

CyberMag



**TAGS Güvenlik Çözümleri
Yönetim Kurulu Başkanı
Sedat Gündüz İle Söyleşi**

Bir Milli Güvenlik Meselesi: ZOOM, TEAMS, MEET ve Diğerleri

Kurumsal Siber
Güvenlikte İçeriden
Gelen Tehditler

Türkiye'de 1,6 Milyon
Siber Saldırı Gerçekleşti

Online Oyunları
Hedefleyen Siber Casusluk
Saldırısı Ortaya Çıktı

Küresel Salgın Döneminde
Kişisel Veriler ve Temas
Takip Uygulamaları

İşletmeler İçin 2021 Yılı
BT Güvenlik Önerileri

Pandemi Döneminde
Siber Zorbalık %81
Oranında Arttı!



Bir Milli Güvenlik Meselesi: ZOOM, TEAMS, MEET ve Diğerleri



**Dr. Öğr. Üyesi Yavuz
CANBAY**

Kahramanmaraş Sütçü İmam
Üniversitesi /
Bilgisayar Araştırma ve Uygulama
Merkez Müdürü

COVID-19 pandemisinin ortaya çıkması ile beraber hayatımıza giren "yeni normaller", özellikle dijital dünyada ağırlığını zamanla hissettirmeye başlamıştır. Pek çok fiziksel aktivite ve ortamın, evden çalışma, uzaktan eğitim, çevrimiçi toplantılar gibi sanal ortamlara taşındığı günümüzde, insanlar arası toplu etkileşimi sağlamak için çeşitli çevrim içi görüşme ve video konferans uygulamalarından faydalanılmaktadır. Pek çok uygulamada olduğu gibi video konferans uygulamalarında da çok sayıda kişisel veriler toplanmakta ve bu veriler uygulama geliştirici firma tarafından işlenip analiz edilmektedir. Özellikle video, ses, görüntü gibi insanı doğrudan tanımlayabilecek pek çok verinin aktarıldığı bu ortamlarda, toplanan verilerden ne tür çıkarımlar yapılabileceği hakkında bir farkındalık olmadığı için insanlar rahatlıkla bu tür uygulamaları kullanabilmektedir. Ülkemizde, pandemiden kaynaklı olmak üzere okul öncesi eğitimde bile kullanılabilen bu uygulamalar, getirdiği faydalarının yanı sıra çeşitli olumsuzlukları da barındırmaktadır.

Yabancı menşeli video konferans ve çevrimiçi görüşme uygulamaları, ülkemiz vatandaşları hakkında şimdiye kadar sahip olmadıkları büyüklükte ve nitelikte kişisel verilere maalesef ki pandemi sürecinde sahip oldular. Bu yazının amacı, faydalı gibi görünen özellikle yabancı menşeli video konferans uygulamalarının ülkemiz için nasıl bir milli güvenlik meselesi haline dönüşebileceğine dikkat çekmektir.

Dünyayı kasıp kavuran, bilim insanlarının bir çözüm aramaya çalıştığı ve muhtemelen önümüzdeki yıllar boyunca da aramızda olacak olan COVID-19 pandemisi, ortaya çıktığı günden bu yana insanların hayatını olumsuz yönde etkilemektedir. Özellikle sosyal hayatı büyük ölçüde etkileyen COVID-19 pandemisi, insanların tüm yaşayış modellerinin değişmesine neden olmuştur.

Eğitim ve iş gibi alanlar başta olmak üzere; insanların, kurum ve kuruluşların yeni normallerini tanımladığı bu zamanda, sosyal bir varlık olarak insanı bir okul veya iş ortamında bir araya getirme imkânı zorlaşırken, çevrimiçi olarak yapılan

aktiviteler ile bu zorluk aşılmaya çalışılmaktadır. Dolayısıyla eğitim ve iş gibi aktivitelerin gerçek ortamdan artık sanal ortama taşındığı bir döneme girmiş bulunmaktayız.

Böylesi bir dönemde, insanların eğitim ve iş alanında gerekli faaliyetlerini yürütebilmeleri için amaçlarına yönelik pek çok uygulamayı kullandıklarını bilmekteyiz. Özellikle gerek eğitim gerekse de iş için çeşitli görüntülü iletişim ve video konferans araçlarından sıklıkla faydalanılmaktadır. Zoom, Google Meet, Microsoft Teams ve Webex bu uygulamalardan bazıları olarak sayılabilir.

