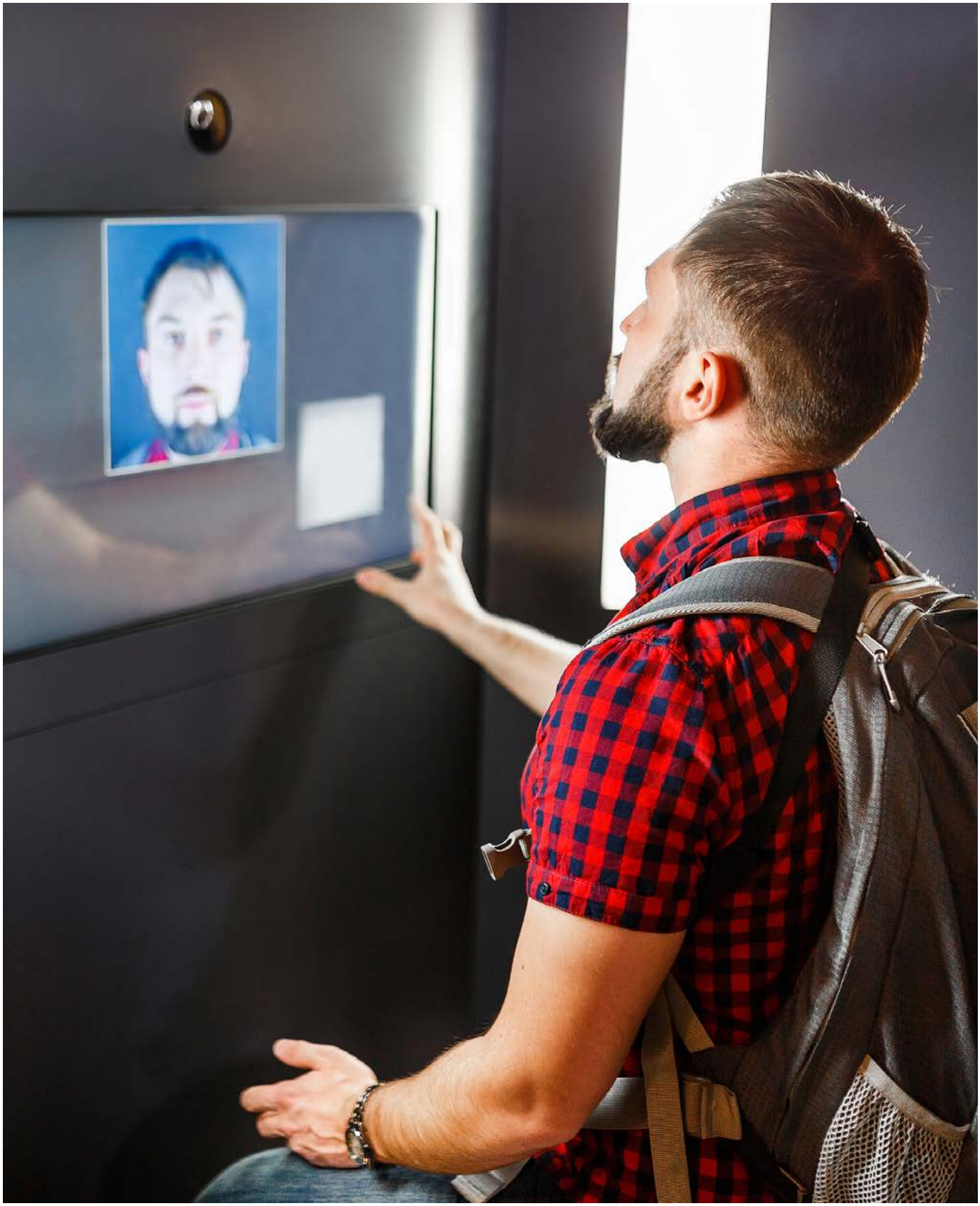
YÜZ TANIMA SİSTEMLERİNİN BUGÜNÜ VE GELECEĞİ

TREND ANALİZİ EKİM 2021

thinktech
STM Teknolojik Düşünce Merkezi



STM ThinkTech

1. GİRİŞ

Günümüzün küreselleşen dünyasında kişilerin, mal ve hizmetlerin dolaşımı kolaylaşırken, terör ve suç amaçlı gruplar da bu durumu suiistimal etmişlerdir. Pek çok alanda birbirine eklemlenmiş bir dünyanın faydalarından yararlanma sürdürülürken terör ve suçu önlemek büyük önem kazanmıştır. Terör ve suçun önlenmesi için ise öncelikle bunları tertipleyenlerin kimliklerinin tespit edilmesi gereği ortaya çıkmıştır.

Bugüne kadar kimliğini saklayarak suç işleyenlerin tespiti için pek çok yöntem geliştirilmiştir. Kişiye özgün bedensel ayrıntılardan faydalanan biyometrik sistemler bunların başında gelmektedir. Biyometrik sistemler, kişinin sahip olduğu fizyolojik ve davranışsal özellikleri kullanarak kişinin tanınmasını ve onaylanmasını sağlamaktadır. Bu amaçla, parmak izi, iris, yüz, ses, avuç içi ve hatta kulak gibi kişinin fizyolojik özelliklerinin yanı sıra yürüyüşü, imzası, konuşması gibi davranışsal özellikleri de biyometrik sistemlerde sıkça kullanılmaktadır. Söz konusu biyometri sistemleri, doğruluk, güvenilirlik ve erişilebilirlik açılarından farklılık göstermektedir. Biyometrik kimlik doğrulama yöntemlerinin her biri diğerine kıyasla avantaj ve dezavantajlara sahip olabilmektedir.

Biyometrik sistemler arasında son yıllarda en çok gelişme kaydeden tür yüz tanımadır. Akıllı cep telefonlarının kilidini açmak için kullanılması veya sosyal medya sitelerine yüklenen fotoğraflardaki kişilerin kimliklerinin otomatik olarak tanımlanmasıyla popülerlik kazanan Yüz Tanıma Teknolojisi (YTT) uygulamaları uzun zamandır günlük yaşamda kullanılmaktadır. Başta havaalanları ve sokak kameraları olmak üzere kent güvenlik sistemlerinde YTT yaygın olarak kullanım bulmaktadır. 2019'da yayınlanan bir araştırmaya göre 64 ülkede YTT kullanılmaktadır[1]. Yüz tanımanın yanı sıra kimlik doğrulamak için de kullanılan YTT; yapay zekâ, büyük veri, bilgisayarlı görü ve kızılötesi görüntüleme gibi teknolojilerde sağlanan gelişmeye paralel olarak, giderek daha güvenilir bir kimlik tespit ve doğrulama yöntemi olarak ön plana çıkmaktadır. Öyle ki ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) yaptığı testlere göre 2014'te en gelişmiş yüz tanıma algoritmasının hata oranı yüzde 4,1 seviyesindeyken, bu oran Nisan 2020'de yüzde 0.08'e kadar düşmüştür[2]. Hata oranındaki bu çarpıcı düşüş yüz tanıma teknolojilerinin sadece güvenlik alanında değil, sağlıktan eğitime psikolojiden lojistiğe kadar pek çok alanda yararlı bir araç hâline gelmesine yol açmıştır.

Bu alanlardan biri de savunmadır. Bugün askeri tesislerin savunmasından savaş alanında dost ve düşman birliklerinin ayırt edilmesine ve gece yüz tanınmasına kadar pek çok alanda YTT askeri birliklerin önemli bir yardımcısı hâline gelmektedir.

Fakat bu ilerlemelere karşın YTT'nin zafiyetleri sürmekte ve kullanımına ilişkin yaygın bir endişe bulunmaktadır. Analizimizde YTT'nin çalışma prensipleri, kullanım alanları ve bu teknolojiler üzerindeki tartışmalar ele

alınacaktır. Analizde özellikle yüz tanımanın savunma ve güvenlik alanındaki uygulamaları ayrıca değerlendirilecek ve gelecekte bu teknolojinin getirebileceği faydalara değinilecektir.

2. YÜZ TANIMA SİSTEMLERİ VE KULLANIM ALANLARI

Teorisi 1960'lı yıllarda[3] ortaya atılmasına rağmen uygulama bulması gelişmiş kameralar, bulut bilişim ve yapay zekâ alanlarındaki gelişmeleri beklemiş olan YTT dünyada büyük yaygınlık kazanmaktadır.

2.1 Tanımı ve Diğer Teknolojilerle İlişkisi

Yüz tanımaya ilişkin olarak literatürde çeşitli başlıklar altında tanım önerileri bulunmaktadır. Örneğin NATO, yüz tanımayı biyometrik sistemler başlığı altında değerlendirmektedir. NATO'ya göre biyometri, "Kişilerin davranışlarının ve biyolojik özelliklerinin temel alınarak kimliklerinin otomatik olarak tanımlanmasıdır"[4]. ABD ordusu ise yüz tanımayı "Kimlik istihbaratı" kavramı altında değerlendirmekte ve bunu da "İlgili şahıs, grup, ağ veya toplumlara atfedilebilir kimliklerin işlenmesi sonucu elde edilen istihbarat" olarak tanımlamaktadır[5].

Doğrudan yüz tanımaya ilişkin bir tanım ise Avrupa Birliği tarafından önerilmiştir. Avrupa Konseyi'nin Yüz Tanımlama Yönergesi'nde[6] ifadesini şöyle bulmuştur: "Yüz tanımlama, yüz şablonları kullanarak bireylerin yüzlerini içeren dijital görüntülerin söz konusu kişinin kimliğini tespit etmek için otomatik olarak işlenmesidir."

Daha basit bir ifadeyle yüz tanıma, bir bireyin yüzünü kullanarak kimliğini tespit etme veya doğrulama yöntemidir[7]. Yüz tanımlama sistemleri ise fotoğraflar, videolar veya gerçek zamanlı görüntüler kullanarak insanların kimliklerini tespit etmektedir.

