzerinde herhangi bir etkide bulunmadığı için bu raporun devamında bahsedilmemiştir. DFM gereksiz kelimelerden temizlemek için *dfm_trim* fonksiyonu kullanılmıştır (sparsity=0.985). Daha sonra kelime frekansları aşağıdaki formüle göre ağırlıklandırılmıştır.

$$weight = \frac{1+\log_{10} tf_{,j}}{1+\log_{10} \sum_j tf_{,j}/\mathrm{N},}$$

c. Sınıflandırıcı Seçimi ve Düzenleme

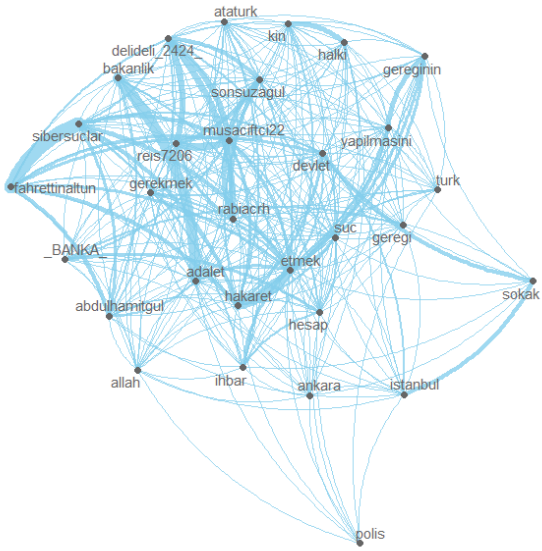
Bu çalışmada veriler 10 tekrarlı 10 katmanlı çapraz doğrulama metoduyla sınıflandırılmıştır. Her bir tekrar için sınıflandırılmak istenen grup verilerinin tamamı alınırken aynı sayıda tweet bu sınıfa dahil olmayan veriler arasından rastgele seçilmiştir. Böylece dengeli bir eğitme veri seti oluşturulmuş, meydana gelebilecek bir algoritma yanlılığı en aza indirgenmiştir.

Sınıflandırıcı olarak Naïve Bayes ve Supoort Vector Machines kullanılmıştır. Naïve Bayes sınıflandırıcı için multinomial dağılım seçilmiş ve laplace smoothing 1'e ayarlanmıştır. SVM sınıflandırıcı için linear, radial, sigmoid ve polynomial kerneller kullanılmıştır (Meyer vd.,2017). Her bir kernel için her tekrardan önce ayarlama yapılmıştır (cost= (0.01,0.1,1,5,10,100), gamma = (0.01,.1,1,5,10) , coef= (0.5,1,3,4), degree=(3,4)). Böylece farklı şekilde oluşan veri setleri için

optimizasyon sağlanmıştır.

d. Bulgular

Verilerin betimleyici istatistiklerine bakıldığında kurumsal Twitter hesaplarına verilen mentionlar ön plana çıkmaktadır. Bunun yanı sıra Trafik ve Dolandırıcılık ile ilgili tekil tweet sayısı çok olmasına rağmen etkileşim oranı çok düşük kalmaktadır. Yardım isteme ile ilgili tweetler ise Twitter kullanıcıları tarafından en fazla retweet edilen sınıf olarak ön plana çıkmaktadır. Benzer biçimde hayvanlara yönelik şiddet ve terörizm/ırkçılık diğer gruplardan daha fazla etkileşim almaktadır. Diğer sınıfların tekil ve retweet edilen içerik sayıları arasında doğrusal bir ilişki olduğu gözlenmektedir.