Ülkemizde ilköğretim ve ortaöğretim öğrencilerinin özellikle Millî Eğitim Bakanlığı'nın sunmuş olduğu 'eğitim bilişim ağı' (EBA) üzerinden canlı ders eğitimlerini aldıkları, gerek duyulması halinde ise bu eğitimlerin Zoom gibi çevrimiçi toplantı platformlarında gerçekleştirildiğini bilmekteyiz. Üniversitelerde ise öğrenme yönetim sistemi gibi uygulamaların yanı sıra, Zoom, Youtube, Microsoft Teams, Google Meet gibi uygulamalar sıklıkla kullanılmaktadır.

Gerçek dünyada varlığı ile kendini temsil eden insan, elbette ki sanal ortamlarda da kendini bir şekilde temsil etmektedir. Bu temsil etme biçimi genel olarak kişiyi tanımlayıcı veriler ile sağlanır. Yani insan, sanal dünyada sahip olduğu verileri ile kendini temsil eder. Örneğin, fotoğraflar, videolar, paylaşımlar, ses bilgileri gibi pek çok bilgi aslında insanı temsil eden çeşitli verilerdir. Yani başka bir ifadeyle kişisel verilerdir.

Kişisel veri, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanır. Gerek işlenmesi gerekse de paylaşılması kapsamında kanuni bazı gereklilikleri beraberinde getiren kişisel veriler, insanların farkındalık seviyeleri kadar değer kazanabilmektedir. Yani farkındalık seviyesi düşük olması halinde kişisel veriler çok kolay bir şekilde üçüncü kişi veya uygulamalarla paylaşılabiliyorken, farkındalığın yüksek olması durumunda ise bu paylaşım minimum seviyelerde gerçekleşebilmektedir.

Özellikle 2018 yılında meydana gelen Cambridge Analytica skandalıyla beraber insanların kişisel verilerini koruma konusunda genel olarak farkındalıklarının arttığı söylenebilir. Ayrıca ülkemizde ise 8 Ocak 2021 tarihinde meydana gelen WhatsApp gizlilik sözleşmesi güncellemesi ile beraber, özellikle üst yönetici-

ler ve karar vericiler seviyesinde oluşan kişisel veri mahremiyeti farkındalığının ülkemiz vatandaşlarına da yansıdığını görebilmekteyiz.

İnsanların kişisel verilerini koruma farkındalıkları genel olarak bir ihlal meydana geldiğinde oluşmakta veya artmaktadır. Yukarıda verilen Cambridge Analytica ve WhatsApp örnekleri dikkate alındığında, insanlarda bu konularda bir farkındalık oluşmuş iken, halen genel bir kişisel veri mahremiyeti farkındalıkları olduğunu söylemek yeterli olamaz. Örneğin, TikTok uygulaması için yayımlanan istatistiklere bakıldığında, ülkemizin 28.4 milyon kullanıcı ile dünyada 3. sırada yer aldığı görülmektedir. Her ne kadar basit bir sosyal medya uygulaması olarak görünüyorsa da kişiler hakkında çok sayıda kişisel veri topladığı da bir gerçektir. ABD'de ulusal güvenlik ve veri güvenliği gerekçesiyle yasaklanan bu uygulamayı ülkemizde nüfusun neredeyse üçte birinin kullanması hali hazırda vatandaşlarımızın genel bir kişisel veri mahremiyeti farkındalıklarının tam olarak oluşmadığının en önemli kanıtıdır.

Görüntülü görüşme ve video konferans uygulamaları arasında dünyada en çok günlük katılımcı sayısına sahip olan uygulama Zoom'dur. Mobil aplikasyon kapsamında yayımlanan istatistiklerde Zoom uygulamasının ülkemizde Mayıs ayında 3.7 milyon gerçek kullanıcıya sahip olduğu raporlanmıştır. Bu uygulama için kullanıcı sayısına dair net rakamlar ilgili firma tarafından yayımlanmasa da bu konuda yayımlanan tek resmi istatistik Türkiye'de kullanıcı sayısının pandemi-den sonra 139 kat arttığı bilgisidir.

Ülkemizde okul öncesi eğitim, ilköğretim, ortaöğretim ve yükseköğretim gibi eğitim basamaklarında Zoom uygulaması yaygın olarak kullanılmaktadır.