Teknolojik açıdan bakıldığında yapay zekâ veya bilgisayarlı görü'nün[8] bir dalı olan "Yüz tanıma", aslında bir teknoloji değil, diğer teknolojilerden yararlanan bir yöntemdir. Bu yüzden yüz tanıma, yapay zekâ veya bilgisayarlı görü teknolojisinin bir "uygulama alanı" olarak da tanımlanmaktadır.

Yüz tanıma sistemleri için yapay zekâ algoritmaları vazgeçilmezdir. Bu yöntem, insan yüzünün kalıplarını öğrenmek için yapay zekâya güvenir. Yapay zekâ sistemi, insan yüzlerinden oluşan bir veri kümesinden öğrenmek için bir makine öğrenmesi modeli kullanır. Bu veri kümeleri, sosyal medya platformlarından ve milyonlarca başka internet sitesinden alınan veriler kullanılarak derlenebilir ve milyonlarca görüntüyü içerebilir[9].

Bilgisayarlı görü ise, sistemlerin bilgi elde etmek için görsel verileri (fotoğraflar veya videolar) yorumlamasını sağlar. Sistemlerin bu görüntüleri işlemesine ve analiz etmesine izin veren sinir ağları oluşturmak için derin öğrenmeyi kullanır. Bu modeller eğitildikten sonra nesneleri ve insanları tanıyabilir ve hatta hareketlerini takip edebilir.

Yüz tanıma sistemleri yaygınlaştıkça veritabanları genişlemekte ve tanımlama işlemleri güçleşmektedir. Bu nedenle günümüzde yüz tanıma sistemleri derin öğrenme[10] ile desteklenmektedir. Derin Öğrenme, çok sayıda yüz verilerini işlerken aralarındaki örüntüleri de ortaya çıkarır. Daha sonra bu örüntüleri yeni görüntüleri işlemek için kullanır.

Yüz tanıma sistemleri, bir görüntüde algılanan bir yüzün belirli özellikleri arasındaki mesafeleri ölçer. Kişinin teninin dokusunu tespit eder. Hatta bir yüzün termal profilini çıkarır. Bunlar sayesinde bir yüzü diğerlerinden ayırabilir. Böylece, tespit edilen kişiye has özellikler daha önce elde edilen yüz profilleriyle karşılaştırılabilir ve kişinin kimliği tespit edilebilir.

2.2 Yüz Tanıma Nasıl Sağlanır?

Yüz tanıma sistemleri bir kişinin yüzünün özel ve ayırt edici özelliklerini toplamak için bilgisayar algoritmaları kullanır. Gözler arasındaki mesafe veya çenenin şekli gibi ayrıntılar daha sonra matematiksel ifadelere çevrilir ve yüz tanıma veritabanında toplanan diğer yüzlere ilişkin verilerle karşılaştırılır. Belli bir yüze ilişkin veriler genellikle bir yüz şablonu olarak adlandırılır ve bir fotoğraftan farklıdır çünkü bir yüzü diğerlerinden ayırt etmekte kullanılabilecek belli detayları içerecek şekilde tasarlanmıştır.

Bazı yüz tanıma sistemleri, bilinmeyen bir kişiyi pozitif olarak tanımlamak yerine, bilinmeyen kişi ile veritabanında saklanan belirli yüz şablonları arasında olası eşleşmeleri bulmak için tasarlanmıştır. Bu sistemler, yalnızca tek bir sonuç yerine, doğru tanımlama olasılığına göre sıralanmış birkaç eşleşme sunmaktadır.

2.2.1 Yüz Algılama Yöntemleri

Bir bilgisayarın yüz tanıma yapabilmesi için kullanabileceği, aydınlatma, yön veya kamera mesafesini telafi eden yöntemler vardır. Yang, Kriegman ve Ahuja, yüz algılama yöntemleri için bir sınıflandırma sunmuştur[12]. Bu yöntemler genelde beş kategoriye ayrılmaktadır. Ancak yüz algılama algoritmaları iki veya daha fazla kategorideki yöntemleri kullanabilir[13].

- **Bilgi Tabanlı Yüz Algılama (Knowledge Based Facial Recognition):** Bu yöntem, insanlar tarafından geliştirilen bir dizi kurala dayanır. Söz konusu kurallar, yüzün temel özellikleri üzerinden belirlenebilir. Örneğin "bir yüzde belli bir aralıkla iki göz, bir burun ve bir ağız olmalıdır" bir kural olabilir. Bu yöntemle ilgili sorun, uygun bir kurallar dizisi oluşturmaktır. Kurallar çok genel veya çok ayrıntılıysa, sistem yanlış eşleşme verebilir. Birden fazla yüzün olduğu görüntülerde de hata oranı artabilmektedir. Ayrıca bu tür sistemlerin tüm ten renkleri için doğru sonuç vermediği bilinmektedir.
- **Şablon Eşleme (Template Matching):** Bu yöntemde, bir şablon eşleştirme algoritmasıyla, yüzleri bulmak veya algılamak için parametreleri önceden tanımlanmış şablonlar kullanılır. Sistem, girilen fotoğraflarla şablonlar arasındaki korelasyonu ölçer. Örneğin şablon; bir insan yüzünün burun, ağız, gözler ve yüz çevre bölgelerine bölündüğünü gösterebilir. Ayrıca, sadece kenar algılama yöntemi kullanılarak

Temel Bir Yüz Tanıma Sistemi Nasıl Çalışır?

- **Görüntü alınır:** Kamera, tek başına veya kalabalık içinde bir yüzün görüntüsünü algılar ve bulur. Görüntü, doğrudan karşıya veya profile bakan kişiyi gösterebilir.
- **Yüz analizi yapılır:** Özel yazılım yüzün geometrisini okur. Kilit faktörler; gözlerin arasındaki mesafe, göz yuvalarının derinliği, alından çeneye olan mesafe, elmacık kemiklerinin şekli, dudakların biçimi, kulaklar ve çenenin çevresidir. Amaç, yüzünüzü ayırt etmek için yüz simgelerini belirlemektir.
- Görüntünün **gri tonlaması** alınır ve kırpılır.
- **Görüntü veriye dönüştürülür:** Yüz karşılaştırma sonuçlarının alınabilmesi için görüntü bir şablona dönüştürülür. Bu aslında matematiksel bir formüldür. Elde edilen koda "yüz izi" veya "yüz şablonu" denir. Parmak izlerinin benzersiz olması gibi, her kişinin kendi yüz izi vardır.
- **Eşleşme bulunur:** Şablonun diğer şablonlarla karşılaştırılması için gelişmiş bir algoritma kullanılarak görüntü aranır ve eşleşmeler bulunur. Çoğu YTT, üç boyutlu görüntülerden ziyade iki boyutlu görüntülere dayanır çünkü iki boyutlu bir görüntüyü genel fotoğraflarla veya bir veritabanındakilerle daha uygun şekilde eşleştirebilir[7],[11].

kenarlardan bir yüz modeli oluşturulabilir. Bu yaklaşımın uygulanması kolaydır ancak yüz algılamak için yetersizdir.

- **Özellik Tabanlı Yüz Algılama (Feature Based Facial Recognition):** Özellik tabanlı yöntem, yüzün yapısal özelliklerini çıkararak yüzlerin yerini belirlemektir. Görünüm tabanlı bir algoritma, bir yüzün nasıl görünmesi gerektiğini "öğrenmek" için bir dizi "eğitici", yani sınıflandırılabilecek ve modelleme çıkarılabilecek görüntü kullanır. Buradaki fikir, içgüdüsel yüz bilgimizin sınırlarının üstesinden gelmektir. Genel olarak, bu yöntem, yüz özelliklerini belirlemek için makine öğrenmesi ve istatistiksel analize dayanır. Ayrıca, daha önce bahsedilen yöntemlerden daha güçlüdür. Birden fazla yüzün olduğu fotoğraflarda yüzde 94'e kadar başarılı sonuç verebilmektedir.
- **Görünüm Tabanlı Yüz Algılama (Appearance Based Facial Recognition):** Bu yöntemde, yüz modellerini bulmak için bir dizi şablon (temsili eğitim) yüz görüntüsü kullanılır. Yüz görüntülerinin ilgili özelliklerini bulmak ve onlardan özellikler çıkarmak için makine öğrenmesi ve istatistiksel analize ihtiyaç duyar. Görünüm tabanlı yüz algılama, özellik tabanlı yaklaşımdan daha ileri bir yöntemdir ve hata oranı çok daha düşüktür. Bu yöntem aynı zamanda yüz tanıma için öznitelik çıkarmada da kullanılır.
- **Video İşleme (Harekete Dayalı Yüz Algılama):** Video görüntülerinden yüz tanıma yöntemidir. Videolarda kişilerin hareketi kılavuz olarak kullanılabilir. Belirli bir yüz hareketi yanıp sönüyor, bu sayede yazılım, bir yanıp sönme düzeni belirleyebiliyorsa yüzü belirleyebilir. Genişlemiş burun delikleri, kalkık kaşlar, kırışmış alınlar ve açık ağızlar gibi diğer hareketler de bir yüzü işaret edebilir. Bir yüz algılandığında ve belirli bir yüz modeli belirli bir hareketle eşleştiğinde, model yüzün üzerine yerleştirilir ve yüz izlemenin daha fazla yüz hareketini algılaması sağlanır.

2.3 Yüz Tanıma Sistemlerinin Sivil Dünyada Kullanım Alanları

Genel olarak, yüz tanıma sistemleri iki farklı görevden birini gerçekleştirmek için kullanılabilir: doğrulama veya kimliğini saptama.