Şekil 2: Birlikte Geçme Sıklığı

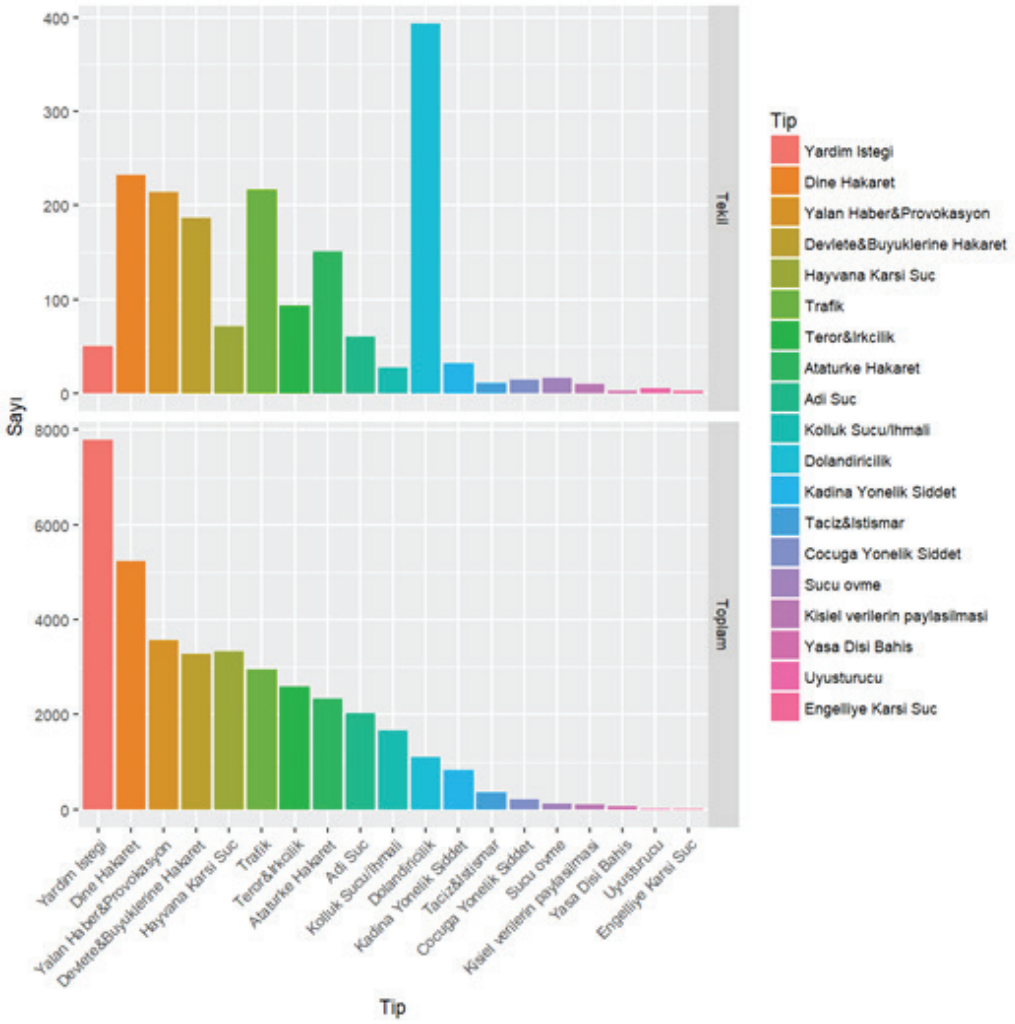
Şekil 3: Kelime Bulutu

Metin birlikte geçme sıklığını gösterir grafiğe göre devlet görevlileri ve resmi kurumların hesaplarına bir arada mention verilmiştir. Buradan yola çıkılarak kurumsallaşmanın geri plana düştüğü kurumların daha çok onları temsil eden şahıslar üzerinden işlediği fikri ortaya çıkmaktadır. Ağ analizinde ortaya dört ana kümenin çıktığı görünmektedir. Birinci küme hakaretle ilgilidir. Burada dini değerler, milli değerler ve ülkenin kurucusu Mustafa Kemal Atatürk'e yapılan hakaretler dile getirilmektedir. İkinci küme ise Türkiye'nin en büyük iki mega kenti İstanbul ve Ankara'da yaşanan trafik sorunları ile ilgilidir. Üçüncü küme ise

banka isimlerinin toplandığı dolandırıcılık ihbarlarının yapıldığı gruptur. Frekans analizine bakılarak çok fazla tekil şikâyet olmasına rağmen bu grupta etkileşim oranı çok düşüktür.

e. Sınıflandırıcı Sonuçları

Sınıflandırıcı sonuçlarına göre svm radial ve naive bayes yedi durumun üçünde en iyi tahminde bulunmuştur. Yedi durumun ikisini en iyi biçimde tahmin eden svm polynomial ve hiçbir durumda tahminlerinde diğerlerinde başarılı olamayan svm linear ve sigmoid sınıflandırıcılar fark yaratamamıştır.