Buna özellikle kamu kurum ve kuruluşları ile özel sektörün de kullanımı eklendiğinde, kullanım oranının çok yüksek rakamlarda olduğu bir gerçektir.

Özellikle eğitim alanında, pandemi ile beraber kullanımı artan EBA uygulaması incelendiğinde, harici canlı ders oluşturma alanında özellikle Zoom uygulaması üzerinden işlenecek derse ait bilgilerin kullanıldığı, ayrıca klasik canlı ders işlenirken ise "Powered by Zoom" ifadesinin ders ekranında bulunduğu görülebilmektedir. Bu kapsamda, özellikle okul öncesi eğitim, ilköğretim ve ortaöğretim gibi eğitim seviyelerindeki öğrencilerin hem klasik hem de canlı ders işlenirken Zoom tarafından uygulanan her türlü politikaya maruz kaldığını söylemek mümkündür. Bir başka ifadeyle gerek dersleri veren öğretmenlerin gerekse de derse katılım sağlayan öğrencilerin ses, görüntü veya video gibi kişisel bilgileri Zoom tarafından toplanmakta ve işlenmektedir denilebilir.

Yükseköğretimde ise her ne kadar öğrenim yönetim sistemlerinden faydalanılsa da muhakkak ki buralarda da bu sistemlere ek olarak Zoom, Meet, Teams gibi uygulamaların kullanıldığı, hatta pek çok konferans ve seminer gibi sosyal etkinliklerde de bu uygulamalardan faydalanıldığı aşikardır.

Eğitimden iş alanına geçecek olursak gerek ücretli gerekse de ücretsiz versiyonlarının bulunduğu Zoom gibi uygulamaların özellikle evden çalışma kapsamında faydalandığı ve sıklıkla kullanıldığı söylenebilir. Bu kapsamda da uygulamayı kullanan gerek çalışanların gerekse de kuruma ait verilerin Zoom gibi uygulamalar tarafından toplandığını ve işlendiğini söylemek yanlış olmaz.

Tablo 1. Zoom Uygulaması Tarafından Toplanan Kişisel Veriler

Ad Soyad	Ses kaydı
Doğum Tarihi	Dosyalar
Telefon	Mesajlar
Eposta	Rehberde kayıtlı kişiler
Toplantı planı	Fotoğraflar
IP Adresi	Takvim bilgileri
Konum	Aygıt kimliği
Video kaydı	Çerez bilgileri

Bu gibi durumlar göz önüne alındığında, okul öncesi yaştaki bireylerden iş alanında çalışan bireylere kadar her yaştan kesimin kullandığı veya bir şekilde kullanılmak zorunda olduğu Zoom gibi uygulamaların, insanlardan topladığı video, görüntü ve ses gibi temel veriler için nasıl çıkarımlar yapabileceği, insanları nasıl modelleyebileceği, bu faydalı gibi görünen uygulamanın insanlarımızı nasıl gelecek vadede zarar verebileceği ve mahremiyetini ifşa edebileceğine yönelik bir analiz ilerleyen bölümde sunulmuştur.

Örnek olması açısından Zoom uygulamasının ilgili tüm platformlarından topladığı kişisel verilerden bazıları bir önceki sayfada Tablo 1’de listelenmiştir.

Video/görüntü ve ses verileri kullanarak ne tür çıkarımlar yapılabilir?

Tablo 1’de sunulan kişisel veriler ayrı ayrı veya bir araya getirilerek kullanıldığında insanlara ait pek çok çıkarımları yapmak mümkündür. Ancak bu çalışmada sadece video ve ses kaydı kullanılarak yapılabilecek analizlere yer verilmiştir.

Video, içerisinde çok sayıda görüntü içeren bir veri türüdür. Bu kapsamda, video için yapılabilecek çıkarımlarda görüntü verilerini içeren çalışmalar ve çıkarımlar dikkate alınmıştır. Bu kapsamda görüntü ve ses verileri kullanılarak literatürde kişiler hakkında elde edilebilecek bazı çıkarımlar Tablo 2’de sunulmuştur.

Tablo 2’de sunulan bilgiler detaylı olarak incelendiğinde; insanlara ait sadece görüntü ve ses verileri kullanılarak çok çeşitli çıkarımların yapılabildiği görülebilmektedir. Kişilik tespitinden IQ seviyesi belirlemeye, politik görüşten hastalık tespitine kadar pek çok kişisel verilerin görüntü veya ses kayıtları aracılığıyla elde edilebileceği gerçeği önemli bir sorundur. Zira, insanı tanımlayıcı pek çok bilgiyi elde eden herhangi bir yapı, bunu o insanlara veya ülkelere karşı çok rahatlıkla kötücül niyetlerle kullanabilir.