Doğrulama (1:1 eşleşme olarak da bilinir), bir kişinin, söylediği kişi olduğunu doğrulamak için kullanılır. Örneğin, bir kişi akıllı telefonunun kilidini açmak, bir bankacılık uygulamasında oturum başlatmak veya uçağa binerken kimliğini doğrulamak için yüz tanımadan yararlanır. Giriş sırasında bir kişinin yüzünün örnek bir görüntüsü alınır ve daha sonra olduğunu iddia ettiği kişinin bilinen bir görüntüsüyle karşılaştırılır. Yüz tanıma sistemleri, kişiler genellikle tarandığını bildiği ve kameraların yüzlerinin görüntüsünü net biçimde alabilmesine izin verdikleri için, doğrulama görevlerinde genellikle isabetli sonuçlar vermektedir.

Kimliğini saptama ise, yazılımın bilinmeyen bir yüzü alıp bilinmeyen kişinin kimliğini belirlemek için, bilinen yüzlerden oluşan geniş bir veritabanıyla karşılaştırmasıdır. Tanımlama, tarandığını bildiği için "işbirliği yapan" veya bilmediği için "işbirliği yapmayan" kişiler üzerinde kullanılabilir. Uzaktan kimlik tespiti, güvenlik kamera görüntülerinden şüphelilerin belirlenmesi, kayıp kişilerin veya kaçırılanların takip edilmesi ve özel sektör hizmetlerinin iyileştirilmesinde kullanılabilir. Uzaktan kimlik tespiti sistemleri, doğrulama sistemlerine kıyasla daha düşük doğruluğa sahiptir çünkü sabit kameraların halka açık alanlarda serbestçe hareket eden bireylerin tutarlı, yüksek kaliteli görüntülerini alması daha zordur.

2019'da yapılan bir pazar araştırmasına göre dünyada yüz tanıma sistemleri pazarının 2019-2024 döneminde yıllık ortalama yüzde 16 büyüyeceği ve 2024'te yedi milyar dolar büyüklüğe ulaşacağı tahmin edilmiştir[14]. Yüz tanıma sistemleri dünya genelinde özellikle savunma ve güvenlik amaçlı olarak kullanılmaktadır. Ancak sivil alanda da kullanımı hızla yaygınlaşmaktadır.

2.3.1 Kapalı Mekânlar ve Açık Hava Etkinliklerinde Kalabalıkların Yönetimi

Yüz tanıma sistemleri kapalı mekânlar veya açık havada yapılan konser, spor müsabakaları, dini etkinlikler, siyasi mitingler ve benzeri büyük kalabalıkların toplandığı alanlarda kullanılmaya başlanmıştır.

Örneğin pandemi koşulları nedeniyle 2021'de yapılabilen Tokyo 2020 Olimpiyat Oyunları, yaygın biçimde yüz tanıma sisteminin kullanıldığı ilk olimpiyat olmuştur. Seyircisiz oyunlar sırasında sporcular, hakemler, yöneticiler ve gazeteciler müsabakaların olduğu alanlara, maskeli olsalar bile, yüz tanıma teknolojisiyle girmiş ve böylece güvenlik üst düzeyde sağlanmıştır[15].

YTT, diğer izleme ve gözetim teknolojileriyle birlikte kalabalıkların yönetiminde de kullanılmaktadır. Örneğin Suudi Arabistan'ın Mekke Bölgesi Kalkınma Otoritesi (MRDA), hacı adaylarının güvenliğini artırmak için bir kalabalık kontrol sistemi oluşturmuştur. Veriler, kimlik bilgilerini içeren bir bileklik, özel sağlık gereksinimleri ve bir GPS aracılığıyla toplanmaktadır. Ayrıca kutsal mekânlarda gerçek zamanlı video görüntüleri toplamak ve analiz etmek için güvenlik kameraları kurulmuştur. Kameralar izdiham oluşabilecek noktalarda hacı adaylarının trafiğini düzenlemenin yanı sıra kayıp hacı adaylarının tespitinde de kullanılmaktadır[16].

Yüz tanıma kalabalık mekânlarda kişisel amaçlarla suçluların ve suç şüphelilerinin tespiti için de kullanılmaktadır. Örneğin: Amerikalı şarkıcı Taylor Swift'in 2018'de bir konserinde, rahatsız eden kişileri tespit edebilmek için yüz tanıma teknolojisinden yararlandığı belirtilmektedir[17].

2.3.2 Alışveriş Merkezleri, Büyük Mağazalar ve Kalabalık İşyerleri

Özel sektör işyerleri müşteri deneyimini artırma ve güvenliği sağlamak için yüz tanıma teknolojisinden yararlanabilmektedir.

Yüz tanıma yazılımı, mağaza hırsızlığına karşı etkili bir önleyici tedbir olabilir. İşletme sahipleri, bilinen veya şüphelenilen hırsızları belirlemek için yazılımı ve güvenlik kameralarını kullanabilir ve kameraların varlığı, ilk etapta hırsızlığı caydırabilir.

Yüz tanıma, bilinen hırsızların, organize perakende suçlularının veya dolandırıcılık geçmişi olan kişilerin mağazalara ne zaman girdiğini belirlemek için kullanılır. Bireylerin fotoğrafları, büyük suçlu veritabanlarıyla eşleştirilebilir, böylece potansiyel olarak bir tehdit oluşturan kişiler mağazaya girdiğinde kayıp önleme ve perakende güvenlik uzmanları bilgilendirilebilir. Bu tür sistemler perakende zincir mağazalarında yaygın olarak kullanılmaktadır. ABD'de yapılan araştırmada, aralarında "kullanmadığını" iddia edenler de olmak üzere 60'tan fazla zincir mağazanın yüz tanıma sistemi kullandığı tespit edilmiştir[18].

Teknoloji, müşteriler için perakende deneyimlerini iyileştirme potansiyeli sunmaktadır. Örneğin mağazalardaki yüz tanıma sistemleri müşterileri tanıyabilir, satın alma geçmişlerine göre ürün önerilerinde bulunabilir ve onları doğru yöne yönlendirebilir[19]. "Yüzden ödeme" teknolojisi, alışveriş yapanların daha yavaş ödeme yöntemleriyle uzun ödeme sıralarını atlamasını sağlayabilir. Örneğin uluslararası bir restoran zinciri 2017 yılından beri Çin'in Hangzhou kentinde müşterilerine yüzleriyle ödeme imkânı vermektedir[20].

2.3.3 Bankacılık

Bankacılık alanında yüz tanıma teknolojisine, mali suçlara karşı güvenliğin ve müşteri deneyiminin artırılması amacıyla başvurulmaktadır.

Güvenlik açısından YTT bankalara, olay öncesi ve sonrası olarak iki alanda destek verebilmektedir. YTT, gelişmiş video analitik teknolojisinin desteğiyle banka şubeleri ve ATM makinelerinin güvenliğini artırabilmektedir. Şubeler veya ATM'lerin pek çoğunda kameralar bulunmaktadır. Bunların görüntülerini takip etmek veya işleyebilmek için video analiz programları geliştirilmiştir. Bu programlar banka kayıtlarında bulunmayan şüpheli kişilerin duygu (stres) analizini yapabilmekte ve güvenlik birimlerini haberdar edebilmektedir. Olay sonrasında ise videoların hızla işlenerek, şüphelilerin kimliklerinin tespitine ilişkin her türlü verinin elde edilmesine yardımcı olabilmektedir.

Bankalar müşterilerinin bankacılık işlemlerini daha güvenli ve hızlı biçimde yapabilmesi için de YTT'ye başvurabilmektedir. Öyle ki banka kartları ve imzalar yakın gelecekte yerini yüz tanımaya bırakabilir. Yüz tanıma biyometrik çevrimiçi bankacılığa imkân tanımaktadır. Müşteriler tek seferlik şifreler kullanmak yerine akıllı telefonlarına veya bilgisayarlarına bakarak işlemleri yetkilendirilebilmektedir.

YTT'de bilgisayar korsanlarının eline düşebilecek şifreler ve imzalar yoktur. Bu da müşteri güvenliğini en üst düzeye çıkarabilmektedir. Ancak kişinin yüzünü, sesini ve jestlerini taklit edebilen "deepfake"[21] uygulamaları endişe konusudur. Teknoloji şirketlerinin bankalarla birlikte bu tür sahtekârlıkların önüne geçecek uygulamalar üzerinde çalıştığı belirtilmektedir.

2.3.4 Pazarlama ve Reklamcılık

Bir işletme veya kuruluş için pazarlamada YTT kullanmanın birçok faydası bulunmaktadır. Yüz tanıma, pazar araştırmacılarının yüz ifadelerini uygun ölçekte analiz etmelerine olanak tanır. Odak grupları ve çağdaş sinirbilim teknikleri gibi geleneksel analiz araçlarıyla yapılan pazar ölçümlerine katılan denekler önyargılı olabilir veya gerçek fikirlerini paylaşma konusunda isteksiz olabilir. Yüz tanıma, bir katılımcının tarafsız ve filtrelenmemiş duygusal tepkilerini göze batmayan bir şekilde yakalar. Duygunun çeşitli boyutlarının (değerlik, dikkat, ifade/yoğunluk) incelenmesi ve çeşitli gizli duyguların (zevk, konsantrasyon, şaşkınlık, hoşlanmama ve şüphe) incelenmesi yoluyla markalar tüketicilerini daha iyi anlayabilir ve daha güçlü bir duygusal bağlantı kurabilir.

Yüz tanıma verilerinin analizi yoluyla bir marka, paylaşım davranışını, marka sadakatini ve satınalma kararını artırabilecek belirli duyguları uyandırarak tüketicilerle olan bağlantıları iyileştirebilir. YTT, bilinçli pazarlama ve

iş kararları vermesi için bir markayı veya kuruluşu değerli verilerle güçlendirebilir. Örneğin ABD'de bir dondurulmuş gıda firması, yeni ürünlerini test etmek için partiler düzenlemiş ve katılımcıların görüntülerinden ürüne karşı gerçek tepkilerini ölçmeye çalışmıştır[19].