Şekil 4: Kod Dağılımı

Naive bayes sınıflandırıcı ayırt edici kelimeler diğer sınıflarda olmadığında (banka, park, trafik…) svm sınıflandırıcılardan daha iyi sonuç vermiştir. Ancak devlete, Atatürk'e ya da dine hakaret gibi metinlerin birbirine çok benzediği daha karmaşık durumlarda svm radial başarılı olmuştur.

Tablo 1: Yapay Zeka Sınıflandırıcı Sonuçları

Grup	nb_multi	svm_linear	svm_polynomial	svm_radial	svm_sigmoid
Ataturke_Hakaret	0.813	0.927	0.936	0.938	0.897
Devlete_Buyuklerine_ Hakaret	0.799	0.818	0.825	0.825	0.742
Dine_Hakaret	0.833	0.862	0.863	0.873	0.813
Dolandiricilik	0.915	0.903	0.912	0.909	0.887
Teror_Irkcilik	0.733	0.756	0.780	0.774	
Trafik	0.901	0.875	0.883	0.900	0.867
Yalan_Haber_ Provokasyon	0.819	0.792	0.817	0.810	0.736

4. SONUÇ

Günümüzde teknoloji şirketleri akademisyenlere veriler üzerinde araştırma yapmaları için yeterince destek sağlamamaktadırlar. Bu da demokrasiyi, devleti ve toplumu tehditlere karşı savunmasız bırakmaktadır. Teknoloji şirketleri verilerini kar amacı gütmeyen bağımsız araştırmacılara açmalıdırlar. Kısıtlı ve hiyerarşik bir yaklaşımla da olsa Twitter dışında diğer şirketler akademisyenlere imkân sağlamamaktadır.

Bilgi teknolojileri ile seçmen tercihleri üzerinde yoğun biçimde deneylerin yapılması demokrasi anlayışı ile bağdaşmamaktadır. Bireyin ne isteyeceği sistem tarafından psikolojik analizlerle seçmene söylenmektedir. Gerçeklik sonrası bu dönemde insanlık veriye hükmedenlerin kölesi olma tehdidi ile karşı karşıyadır.

Devlet kurumlarını ortadan kaldırmak yerine bireylerin kurumları ve kurumların da bireyleri denetlediği bir sistem inşa etmek hak ve hürriyetlerin korunması

için çok önemlidir. Foucault'nun dediği gibi bilgi/iktidar üzerinden işlediği özneleri tekrar üretmekte ve mikro tekniklerle onu uysallaştırmaktadır (Foucault, 1982). Günümüzde ise bu teknikler çok daha sinsi biçimde işler hale gelmiştir ve yabancı istihbarat servisleri gibi kurumsallaşmış tehditlere karşı liberteryen bireysel çözümlerin etkisiz kalma tehlikesi vardır. Bunun nedeni bir veri noktasına dönüştürülen vatandaşların iktidarın bütün yüzlerine karşı savunmasız hale gelmesidir (Digeser, 1992).

Yapay zekâ araçları olumlu etkilerinin yanı sıra olumsuz sonuçlara da sebep olabilmektedirler. Bu çalışmada ise olumsuz etkilerin toplumun iyi biçimde bilgilendirilerek sosyal medya aracılığıyla güvenliği iyileştirmesine yönelik geliştirilebilecek bir proje önerilmiştir.

Elde edilen sonuçlara göre vatandaşlar sosyal medya aracılığıyla ihbarda bulunmakta ve ilgili kurumları müdahale etmeye davet etmektedirler. Bu içeriklerin makine öğrenmesi ile sınıflandırılarak daha hızlı ve daha etkin müdahale yeteneğinin kazandırılabileceği, vatandaşların özellikle provokatif ve dezenformatif içerikler karşısında korunabileceği gösterilmiştir.