Özellikle bu çıkarımlar yapılırken klasik yaklaşımlardan ziyade, makine öğrenmesi ve derin öğrenme gibi bilgisayar destekli teknolojilerin de kullanılabilirdiği ve bu şekilde aslında çok miktarda verilerden çıkarımların rahatlıkla ve otomatik bir şekilde yapılabildiğini söylemek yerinde olacaktır. Yani milyonlarca kişi hakkında bilgi çıkarımında bulunmak için önemli bir insan desteğine ihtiyaç duyulmayacağını söylemek gerekir.

Tablo 2. Görüntü ve Ses Verilerinden Yapılabilecek Bilgi Çıkarımları

Odak	Veri türü	Kullanılan Teknik	Yapılan Bilgi Çıkarımı
Deneyime Açıklık, Sorumluluk, Uyumluluk, Duygusallık, Dışadönüklük	Görüntü	Derin Öğrenme	Kişilik tespiti
Suç eğilim	Görüntü	Makine Öğrenmesi	
Kişilik izlenimi	Görüntü	Makine Öğrenmesi	
Deneyime Açıklık, Sorumluluk, Uyumluluk, Duygusallık, Dışadönüklük, Narsisizm, Makyavelizm, Psikopati	Görüntü	Araştırma	
Deneyime Açıklık, Sorumluluk, Uyumluluk, Duygusallık, Dışadönüklük	Ses	Makine Öğrenmesi	
Korku, Sinir, Mutluluk, Üzgünlük, Tiksinme, Aşağılama, Neşeli Durumları	Ses	Makine Öğrenmesi	Duygu tespiti
Can Sıkıntısı, Korku, Sevinç, Üzgünlük	Ses	Makine Öğrenmesi	
Kabul Etme, Konsantre Olma, Katılmama, İlgilenme, Düşünme, Emin Olmama	Görüntü	Makine Öğrenmesi	Mental Durum Tespiti
Cinsiyet	Ses	Makine Öğrenmesi	Cinsiyet Tespiti
Yüz İfadeleri, Mimik	Görüntü	Derin Öğrenme	Politik Görüş Tespiti
Yüz Yapısı	Görüntü	İstatistiksel	IQ Seviyesi Tespiti
Yüz Özellikleri	Görüntü	Derin Öğrenme	Yaş Bilgisi Tespiti
Yüz, Vücut Bilgileri	Görüntü	Makine Öğrenmesi	Meslek Bilgisi Tespiti
Geometrik Özellikler, Ten Rengi	Görüntü	Derin Öğrenme	Etnik Köken Tespiti
Genetik hastalık	Görüntü	Makine Öğrenmesi	Hastalık Tespiti
Akromegali	Görüntü	Makine Öğrenmesi	
Ateş	Görüntü	Derin öğrenme	
Kalp Atışı	Görüntü	Makine öğrenmesi	
Parkinson	Görüntü	Derin öğrenme	
Parkinson	Ses	Makine Öğrenmesi	
Normal, Kilolu, Obez	Ses	Makine Öğrenmesi	Vücut Kitle Endeksi Tespiti
Boy, Kilo	Görüntü	Derin öğrenme	Fiziksel Görünüş Tespiti

Tablo 2’de sunulan bilgiler ışığında, okul öncesi eğitimden yükseköğretime kadar ülkemizin genç nüfusu hakkında çok kolay çıkarımların Zoom uygulamasının topladığı verilerle yapılabileceği, önemli bir güvenlik meselesidir. Nitekim özellikle bu yaş aralığındaki bireylerin ülkemizin geleceğini temsil eden bireyler olduğu düşünüldüğünde özellikle politik görüşten muhtemel hastalıklara kadar pek çok bilginin başka ülkeler tarafından edinilmesi, bu bireylerin hayatlarını çok olumsuz şekillerde

etkileyebilir ve çok rahatlıkla bu bireyler yönlendirilebilir.