Medya şirketleri ayrıca izleyicilerin film fragmanlarına veya dizilerin pilot bölümlerine karşı tepkilerini test etmek için yüz tanıma kullanmaktadır. YTT insanların günlük hayatta reklamlara tepkilerini ölçmek için de kullanılmaktadır. Örneğin 2017'de, Londra'daki Piccadilly Circus Meydanı'ndaki reklam ekranının arkasına yüz tanıma özellikli kameralar yerleştirilmiştir. Sistem kişilerin yaşını ve cinsiyetini ve ayrıca reklam tepkilerini ölçebilmektedir[22].

Ancak bu tür yöntemlere karşı tepkiler de giderek artmaktadır. YTT pazarlama için kullanıldığında, yüz tanıma yazılımı karşıtları, insanların işletmeler veya kuruluşlar tarafından manipüle edildiğini ve bunlardan yararlanıldığını iddia etmektedir. Ayrıca YTT, görüntüleri saklanan ve pazarlama amacıyla kullanılan kişiler için risk oluşturmaktadır. Zira verileri saldırıya uğrayabilir ve izinsiz olarak kullanılabilir.

2.3.5 Sağlık Hizmetleri

YTT sağlık alanında giderek daha fazla kullanılmaktadır. COVID-19 pandemisi sektörde YTT'nin kullanımı açısından bir dönüm noktası olmuştur. Pandemi ile birlikte YTT, diğer biyometri türleri ile birlikte dijital sağlık hizmetlerinden yararlanılması, salgınların önlenmesi, vücut ısısının ölçümü ve maskeli kişilerin kimliğinin tespitine kadar pek çok durumda kullanılmıştır. Örneğin Çin'de henüz pandemiye dönüşmeden önce salgını kontrol altına almak için temasın azaltılması amacıyla sağlık personeli ve diğer görevlilerin kimlik doğrulaması yüz tanımlama ile yapılmış, kamuya açık alanlar ve toplu taşımada maske takmayanlar bu yolla tespit edilmiştir. Söz konusu alanlarda ateş ölçümleri için bile yüz tanıma teknolojisinden yararlanılmıştır[23].

YTT sağlık hizmetlerinin vazgeçilmez öğelerinden biri hâline gelmiştir. Sağlık profesyonelleri tedavi gören hastaları artık yüz tanıma yöntemiyle izleyebilmektedir. Örneğin AiCure, insanların ilaçlarını reçete edildiği gibi almasını sağlamak için YTT'den yararlanan bir uygulama geliştirmiştir[24]. Özellikle destekli yaşam alanlarında ve Alzheimer, bunama veya herhangi bir tür bilişsel bozukluktan muzdarip hastalar için yüz tanıma büyük önem taşımaktadır. Sağlık çalışanları söz konusu hastalar üzerinde kimliği olmadan bir tesisten uzaklaşırsa, yüz tanıma, onları hızlı bir şekilde tanımlamaya ve güvenli hâle getirmeye yardımcı olabilir. STM ThinkTech'in "Sağlıkta Dijitalleşmenin Önündeki Yol Haritası" başlıklı Araştırma Raporunda bahsedildiği üzere YTT, günümüzde büyük oranda dijitalleşen[25] dijital sağlık hizmetlerinin geleceğinde önemli bir rol oynayabilir. Bilim insanları ve bilişim teknolojileri firmaları sağlık hizmeti sağlayıcıları için hasta kayıtlarına erişmek[26], hasta kaydını kolaylaştırmak[27], hastalarda duygu ve acıyı tespit etmek[28] ve hatta belirli genetik hastalıkları tespit edebilmek[29] amacıyla YTT'den yararlanmak için araştırmalar yürütmektedir.

2.3.6 Seçimler ve Oylamalarda Kullanımı

YTT'nin seçimlerde kullanılarak seçim güvenliğinin en üst seviyeye çıkarılması da gündemdedir. ABD'de Batı Virginia eyaletinde 2018 yılında yapılan ara seçimlerde YTT özellikli bir akıllı cep telefon uygulamasıyla oy vermek mümkün kılınmıştır. Uygulama kullanıcının yüzünü taramakta ve kullanıcının daha önce kaydettirdiği yüzü, parmak izi ve diğer biyometrik verilerle karşılaştırarak oy kullanmasına izin vermektedir. Uygulama blokzincir teknolojisiyle oylamayı uçtan uca şifrelemekte ve olası müdahaleleri engelleyebilmektedir[30]. Sistem daha sonra başka eyaletlerde de denenecektir.

2.3.7 Eğitim

Yüz tanıma teknolojisinin eğitim kurumlarında kullanılması da tartışmalı bir konudur. Teknoloji şirketleri yüz tanıma sistemleri sayesinde eğitim binaları ve kampüslerinde güvenliğin sağlanabileceğini, sınav yolsuzluklarının (kopya, başkası yerine sınava girme vb.) önüne geçilebileceğini, derslere katılımın takip edilebileceğini ve hatta eğitimcilerin öğrencilere ilgisini yüz ifadelerinden ölçebileceğini ileri sürmektedir[31].

Özellikle güvenlik ve takip amaçlı sistemler dünyanın çeşitli ülkelerindeki okullarda kullanılmaya başlanmıştır. ABD'de son yıllarda artan okul saldırılarından ötürü, sadece kimlikleri değil sıra dışı davranışları da tespit eden sistemlere yönelik ilgi mevcuttur[32]. Çin'deki bazı eğitim kurumları, öğrencilerin derslere devamını sağlamak için yüz tanıma özelliğini kullanmaktadır[33].

COVID-19 pandemisi kısıtlamalarının ardından kısmen de olsa yüz yüze eğitime dönen eğitim kurumlarının temasın azaltılması amacıyla kimlik kartları, imza veya parmak izi yerine YTT'den daha fazla yararlanmak için hazırlık yaptığı belirtilmektedir. Öte yandan bu uygulama diğer alanlarda olduğu gibi; eğitimde de ayrımcılık, özel hayatın gizliliği, kişisel verilerin güvenliği ve gözetimi kurumsallaştırma gibi nedenlerle eleştirilmekte hatta yasaklanması önerilmektedir[34].

2.3.8 Konutlar ve Araçların Güvenliği

Konutlar ve araçlarda anahtar yerine YTT'den yararlanılması da gündemdedir. New York[35] ve Moskova'da[36] bazı sitelerin anahtar yerine kimlik tespiti için bu sistemi kullanmaya başladığı bilinmektedir.

Bazı otomotiv üreticileri de otomobil anahtarları yerine yüz tanımayı kullanmak üzere testler yürütmektedir[37]. Buna göre YTT araca erişmek ve aracı çalıştırmak için anahtarın yerini alabilecek. Ayrıca araç, sürücülerin koltuk ve ayna konumları ile radyo istasyonu ön ayarlarına ilişkin tercihlerini hatırlayabilecektir.

2.3.9 Bağımlıların İzlenmesi

Yüz tanıma, bağımlılık gibi psikolojik sorunların önlenmesinde de yer bulmaya başlamıştır. Örneğin Çin'de çocukların online video oyun alışkanlıklarının sınırlanması için hükümet tarafından yayınlanan yönergenin ardından ülkenin en büyük online oyun şirketi Tencent, ekran önünde belirlenenden fazla süre geçiren çocukları tespit etmek için YTT'den yararlanmaktadır[38].

YTT, kumar bağımlılarının kumarhanelere girişinin engellenmesi veya belli sınırlamalar içinde bu tesislerde bulunması için de kullanılabilmektedir. Avustralya'da 200'den fazla kumarhanede bu tür izleme alarm sistemi kurulmuştur[39].

Çin'in Şangay kentinde, özellikle sakinleştirici ve psikiyatrik ilaçların aşırı kullanımının önüne geçmek için bu ilaçların satıldığı eczane ve diğer satış noktalarında alıcılardan yüzlerini tarayarak kimliklerini doğrulamaları istenmeye başlanmıştır[40].

2.3.10 Hayvancılık

YTT hayvancılıkta da uygulanmaya başlanmıştır. Çin'de bazı domuz çiftliklerinin hayvan yüz tanıma sistemi kullandığı belirtilmektedir. Sistem hayvanların açlık ve stres seviyelerini de ölçebilmekte ve böylece yemin daha verimli kullanılmasını sağladığı gibi olası hastalıklar önlenebilmektedir. Sistemin "hayvan refahını" artırarak hayvancılığın verimini yükselttiği de kaydedilmektedir[41]. Yöntemin Avrupa'da da kullanımı için araştırmalar yapılmaktadır[42].

2.4 Yüz Tanıma Sistemlerinin Sağladığı Kolaylıklar

Yüz tanıma, çok sayıda avantaj sağlamaktadır. Bunlardan bazıları aşağıda sıralanmıştır:

- **Verimlilik:** Yüz tanıma yazılımı, yalnızca insanlar tarafından yapılan manuel aramalara kıyasla, tanımlama ve doğrulama sürecinin hızını artırma potansiyeline sahiptir.
- **Ölçek:** YTT, analiz edilebilecek veri miktarını da artırabilir. Örneğin, büyük kalabalıklarda tanımlama veya büyük bir veritabanı kullanarak görüntü karşılaştırması yapılabilir.
- **Kişisel Güvenlik ve Kamu Güvenliği:** Devlet düzeyinde, yüz tanıma, teröristleri veya diğer suçluları tanımlamaya yardımcı olabilir. Pahalı olan ve üretilmesi bir laboratuvar günü sürebilen DNA kanıtının aksine, bir sistem kurulduktan sonra yüz tanıma çok az ek yük gerektirir. Göreceli kullanım kolaylığı, emniyet teşkilatlarının bu teknolojiyi günlük işlerinin bir parçası hâline getirmelerine olanak tanır.