KAYNAKÇA

Adrews, E. (2018). The Science Behind Cambridge Analytica: Does Psychological Profiling Work? Geliş tarihi 13 Nisan 2019, gönderen Stanford Graduate School of Business website: https://www.gsb.stanford.edu/insights/science-behind-cambridge-analytica-does-psychological-profiling-work

Askonas, J. (2019). How Tech Utopia Fostered Tyranny. *The New Atlantis*, 3-13.

Bakan, S., & Şahin, S. (2018). *Uluslararası Güvenlik Yaklaşımlarının Tarihsel Dönüşümü ve Yeni Tehditler*. 18.

Bashyakarla, V. (2018). France: Data Violations in Recent Elections - Our Data Our Selves. Geliş tarihi 27 Mart 2019, gönderen Tactical Technology Collective website: https://ourdataourselves.tacticaltech.org/posts/overview-france/

Benoit, K. (2019). quanteda: Quantitative Analysis of Textual Data (Versiyon 0.99.22) [R]. Geliş tarihi gönderen http://quanteda.io

Beres, D. (2019, Şubat 20). How Spotify manipulates your emotions and sells your data. Geliş tarihi 15 Nisan 2019, gönderen Big Think website: https://bigthink.com/technology-innovation/is-spotify-spying-on-you

Cadwalladr, C. (2017, Temmuz 5). The great British Brexit robbery: how our democracy was hijacked | Technology | The Guardian. *The Guardian*. Geliş tarihi gönderen https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

Chen, X., Wang, Y., Agichtein, E., & Wang, F. (2015). *A Comparative Study of Demographic Attribute Inference in Twitter*. 4.

Christian, B. (2012, Nisan 26). The A/B Test: Inside the Technology That's Changing the Rules of Business. *Wired*, *20*(5). Geliş tarihi gönderen https://www.wired.com/2012/04/ff-abtesting/

Christl, W. (2017). *Corporate Surveillance in Everyday Life*. 93.

Condliffe, J. (2017). Fake news is everywhere. Why? Because it's unbelievably cheap. Geliş tarihi 27 Şubat 2019, gönderen MIT Technology Review website: https://www.technologyreview.com/s/608105/fake-news-is-unbelievably-cheap/

Cookie Central. (t.y.). What Went Wrong? Geliş tarihi 27 Mart 2019, gönderen

http://www.cookiecentral.com/cookie5.htm

Cookiebot. (t.y.). Cookie consent | How to get valid consent for your website. Geliş tarihi 27 Mart 2019, gönderen Cookiebot website: https://www.cookiebot.com/en/cookie-consent/

Corner, J. (2017). Fake news, post-truth and media–political change. *Media, Culture & Society*, *39*(7), 1100-1107. https://doi.org/10.1177/0163443717726743

Digeser, P. (1992). The Fourth Face of Power. *The Journal of Politics*, *54*(4), 977-1007. https://doi.org/10.2307/2132105

European Commission. (2018, Mayıs). 2018 Reform of EU Data Protection Rules [Text]. Geliş tarihi 26 Şubat 2019, gönderen https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Foucault, M. (1982). The Subject and Power. *Critical Inquiry*, *8*(4), 777-795.

Froio, C., & Ganesh, B. (2018). The transnationalisation of far right discourse on Twitter. *European Societies*, *0*(0), 1-27. https://doi.org/10.1080/14616696.2018.1494295

Gebru, T., Krause, J., Wang, Y., Chen, D., Deng, J., Aiden, E. L., & Fei-Fei, L. (2017). Using deep learning and Google Street View to estimate the demographic makeup of neighborhoods across the United States. *Proceedings of the National Academy of Sciences*, *114*(50), 13108-13113. https://doi.org/10.1073/pnas.1700035114

Gilani, Z., Farahbakhsh, R., & Crowcroft, J. (2017). Do Bots impact Twitter activity? *Proceedings of the 26th International Conference on World Wide Web Companion - WWW '17 Companion*, 781-782. https://doi.org/10.1145/3041021.3054255