Yönlendirme aşamasında en kolay yöntem kişiselleştirilmiş yapılardır. Örneğin; kişiselleştirilmiş reklamlar, kişiselleştirilmiş videolar, kişiselleştirilmiş Facebook ana sayfaları, kişiselleştirilmiş TikTok ana sayfaları gibi pek çok ürün ve uygulama insanlara özgü çeşitli yardımcı bilgileri kullanarak o kişilere özel hizmetler sunmayı amaçlar. Karakter, kişilik, IQ, cinsiyet, politik görüş, fiziksel görünüş, mental durum, meslek bilgileri gibi pek çok bilgi



kötü niyetli kişilerin veya ülkelerin tespit etmesi halinde; bu bilgilere göre kişileri modelleyip, oluşturdukları bu modellere göre kişiselleştirilmiş hizmetler sunmaları çok da zor bir durum değildir. Nihayetinde yapacakları her türlü kötü niyetli faaliyet ile amaçlanan ana unsur, insanları yönlendirme becerisi üzerine olacaktır.

Buna ek olarak, iş hayatında da bu uygulamanın kullanılması genel anlamda ticari sırların deşifre edilmesi ve hatta rakip firmalara satılabileceği durumunu da muhakkak ortaya çıkarabilecektir. Ayrıca çalışanlar hakkında yine tabloda sunulan verilerin elde edilmesi de bu kişilerin mahremiyetini ifşa edebilecek potansiyel çıkarımlar yapılmasına neden olacaktır.

Bu yazı kapsamında Zoom özelinde yapılan analizlerin, yabancı menşeli diğer video konferans uygulamaları için de geçerli olacağını söylemekte fayda vardır. Neticede ülke sınırları içerisinde kalmayan her türlü kişisel veri üzerinde yabancı ülkelerin bir tasarrufu olacağı ve bu bilgileri yakın gelecekte ülkemize karşı kullanabileceği gerçeğini göz ardı etmemekte fayda vardır.

Sonuç ve Değerlendirmeler

Siber vatan kavramının hayatımıza girdiği bu zamanda, özellikle vatandaşlarımıza ait verilerin ülkemizde kalması, ancak ve ancak milli ve yerli yazılımlar ile mümkündür.

Bu açıdan HAVELSAN tarafından geliştirilen Diyalog uygulamasının önemi büyük olmakla beraber, bu uygulamanın kullanım alanının genişletilmesi, buna benzer yerli ve milli video konferans uygulamalarının ülkemizde sayısının artırılması ve desteklenmesi, geleceğimizin teminatı olan gençlerimizin kişisel verilerini koruyarak geleceğe güvenle bakılması açısından millî bir güvenlik meselesi haline gelmiştir.

İnsanların görüntü ve sesinden bu çıkarımların yapılabilmesinin en tehlikeli yanı, insanları modelleyerek kişilik tespitinden fiziksel görünüşün tespitine kadar pek çok farklı bilgiyi kullanarak çeşitli yaş gruplarını yönlendirebilmenin veya yönetmenin kolay olacağıdır. Örneğin, kişinin suça meyillini belirledikten sonra o kişiden bir terörist yaratmak, kişinin politik görüşünü belirledikten sonra onu yönlendirmek zor bir durum olmasa gerek.

Özellikle "Türkiye'nin verisi Türkiye'de kalmalı" sloganıyla başlatılan hareketin ülkemizde pek çok alanda milli ve yerli yazılımların geliştirilmesi ve ülke sınırları içerisinde bulunan veri merkezlerinin kurulması ile ancak gerçekleştirilebileceği aşikardır. Vatandaşlarımızın kişisel verilerinin toplandığı ve işlendiği tüm uygulamaların verilerini bu merkezlerde tutması zorunluluğu önemli bir adım olacaktır.

Vatandaşlarımıza ait kişisel verilerin yabancı ülkelerin eline geçmesi ile ülkemizi her alanda rahatlıkla yönlendirebilecekleri unutulmamalı ve bu kapsamda gerekli tüm tedbirler acilen alınmalıdır. Eğitimde ise yabancı menşeli uygulamaları kullanmadan, yerli ve milli yazılımların sayısının ve kapasitelerinin hızla artırılıp bunların tercih edilmesi gerekmektedir.

“

İnsanların görüntü ve sesinden bu çıkarımların yapılabilmesinin en tehlikeli yanı, insanları modelleyerek kişilik tespitinden fiziksel görünüşün tespitine kadar pek çok farklı bilgiyi kullanarak çeşitli yaş gruplarını yönlendirebilmenin veya yönetmenin kolay olacaktır.

”