YTT ayrıca, otomatik bir süreçle kalabalıklar arasındaki şüphelileri seçerek, potansiyel önyargıyı azaltmaya ve yasalara uyan vatandaşlarla ilgili duraklamaları ve aramaları azaltmaya yardımcı olabilir. Örneğin Türkiye'de SimBT firması tarafından geliştirilen "Tak-Bul" adlı artırılmış gerçeklik gözlüğü jandarma teşkilatı tarafından kullanılmaya başlanmıştır. "Tak-Bul" ve araçları birkaç saniye içinde sadece yüzlerine, kimlik kartlarına ve araçların plakalarına bakarak kişilerin tespit edilmesini ve tanınmasını sağlayabilmektedir[43]. Artırılmış gerçeklik uygulamasının yanı sıra yüz tanıma özelliğine de sahip olan Tak-Bul, kimliklerdeki resimleri tanımlayarak kişinin aranılanlar listesinde olup olmadığına dair uyarıda bulunabilmektedir.

Kişisel düzeyde, yüz tanıma, kişisel cihazları kilitlemek ve kişisel güvenlik kameraları için bir güvenlik aracı olarak kullanılabilir. Yüz tanıma, izinsiz girişleri izlemeyi kolaylaştırır. Bir yüz tanıma sisteminin varlığı, özellikle adi suçlar için caydırıcılık işlevi görebilir. Fiziksel güvenliğin yanı sıra siber güvenliğin de faydaları vardır. Şirketler, bilgisayarlara erişmek için parolaların yerine yüz tanıma teknolojisini kullanabilir. Teoride, şifrede olduğu gibi çalınacak veya değiştirilecek hiçbir şey olmadığı için teknoloji siber saldırıya maruz kalamaz.

- **Alışveriş ve Günlük Yaşamda Daha Fazla Hız ve Konfor:** YTT teknolojisi perakende sektöründe hız ve konfor yaratarak fayda yaratabilir. Siber saldırılar ve gelişmiş bilgisayar korsanlığı çağında, şirketlerin hem güvenli hem de hızlı teknolojilere ihtiyacı vardır. Yüz tanıma, kişilerin kimliğinin hızlı ve doğru bir şekilde doğrulanmasını sağlar. Teknoloji yaygınlaştıkça, müşteriler mağazalarda kredi kartlarını veya nakit paralarını kullanmak yerine yüzleriyle ödeme yapabilecektir. Parmak izi veya diğer güvenlik önlemlerinde olduğu gibi yüz tanıma için herhangi bir temas gerekmediğinden yüz tanıma hızlı, otomatik ve sorunsuz bir doğrulama deneyimi sunar.
- **Diğer Teknolojilerle Entegrasyon:** Çoğu yüz tanıma çözümü, diğer biyometrik güvenlik sistemi yazılımıyla uyumludur. Bu, onu uygulamak için gereken ek yatırım miktarını sınırlar.

2.5 Yüz Tespit Sistemlerinin Zayıf Yönleri ve Endişeler

Yüz tanıma sistemleri 2015-2020 döneminde hızlı bir gelişme göstermekle birlikte kusursuz değildir. Özellikle veritabanlarında bulunmayan kişilerin kimliklerinin tespitinde birtakım zafiyetlere sahiptir ve hatalı sonuçlar verebilir. Bu hatalar vahim sonuçlar doğurabilir. YTT ve kullanımına ilişkin standartlar ve etik kurallar üzerinde henüz uzlaşıya varılmamış olması da bu teknolojiye karşı güvensizliği beslemektedir. Bu bölümde söz konusu teknolojinin zayıf yönleri ile kullanımına ilişkin tartışmalar ele alınacaktır.

2.5.1 Yüz Tanıma Sistemlerinin Zayıf Yönleri

Yüz tanıma sistemlerinin zayıf yönlerinin başında belli koşullarda yüksek hata oranı gelmektedir. Hata oranı sistemin verdiği sonuçlarda hata payını ifade etmektedir. Yüz tanıma sistemleri insanların kimliklerini tespit yetenekleri, zayıf aydınlatma, düşük kaliteli görüntü çözünürlüğü ve yetersiz görüş açısı gibi zorlu koşullar altında farklılık gösterir[7].

2.5.1.1 Yüz Tanımada Hata Türleri

Literatürde yüz tanıma sistemlerine ilişkin hatalar "Yanlış Negatif" ve "Yanlış Pozitif" olarak iki türde ele alınmaktadır.

"Yanlış Negatif", yüz tanıma sisteminin bir kişinin yüzünü, bir veritabanında bulunan bir görüntüyle eşleştiremediği zamandır. Başka bir deyişle, sistem bir sorguya yanıt veremez ve "sıfır" sonuç alınır.

Yüz tanıma sistemlerinden sonuç alınamamasının belli sebepleri vardır. Yüzü belirlemeyi engelleyici durumlar ve kişinin hareket hızı negatif hata oranını artırabilmektedir. Örneğin özellikle pandemi döneminde pek çok yerde kullanımı zorunlu hâle gelen maskeler yüz tanımayı hayli zorlaştırmaktadır. ABD Ulusal Standartlar ve Teknoloji Enstitüsünün (NIST) Temmuz 2021'de yayınladığı bir rapora göre, yüz tanıma yazılımlarından bazıları maske takan kişilerin yarısının kimliğini tespit etmekte güçlük çekmektedir[44]. Rapora göre bazı yazılımlar, maske yüzün önemli bir kesimini kapsarsa yüzü ayırt etmekte bile güçlük çekmektedir[45].

"Yanlış Pozitif" ise, yüz tanıma sisteminin bir kişinin yüzünü bir veritabanındaki görüntüyle eşleştirmesi, ancak bu eşleşmenin aslında yanlış olması durumudur. Yanlış pozitif sonuçlar olası sonuçları nedeniyle büyük tartışma yaratmaktadır ve bu tür sistemlerin güvenilirliğine gölge düşürmektedir. Medyaya yansıyan vakalar bu güvensizliği körüklemektedir. Örneğin 2018 yılında ABD medyasında çıkan bir habere göre Amazon'un yüz tanıma programı Rekognition, 29 ABD Kongresi üyesini suçlularla eşleştirmiştir[46].

Yüz tanıma algoritmalarının hata oranları bazı koşullarda artmaktadır. Örneğin önde gelen yüz tanıma algoritmalarından birinin sabıka kayıtları fotoğraflarında hata oranı yüzde 0,1 düzeyindeyken, açık alanda çekilmiş görüntülerde bu oran yüzde 9,3'e kadar yükselmektedir[47].

Kimliği tespit edilmeye çalışılan kişilerin yaşlanması da hata oranını artırmaktadır. Örneğin veritabanında bir kişinin belli bir yaştaki yüzü kayıtlıysa 20 yıl sonra kişinin yeni hâli farklı olabileceğinden hata oranı yükselecektir.

Aranılan kişinin yüz şablonu veritabanında bulunmuyorsa, sistemin hâlâ bir veya daha fazla potansiyel eşleşme üretmesi ve "yanlış pozitif sonuçlar" oluşturması olasılığı yükselecektir. Örneğin İngiltere'de Londra Polisi 2018 ve 2019 boyunca yüz tanıma denemeleri yapmış, polis kontrollerinde durdurulan 42 kişiden sadece sekizinin arandığı doğru olarak belirlenebilmiştir[48].

Bu tür pozitif yanlışlar, adli hatalara yol açabilir. Kişiler işlemedikleri suçlara ilişkin suçlamalarla karşı karşıya kalabilir. Yapılan araştırmalara göre, yüz tanıma yazılımları özellikle azınlıklar, kadınlar ve gençlerin yüzlerini tanımlamakta güçlük çekmektedir[49]. Bu durum özellikle ABD'de büyük sorun yaratmaktadır. 2020 yılında George Floyd işlemediği bir suçtan, YTT "Yanlış pozitif" sonuç verdiği için gözaltına alınırken gördüğü kötü muamele sonucu yaşamını yitirmiş, bu trajik ölüm ülke genelinde ve hatta dünyanın pek çok ülkesinde büyük protesto gösterilerine yol açmıştır. Gösteriler üzerine aralarında Amazon, Microsoft ve IBM'in olduğu teknoloji devleri yüz tanıma teknolojisini güvenlik güçlerine satmayacağını duyurmak zorunda kalmıştır[50].

Ayrıca söz konusu hataların tekrarlanma olasılığı yüksektir. Yüz tanıma verileri genellikle, bir yargıç suçlu veya masum olup olmadığına karar verme şansı bulamadan, tutuklanma üzerine çekilen sabıka fotoğraflarından elde edilir. Tutuklanan kişiye karşı hiçbir suçlama yapılmamış olsa bile, söz konusu fotoğraflar genellikle veritabanından asla kaldırılmaz. Veritabanındaki kişi sayısı arttıkça yüz tanıma daha da kötüleşmektedir. Bunun nedeni, dünyadaki birçok insanın birbirine benzemesidir. Benzer yüzlerin olasılığı arttıkça, eşleştirme doğruluğu azalır.

2.5.2 Yüz Tanıma Teknolojilerine İlişkin Diğer Endişeler

Her yeni teknolojide olduğu gibi yüz tanıma teknolojisinin yaygınlaşmasıyla birlikte de birtakım endişeler ortaya

çıkmaktadır. Özel hayatın ve kişisel verilerin gizliliğinin ihlali, suiistimaller, suç amaçlı siber saldırılar ve insan hakları ihlalleri YTT ile de birlikte anılmaktadır.

YTT, kötüye kullanım potansiyeli nedeniyle yaygın endişeye neden olmaktadır. Yüz tanıma sistemlerinin hızla artan doğruluğu, yanlış tanımlamadan kaynaklanan zararların önlenmesine yardımcı olacaktır. Ancak bu iyileşme söz konusu teknolojiyi, kötüye kullananlar için daha çekici hâle getirerek diğer riskleri de artırabilir.

Bu nedenle kamu otoriteleri bu alanda tedbirlere başvurmak zorunluluğu hissetmektedir. Nitekim Avrupa Birliği Komisyonu 2020 yılında, YTT'nin kamusal alanlarda kullanımını yasaklamayı düşündüğünü bildirmiştir[51]. Yasaklama düşüncesinin ardında bu teknolojinin kötüye kullanımı olasılığı yatmaktadır. Avrupa Komisyonuna göre bu teknolojinin kullanımına izin verilmeden önce Avrupa'da mahremiyet ve bilgi koruma haklarının daha sıkı korunmasını sağlayacak düzenlemelerin getirilmesi gerekmektedir.