Google. (2019). *Fighting disinformation across our products*. Geliş tarihi gönderen https://www.blog.google/around-the-globe/google-europe/fighting-disinformation-across-our-products/

Hern, A. (2019, Ocak 28). Facebook to create "war room" to fight fake news, Nick Clegg says. *The Guardian*. Geliş tarihi gönderen https://www.theguardian.com/technology/2019/jan/28/facebook-war-room-fight-fake-news-nick-clegg-eu-elections-dublin-operations-centre

Hootsuite. (2017, Temmuz 10). A/B Testing on Social Media: How to Do it with Tools You Already Have. Geliş tarihi 27 Mart 2019, gönderen Hootsuite Social Media Management website: https://blog.hootsuite.com/social-media-ab-testing/

I Side With. (2017). Seçimler, siyasi konular, adayların ve anket veriler için Amerika'nın en popüler oylama kılavuzu. Geliş tarihi 14 Nisan 2019, gönderen iSideWith website: https://www.isidewith.com/tr/

Jiang, S., Martin, J., & Wilson, C. (2019). Who's the Guinea Pig? Investigating Online A/B/n Tests in-the-Wild. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 201–210. ACM.

King, G., Lam, P., & Roberts, M. E. (2017). Computer-Assisted Keyword and Document Set Discovery from Unstructured Text: Keyword and Document Set Dıscovery. *American Journal of Political Science*, *61*(4), 971-988. https://doi.org/10.1111/ajps.12291

Levin, S. (2018, Mayıs 14). Facebook suspends 200 apps as part of investigation into data misuse. *The Guardian*. Geliş tarihi gönderen https://www.theguardian.com/technology/2018/may/14/facebook-apps-suspended-privacy-scandal-cambridge-analytica

Li, Y., Yang, L., Xu, B., Wang, J., & Lin, H. (2019). Improving User Attribute Classification with Text and Social Network Attention. *Cognitive Computation*, *11*(4), 459-468. https://doi.org/10.1007/s12559-019-9624-y

Liu, Y., Cheng, D., Pei, T., Shu, H., Ge, X., Ma, T., … Xu, L. (2019). Inferring gender and age of customers in shopping malls via indoor positioning data. *Environment and Planning B: Urban Analytics and City Science*, 2399808319841910. https://doi.org/10.1177/2399808319841910

LIWC | Linguistic Inquiry and Word Count. (2018, Mart 9). Geliş tarihi 09 Mart 2018, gönderen https://liwc.wpengine.com/

Margetts, H. (2019). 9. Rethinking Democracy with Social Media. *The Political Quarterly*, *90*(S1), 107-123. https://doi.org/10.1111/1467-923X.12574

Matney, L. (2019, Ocak). Twitter testing 'Original Tweeter' tag to distinguish who started a thread. Geliş tarihi 20 Şubat 2019, gönderen TechCrunch website: http://social.techcrunch.com/2019/01/23/twitter-testing-original-tweeter-tag-to-distinguish-who-started-a-thread/

Mayer, J. R., & Mitchell, J. C. (2012). Third-Party Web Tracking: Policy and Technology. *2012 IEEE Symposium on Security and Privacy*, 413-427. https://doi.org/10.1109/SP.2012.47

Meyer, D., Dimitriadou, E., Hornik, K., Weingessel, A., & Leisch, F. (2017). e1071: Misc Functions of the Department of Statistics, Probability Theory Group (Versiyon 1.6-8) [R]. Geliş tarihi gönderen https://CRAN.R-project.org/package=e1071

Nguyen, D., Gravel, R., Trieschnigg, D., & Meder, T. (2013). " How Old Do You Think I Am?" A Study of Language and Age in Twitter. *ICWSM*.

Nielsen, N. (2018, Mart 28). Brexit vote manipulated, says data whistleblower. Geliş tarihi 26 Şubat 2019, gönderen https://euobserver.com/justice/141470

Pennycook, G., & Rand, D. (2019, Ocak 25). Opinion | Why Do People Fall for Fake News? *The New York Times*. Geliş tarihi gönderen https://www.nytimes.com/2019/01/19/opinion/sunday/fake-news.html

Rao, D., & Yarowsky, D. (2010). *Detecting Latent User Properties in Social Media*. 7.