Yüz tanıma teknolojisinin kötüye kullanımına ilişkin kaygılardan bazıları şunlardır:

- **Kitlesel Takip:** Her yerde bulunan video kameralar, yapay zekâ ve veri analitiği ile birlikte yüz tanımanın kullanılmasının, bireysel özgürlüğü kısıtlayabilecek toplu gözetleme potansiyeli yarattığından endişe edilmektedir. YTT, hükümetlerin suçluları takip etmesine izin verirken, aynı zamanda sıradan ve masum insanları her an takip etmelerine de izin verebilir. Toplu takipler güvenlik güçlerinin olası insan hakları ihlallerini ağırlaştırabilir ve barışçıl protesto ve gizlilik haklarını zayıflatabilir[52].
- **Etik Sorunlar ve Mahremiyetin Korunması:** Kamu ve özel kuruluşlar, yüz tanıma teknolojilerini daha fazla kullanmaya başladıkça bunlara ilişkin etik sorunlar ve mahremiyetin ihlali kaygıları ortaya çıkmaktadır. Bunların çoğu, veri kullanımlarıyla ilgili genel sorulardır. Örneğin, verilerin nasıl toplandığı etik bir sorundur. Yüz tanıma teknolojisinin geliştirilmesi ve uygulanması sırasında toplanan görüntülerin büyük bir bölümü ilgili kişilere haber verilmeden, çoğunlukla başta sosyal medya olmak üzere çevrimiçi ortamlardan toplanmaktadır. Ayrıca veri toplanırken çeşitliliğin sağlanamaması, bunlar üzerine geliştirilecek algoritmaların yanlı ve önyargılı olarak geliştirilmesine neden olabilmektedir. Toplanan görüntülere kimlerin erişebileceği, bunların nasıl ve hangi amaçlarla paylaşılacağına dair net ve genel düzenlemelerin olmaması da mahremiyet ve kişisel verilerin korunması açısından kaygıları artırmakta ve bu tür sistemlere güveni zedelemektedir.
- **Ayrımcılık:** Araştırmalar, YTT sistemlerinin bazı yüzleri; ten rengi, etnik aidiyet ve toplumsal cinsiyet gibi önemli özelliklere göre farklı doğruluk oranlarıyla işlediğini pek çok kez ortaya koymuştur. Örneğin, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ırksal aidiyet, yaş ve cinsiyetin ABD'de kullanılan başlıca YTT sistemlerinde hata paylarını ölçmüş, algoritmaların "yanlış pozitiflik" oranlarının yüksek olduğunu saptamıştır[53]. Ayrıca bazı YTT ve uzaktan biyometrik tanıma uygulamalarının, insanları yasal kimlikleriyle ilişkilendirmedikleri için kamusal alanlarda insanları ayrıştırmak için ya da insanların özellikleri ve davranışları hakkında çıkarımlarda bulunmak için kullanılabileceğinden endişe edilmektedir[54]. Zira insanların cinsiyetleri, duyguları veya diğer kişilik özellikleri hakkında çıkarımlarda ve tahminlerde bulunan biyometrik sınıflandırma uygulamaları, bilimsel esaslardan uzak olacaktır. İnsani özeliklerin bilimsellikten uzak şekilde sınıflandırılması yeni adli hatalara ve mağduriyetlere neden olabilir.
- **Siber Saldırılar ve Kimlik Sahtekârlıkları:** Yüz tanıma sistemleri, iki nedenden ötürü siber saldırıların ve diğer dijital suçların hedefi olmaktadır. Birincisi, YTT suçluların ardına sığındığı anonimliği ortadan kaldırmakta, kimliğini gizli tutma veya saklama olanağını büyük ölçüde zayıflatmaktadır. İkincisi, YTT özellikle finans sektöründe kimlik doğrulamada başvurulan başlıca yöntemlerden biri hâline gelmiştir ve bu durum dijital servet hırsızlarının bu teknolojiye yönelik saldırılarının artmasına yol açmaktadır. Özellikle yüz tanıma özellikli cep telefonlarına erişim sağlanması için çok sayıda girişim olduğu belirtilmektedir. Yapılan araştırmalar genellikle güvenli bulunan bu sistemlerin, canlı bir yüz yerine yüzün basılı bir görüntüsünün veya çalıntı biyometrik özellik dosyalarının kullanılması gibi yöntemlerle yanıltılabileceğini göstermektedir[55]. Ayrıca kişilerin biyometrik şablonlarını toplayan şirketlerin veritabanlarına yönelik siber saldırı olasılığı endişe kaynağıdır. Böyle bir durumda yüz şablonlarının çıkarıldığından habersiz binlerce kişinin banka hesap bilgileri ve değerli kişisel verileri suç şebekelerinin eline geçebilir.

3. SAVUNMA VE GÜVENLİK ALANINDA YÜZ TANIMA TEKNOLOJİSİNİN KULLANIMI

Yüz tanıma teknolojisi, kimlik arama ve doğrulama için temassız bir yöntemdir. İlgili kişiyle etkileşime girmeden görüntü ve video çekilebilir, bu da yüz tanımayı verimli ve etkili bir biyometrik güvenlik yöntemi yapmaktadır. YTT, tanımlamayı yepyeni bir düzeye getirmiş ve sunduğu çözümler tüm büyük kuruluşlar tarafından bir güvenlik önlemi olarak kullanılmaya başlanmıştır. Bu bölümde YTT'nin güvenlik ve savunma alanında sunduğu olanaklar ve uygulama alanları incelenecektir.

3.1 YTT'nin Emniyet Güçleri Tarafından Kullanımı

Diğer alanlarda kullanımı hızla yaygınlaşsa da YTT çoğunlukla güvenlik güçleri, istihbarat birimleri ve sınır güvenliğinden sorumlu kuruluşlar tarafından kullanılmaktadır. Bunun başlıca nedeni güvenlik birimlerinin yüz verisi toplama araçlarına (pasaport ve kimlik fotoğrafları, şehir

güvenlik kameraları vb.) sahip olması ve kısa sürede güvenilir bir veritabanı geliştirebilecek olmasıdır.

3.1.1 Yurtiçi ve Uluslararası Güvenlikte YTT Kullanımı

Emniyet teşkilatları YTT'yi yetki sahalarındaki pek çok görevde kullanabilmektedir. Suçluların tespiti ve aranan kişilerin bulunması bunların başında gelmektedir. Emniyet teşkilatları, başka hiçbir kimlik tespit aracı olmaksızın suçluları tespit etmek ve canlı kamera görüntülerindeki yüzleri izleme listesindeki yüzlerle karşılaştırarak kayıp kişileri bulmak için yüz tanıma özelliğini kullanır.

Başta çocuklar olmak üzere kayıp şahısların ve insan ticareti mağdurlarının bulunmasında da YTT'den yararlanılır. Derin öğrenme teknolojisi sayesinde çocukların birkaç yıl sonra nasıl görüneceğini tahmin etmek mümkün hâle gelmiştir. Bu da yıllardır kayıp olsalar bile emniyet güçlerinin onları bulmasını kolaylaştırmaktadır.

Yüz tanıma nihayet farklı video dizilerinde kimliği belirsiz kişileri bulmayı ve bir suç mahallini daha iyi anlamayı mümkün kılmaktadır. 2013 Boston Maratonu bombalı saldırısı örneği bu açıdan semboliktir. Boston polisi maratonun canlı yayınlanmasına ve kentin güvenlik kameralarının bulunduğu bir noktada yaşanmasına rağmen şüphelileri tespit etmekte uzun süre zorlanmıştır. Yapılan araştırmalar söz konusu kamera görüntülerinin yapay zekâ destekli bir YTT ile incelense şüphelilerin kısa sürede tespit edilebileceğini göstermiştir[56].

Emniyet güçleri, mobil cihazlar sayesinde rutin güvenlik uygulamalarında yüz tanımayı giderek daha yaygın olarak kullanmaktadır. Polis, tutuklulardan sabıka görüntüleri toplayabilmekte ve bunları yerel, ulusal ve uluslararası yüz tanıma veritabanlarıyla karşılaştırabilmektedir. Mobil yüz tanıma, memurların akıllı telefonları, tabletleri veya diğer taşınabilir cihazları kullanarak sahadaki bir sürücünün veya yayanın fotoğrafını çekmesine ve bu fotoğrafı hemen bir veya daha fazla yüz tanıma veritabanıyla karşılaştırarak bir tanımlama girişiminde bulunmasına olanak tanır. Örneğin, Çin Elektronik Bilim ve Teknoloji Üniversitesinin geliştirdiği, bir polis aracının üstüne yerleştirilen 360 derecelik yüz tanıma kameralarının 60 m çapındaki bir çember içindeki insan kalabalığı arasından suçluları tespit edebildiği belirtilmektedir. Sistem gördüğü her yüzün cinsiyetini, yaşını ve ırkını belirleyip veritabanındaki kimliklerle karşılaştırmakta, aranan herhangi bir şahısla eşleşme olduğunda da aracı kullanan polisi uyarmaktadır[57]. Malezya'daki güvenlik güçleri yine Çin teknoloji şirketi Yitu'nun geliştirdiği yüz tanıma vücut kameralarıyla donatılmıştır. Söz konusu sistemler, güvenlik görevlilerinin "canlı vücut kameraları tarafından yakalanan görüntüleri merkezi bir veritabanından alınan görüntülerle hızla karşılaştırmasını" sağlamaktadır[58].

YTT verilerinin ulusal ve uluslararası güvenlik kuruluşları arasında paylaşımı da giderek artmaktadır. Örneğin INTERPOL, 180'e yakın ülkeden yüz görüntülerini kendi Yüz Tanıma Sistemi'nde (IFS) toplamaktadır. Otomatik bir biyometrik yazılım uygulamasıyla birlikte bu sistem, yüz özelliklerini karşılaştırarak ve analiz ederek bir kişiyi tanımlama veya doğrulama yeteneğine sahiptir. INTERPOL'ün yüz tanıma sisteminin 2016 sonunda kullanıma sunulmasından bu yana 1.000'den fazla suçlu, kaçak, ilgili kişi veya kayıp kişinin kimliğinin belirlendiği bildirilmiştir[59].

3.1.2 Havaalanları ve Sınır Kontrollerinde YTT Kullanımı

COVID-19 pandemisi nedeniyle alınan tedbirler büyük darbe indirmekle birlikte küresel turizm ve seyahat sektörü dünya ekonomisi için önemini sürdürmektedir. Dünya Seyahat ve Turizm Konseyinin (WTTC) 2019 verilerine göre, seyahat ve turizm sektörü, küresel GSYH'nın yüzde 10,3'ünü oluşturmuş ve 2019'da 330 milyon insanın ana geçim kaynağı olmuştur.

Ancak sınır geçişlerindeki bu büyük hareketlilik beraberinde terör ve suçların hızla sınırötesine aktarımını da beraberinde getirmiştir. Yasadışı göç edenler ve adaletten kaçanlar sahte pasaportlar ve diğer yöntemlerle sınırlardan geçiş yapmaya çalışmaktadır. Pandemi ile birlikte enfeksiyon taşıyanların da izlenmesi büyük önem kazanmıştır.

Bu şartlar altında bir yandan seyahatlerin hızı artaken, sınırları ve yolcu güvenliğini sağlayacak çözümler de büyük önem kazanmıştır. Sınır geçişlerinde parmak izi gibi biyometrik yöntemler öteden beri kullanılmaktadır. Fakat COVID-19 pandemisiyle birlikte temassız izleme sistemlerine ilgi daha da artmıştır.

Bu nedenle YTT, dünyadaki birçok havaalanında yaygın olarak kullanılmaya başlanmıştır. Çalışmaları 2010'lu yıllarda hızlanan biyometrik fotoğraflı pasaportların yaygınlık kazanması bu sistemlerin kullanımını kolaylaştırmıştır.

Söz konusu pasaportlar yolcuların uzun kuyrukları atlamalarına ve bunun yerine kapıya daha hızlı ulaşmak için otomatik bir e-Pasaport kontrolünden geçmelerine izin vermektedir. Söz konusu sistemin uygulaması İstanbul Havalimanı'nda 2019 yılında başlamıştır. Hızlı Pasaport Geçiş Sistemi, 18 yaşını doldurmuş, T.C. vatandaşı ve çipli pasaport sahibi olan yolculara "Hızlı Pasaport Geçiş Sistemi'" ile yolculukları esnasında zaman kazandırılmaktadır. Sistem sayesinde yolcular yüz tanıma ve parmak izi kontrollerinin ardından 18 saniye içerisinde havalimanında 16 geliş, 10 gidiş ve dört transfer alanında yer alan toplam 30 hızlı pasaport geçiş bankosundan geçebilmektedir. Geçiş yapan yolcuların pasaportlarına damga vurma işlemi ise emniyet görevlileri tarafından yapılmaktadır[60].

Yüz tanıma, yalnızca bekleme sürelerini azaltmakla kalmamakta, aynı zamanda havalimanlarının güvenliğini artırmasını da sağlamaktadır. Dünya Seyahat ve Turizm Konseyinin (WTTC) sıraladığı, yüz tanımanın önemli bir rol oynadığı Yolcu Dijital Kimlik çözümlerinin yararları Tablo 1'de verilmiştir[61]:

ABD İç Güvenlik Bakanlığı, 2023 yılına kadar yolcuların yüzde 97'sinde yüz tanımanın kullanılacağını tahmin etmektedir[62].

Ancak yeni teknolojiler de terör ve suç örgütlerinin radarına girmekte gecikmemiştir. Teknoloji, hayatı daha

Kamu Sektörü İçin Faydaları	Özel Sektöre Faydaları	Yolculara Faydaları
• Kontrol noktalarının sayısını artırmadan verimliliğini yükseltmek, • Sağlık kontrolü mekanizmalarını güçlendirmek, • Artan sınır kontrolü ve güvenlik, • Riskli yolcuların daha iyi takibi, • Personel harcamalarından tasarruf, • Altyapı üzerindeki baskının azalması.	• Yolcu sağlığını güvence altına almak, • İş akışlarında artan güvenlik, • Yolcular ve seyahat acenteleriyle sağlıklı bilgi paylaşımı, • Artan kişiselleştirilmiş müşteri etkileşimleri, • Artan varlık kullanımı (Ör: Uçaklar, otel, araba kiralama), • Operasyonlarla ilgili düşük ücretler, • Daha az veri yükümlülüğü.	• Gelişmiş seyahat deneyimi, • Kontrol noktalarındaki sürtüşmelerin ortadan kaldırılması, • Artan kişisel güvenlik, • Artan kontrol ve kişisel verilerin şeffaflığı, • Daha az veri yükümlülüğü, • Azaltılmış dolandırıcılık faaliyeti (Ör: Çalıntı kimlik vakaları, çalıntı kredi kartları).

Tablo 1: Yüz tanımanın önemli bir rol oynadığı Yolcu Dijital Kimlik çözümlerinin yararları[61]

otomatik ve kolay hâle getirirken, aynı zamanda yeni biyometrik pasaportlardaki biyometrik veriler de dahil olmak üzere, kötü niyetli kişilerin pasaportları klonlamasına veya taklit etmesine izin vermiştir. Bu yetenek, suçluların pasaporttaki bilgilerle eşleşmesi için biyometriyi manipüle edebilmeleri nedeniyle tespitten kaçmalarını sağlamıştır. Günümüzde biyometrik pasaportlar yaygınlık kazanmıştır ve bu nedenle suç şebekeleri biyometrik pasaportların kopyaları veya sahtelerini üretmek için harekete geçmiştir. Dijital suçlular biyometrik pasaportları üretirken ileri teknolojiden de yararlanmaktadır. Bu nedenle emniyet güçleri ve gümrük yetkililerinin, pasaport kontrollerinde kimlik doğrularken yeni bir yöntem bulması gerekecektir.

3.2 Askeri Alanda Yüz Tanıma Teknolojisinin Kullanımı

YTT ulusal savunma alanında da yaygınlık kazanmaya başlamıştır. Askeri bağlamda YTT'nin ana amacı, algılanan herhangi bir tehdidi tanımlamak, sınıflandırmak, doğrulamak ve gerekirse etkisiz hâle getirmektir[63].

Ancak YTT askeri alanda sadece tehdit tespiti için kullanılmamaktadır. Askeri tesislerin güvenliğinden muharebe alanlarında dost ve düşman kuvvetleri hakkında farkındalığın artırılmasına ve terörle mücadeleye kadar pek çok alanda YTT'den yararlanılmaktadır. Bu bölümde YTT'nin askeri alanda uygulamalarına göz atılacaktır.

3.2.1 Muharebe Sahasında YTT

Muharebe sahasındaki birliklerin dost ve düşman kuvvetleri birbirinden ayırabilmesi hayati önem taşımaktadır. Çatışma esnasında görüş mesafesinin düşmesi, yüksek ses ve diğer zorluklar nedeniyle birlikler arasında kopmanın yaşanması ve düşman sızmalarını engellemek için yüz tanıma ve diğer biyometrik teknikler kullanılarak uyarıcı sistemler geliştirilmeye başlanmıştır. Örneğin ABD Kara Kuvvetleri askerleri için Temel Optik Biyometrik Analiz (BOBA) adı verilen bulut bilişim tabanlı bir uygulama akıllı cep telefonuna benzer hafif cihazlara yüklenerek askerlere verilmeye başlanmıştır[64]. Yüz tanıma, parmak izi ve irisi biyometrik veri olarak kullanan cihazın sahada saniyeler içinde kişilerin kimliklerini bildirdiği belirtilmektedir.

Yüz tanıma için askeri birliklerin avantajı, disiplinli bir kişisel bilgi kayıt sisteminin olması ve bunlarda mutlaka fotoğraf bulunmasıdır. Ancak muharebe sahasında kısıtlı görüş imkânı nedeniyle düşman birliklerini tespit için daha fazlası gereklidir. Bunun için ABD Donanması Hava Muharebe Merkezi'nin (Naval Air Warfare Center -Weapons Division) Silah Bölümünden araştırmacılar, "Uyarlanabilir yüz tanıma yazılımı" geliştirmiştir. Söz konusu yazılım aşırı parlaklık, dar açı, sis vb. durumlarında alınabilen az veriye rağmen makine öğrenmesiyle kimlik tespiti yapabilmektedir[65].

3.2.1.1 Askerlerin Fiziksel ve Zihinsel Durumlarının İzlenmesi

Biyometri sadece savaşçıları tanımlamakla sınırlı değildir. Çatışma bölgelerindeki askerlerin sağlığının izlenmesi ve birliklerine sağ salim dönebilmelerinin sağlanmasında da büyük oranda yardımcı olabilir. Giyilebilir teknoloji alanındaki gelişmeler askeri üniforma, miğfer ve botlara takılabilen ve askerin sağlığının anlık olarak izlenmesini sağlayan çözümler ortaya çıkarmıştı. Özel kuvvetler ve polislerin kullanmaya başladığı üniformaya monte edilebilen kameralara yüz tanıma özelliği kazandırmak, askerin konumu konusunda sağlıklı bilgi aktarabilir. Bu da olası yaralanmalarda onun yerinin kolaylıkla tespit edilmesini, kendisine tıbbi yardım götürülmesini ya da bu askerin çatışma alanından uzaklaştırılmasını sağlayabilir. Ayrıca, yüz tanıma teknolojili otonom araçlar çatışma bölgelerindeki yaralıları ve zor durumdaki askerleri tespit ederek onların güvenli bölgelere aktarımını sağlayabilir. Yüz tanıma özellikli kameralar diğer sağlık takip sensörlerinin tespit edemeyeceği kimyasal zehirlenme, savaş uçaklarında pilotların G kuvvetine maruz kalma veya bilişsel durumlardan komuta merkezlerinin haberdar olmasını sağlayabilir.