Ratkiewicz, J., Conover, M. D., Meiss, M., Gonçalves, B., Flammini, A., & Menczer, F. M. (2011). Detecting and tracking political abuse in social media. *Fifth international AAAI conference on weblogs and social media*.

Sap, M., Park, G., Eichstaedt, J., Kern, M., Stillwell, D., Kosinski, M., … Schwartz, H. A. (2014). Developing age and gender predictive lexica over social media. *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 1146–1151.

Segal, S. (2017, Ağustos 15). Why A/B Testing Should Be Your Next Step on Social Media. Geliş tarihi 27 Mart 2019, gönderen The Oktopost Blog website: https://www.oktopost.com/blog/ab-testing-social-media/

Tirab, T. A. (2017). Küreselleşme Asrında Ulusal Güvenlik Perspektifinden Medya-Güvenlik İlişkisi ve Topluma Yansımaları. *Güvenlik Stratejileri Dergisi*, *13*(24), 113-151. https://doi.org/10.17752/guvenlikstrtj.356952

Torun, A. (2012). *Ulusal Güvenlik ve Küreselleşme: Türkiye'Nin Ulusal Güvenlik Politikasının Dönüşümünde Küreselleşmenin Rolü. ((National Security and Globalization: The Role of Globalization in The Transformation of Turkey's National Security Policy)*. Geliş tarihi gönderen htt-

ps://www.academia.edu/35668756/ULUSAL_G%C3%9CVENL%C4%B0K VE_K%C3%9CRESELLE%C5%9EME_T%C3%9CRK%C4%B0YEN%-C4%B0N_ULUSAL_G%C3%9CVENL%C4%B0K_POL%C4%B0T%-C4%B0KASININ_D%C3%96N%C3%9C%C5%9E%C3%9CM%C3%-9CNDE_K%C3%9CRESELLE%C5%9EMEN%C4%B0N_ROL%-C3%9C._National_Security_and_Globalization_The_Role_of_Globalization_in_The_Transformation_of_Turkeys_National_Security_Policy_

Twitter Public Policy. (2017, Şubat 28). Update: Russian interference in the 2016 US presidential election. Geliş tarihi 26 Şubat 2019, gönderen https://blog.twitter.com/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html

Vanian, J. (2018). Facebook, Twitter Take New Steps to Combat Fake News and Manipulation. *Fortune*. Geliş tarihi gönderen http://fortune.com/2018/01/19/facebook-twitter-news-feed-russia-ads/

Varga, K. (2018). Why European Campaigns Should Invest in Social Media Listening. Geliş tarihi 27 Mart 2019, gönderen Campaigns&Elections website: https://www.campaignsandelections.com/europe/why-european-campaigns-should-invest-in-social-media-listening

Wachter, S. (2018). The GDPR and the Internet of Things: a three-step transparency model. *Law, Innovation and Technology*, *10*(2), 266-294. https://doi.org/10.1080/17579961.2018.1527479

Wang, Z., Hale, S., Adelani, D. I., Grabowicz, P., Hartman, T., FlÃ\Pck, F., & Jurgens, D. (2019). Demographic Inference and Representative Population Estimates from Multilingual Social Media Data. *The World Wide Web Conference*, 2056–2067. https://doi.org/10.1145/3308558.3313684

Whittaker, Ja. (2018). Thousands of Twitter accounts that spread fake news during the 2016 election are still active today, say researchers. Geliş tarihi 27 Şubat 2019, gönderen TechCrunch website: http://social.techcrunch.com/2018/10/04/thousands-of-twitter-accounts-that-spread-fake-news-during-the-2016-election-are-still-active-today-say-researchers/

Who Should You Vote For. (2017). UK 2017 General Election Quiz. Geliş tarihi 14 Nisan 2019, gönderen Who Should You Vote For? website: https://www.whoshouldyouvotefor.com/

Zhang, J., Hu, X., Zhang, Y., & Liu, H. (2016). *Your Age Is No Secret: Inferring*

Microbloggers' Ages via Content and Interaction Analysis. 10.