3.2.1.2 Askerlerin Silah Sistemleri ve Diğer Cihazlarla Senkronize Edilmesi

YTT ile piyadelerin elindeki silah ve silah sistemlerinin düşmanın eline geçmesi veya bunlara izinsiz kişilerin erişmesi önlenebilir. Örneğin ABD Kara Kuvvetleri YTT'ye sahip yeni nesil piyade tüfekleri üzerinde çalışmaktadır[66].

3.3 Terörle Mücadele

Terör, savunma ve güvenlik alanlarının ikisinin de sorumluluk alanına giren bir sorundur. Bu nedenle ordular ve emniyet teşkilatlarının terörle mücadelede istihbarat işbirliği büyük önem taşımaktadır. Her iki alanda elde edilen biyometrik verilerin paylaşılması için mekanizmalar oluşturulmuştur. Örneğin INTERPOL, terörle mücadele için geliştirdiği veritabanına en büyük katkıyı orduların verdiğini kaydetmektedir[67].

Diğer biyometrik araçlar gibi YTT'nin terörle mücadeleye en büyük katkısı, teröristlerin arkasına sığındığı anonimliği ortadan kaldırıp gerçek kimliklere ulaşılmasını sağlamaktır. Terörizm meçhul ve vatansız bir düşmandır ve etkilerini azaltmak için benzersiz bir yaklaşım gereklidir.

Teröristlerin anonimlik silahı, NATO'nun 2014'te kabul ettiği Yeni Stratejik Konsepti'ne de girmiştir. Belgede, "operasyonel ve stratejik avantajlar elde etmek için anonimlik koruması altında hareket eden bireyler ve devlet dışı aktörler tarafından İttifak'a yönelik artan bir tehdit" olduğu kaydedilmiştir[4]. Söz konusu tehdidi oluşturan birey ve gruplar, "teröristler, insan tacirleri, yabancı savaşçılar, isyancılar, bilgisayar korsanları ve deniz korsanları" olarak sıralanmıştır. Belgede ayrıca, "Bu tür aktörleri belirleme ve anonim kalma yeteneklerini azaltma ihtiyacı şu anda NATO'nun gündeminin üst sıralarında yer alıyor ve bu amaçla biyometri, NATO'nun en önemli stratejik ve operasyonel yeteneklerinden biri olarak kabul ediliyor" denilmektedir.

Biyometrik veri kullanımı, anonimliğe karşı koymada güçlü bir araçtır. Yüz görüntüleri ve parmak izleri gibi biyometrik veriler, sahte kimlik kullanan bireylerin doğru bir şekilde tanımlanmasına yarayabilir, böylece teröristlerin yerini belirleme ve başarılı soruşturma ve kovuşturma yürütme çabalarını geliştirebilir. Biyometrik teknikler ile adli tıp teknolojilerinin, kimlik istihbaratı ile birbirine entegre edilmesi, geleceğin savaşlarının daha hassas bir şekilde yapılmasını sağlayabilecek ve doğru insanları hedef alarak daha az sivil zayiatı ile sonuçlanabilecektir[68].

Yüz tanıma, terörle mücadelede kilit rol oynamaktadır. Söz konusu teknoloji tehlikeli bireyleri tanımlamayı kolaylaştırabilir. Örneğin ABD'nin 11 Eylül 2001'deki terör saldırılarından sorumlu tuttuğu Usame Bin Ladin'in yerini tespit ettikten sonra kimliğini YTT ile doğruladığı belirtilmektedir[69]. ABD, Bin Ladin'e karşı yapılan operasyonun çok az sivil kayıpla son bulduğunu ileri sürmektedir.

3.4 Askeri Tesislere Yönelik Risk ve Tehdit Tespiti

Algoritmalar, normal davranışı tanımak ve anormal davranış durumunda bir uyarı göndermek üzere eğitilmiştir. Bu anlamda YTT, askeri üsler, sahalar, eğitim merkezleri ve tesislerin korunması için kullanılabilir. Ordular askeri ve sivil yetkili personelin kimliklerine ilişkin detaylı bilgiye sahiptir. YTT söz konusu tesislere yetkisi olmayan kişilerin girişini tespit etmek için kullanılabilir. Sistem yetkisiz girişleri anında tespit edip uyarıda bulanabilir.

Gözetim, uzaktan veya karanlıkta yaklaşan potansiyel tehditleri ortaya çıkarmak için kullanılan elektro-optik/kızılötesi gibi yüz tanıma yeteneklerini daha da artırmak için çalışmalar yürütülmektedir.

ABD Silahlı Kuvvetleri ayrıca termal kameraları kullanarak gece yüz tanıma yapabilen bir sistem üzerinde çalışmaktadır. Termal kameralar karanlıkta belli bir noktada insanın varlığını tespit edebilmektedir ancak mevcut yüz tanıma uygulamaları bu görüntüleri alarak işleyememekte ve kimlik tespiti yapamamaktadır. ABD Kara Kuvvetleri Araştırma Laboratuvarı yeni bir yöntem geliştirerek termal kameraların yüzdeki ısı değişimlerinden yola çıkarak yüz tespiti için yeterli veriyi alabilmektedir[70].

3.5 Seçilmiş Ülkelerde YTT'nin Savunma ve Güvenlik Alanında Kullanımı

Yüz tanıma teknolojisinin de dahil olduğu biyometri ve kimlik tanıma sektörü dünyada hayli dinamik bir sektördür. Yapılan araştırmalar YTT teknolojisinin 2021 yılında 4-5 milyar dolar büyüklüğe ulaştığına, gelecek 10 yılda ortalama yüzde 15-16 büyüme göstereceğine işaret etmektedir. Sektördeki canlılığa kamu ve özel sektörün savunma ve güvenlik amaçlı yüz tanıma sistemlerine olan ilgisinin yol açtığı hemen hemen tüm raporlarda kaydedilmektedir. Dünyanın belli başlı bütün büyük ekonomilerinde güvenlik amaçlı YTT yatırımları hızla artmaktadır[71]. Bu bölümde seçilmiş bazı ülkelerde savunma ve güvenlik amaçlı YTT alanında genel eğilimler ve Ar-Ge çalışmalarına göz atılacaktır.

3.5.1 ABD

ABD'de yüz tanıma sistemleri yerel, eyalet ve federal seviyelerde yaygın olarak kullanılmaktadır. Tahminlere göre eyalet geneli veya yerleşim yerlerinin dörtte birinde yüz tanıma taramaları yapılmaktadır ve bunların hepsinin veritabanları ayrıdır[72]. Pazar araştırma şirketi Grand View Research tarafından yapılan bir tahmine göre ABD'de, federal, eyalet ve yerel güvenlik teşkilatlarını kapsayan "kamu yüz biyometrisi" pazarının 2018'de 136,9 milyon dolardan 2025'e kadar 375 milyon dolara yükselmesi beklenmektedir[73].

ABD Sayıştayı'nın (Government Accountability Office) Haziran 2021'de açıkladığı bir rapora[74] göre, 2019-2020 döneminde araştırılan 42 federal idareden 20'si ya kendi yüz tanıma teknolojisini kullanmıştır ya da diğer federal idarelerin teknolojisinden yararlanmıştır. Bunlar arasında gizli servis, kongre polisi, narkotikle mücadele idareleri, gümrük ve sınır koruma idaresi ve ABD Federal Soruşturma Bürosu (FBI) bulunmaktadır.

Bu kapsamda en geniş veritabanı FBI'ın elindedir. FBI'ın Yeni Nesil Kimlik Doğrulama veritabanında çeşitli kaynaklardan elde edilmiş 650 milyondan fazla, yani ABD nüfusunun neredeyse iki katı kadar yüz tanımlama kaydı olduğu belirtilmektedir[11]. FBI'ın ayrıca sadece yüz tanımlama çalışmaları için kurduğu Yüz Analizi, Karşılaştırma ve Değerlendirme (Facial Analysis, Comparison ve Evaluation -FACE) adını verdiği bir servisi bulunmaktadır.

FBI dışında pasaport ve vize başvurularında toplanan veriler nedeniyle ABD Dışişleri ve Savunma Bakanlıklarının da geniş bir biyometrik veritabanı olduğu tahmin edilmektedir. Açık kaynaklara yansıyan haberlere göre

bu iki bakanlığın elinde 300 milyondan fazla kişinin biyometrik verisi bulunmaktadır ve bunu ABD İç Güvenlik Bakanlığı (Department of Homeland Security -DHS) ile paylaşması söz konusudur[75]. Ulusal Güvenlik Dairesi'nin de (National Security Agency -NSA) başta sosyal medya fotoğrafları olmak üzere büyük miktarda izinsiz veri topladığı ileri sürülmektedir[76].

ABD Gümrük ve Sınır Koruma Ajansı (CBP) da yüz tanıma sistemlerini yoğun biçimde kullanmaktadır. CBP'nin ABD'deki 172 havalimanından ülkeye girişleri kısmen veya tamamen biyometrik yüz karşılaştırma teknolojisiyle kontrol ettiği ve Haziran 2021 itibarıyla 77 milyon yolcunun yüz verilerinin veritabanına alındığı kaydedilmektedir[77].

ABD'de kamu güvenliğinden sorumlu kuruluşlar kendi biyometri veritabanlarının yanı sıra özel sektörün sağladığı verileri de kullanmaktadır. Bunların başında Clearview AI[78] gelmektedir. ABD merkezli şirket, hükümet kuruluşlarına olduğu kadar özel sektöre de yüz tanıma çözümleri sunmaktadır. Sosyal medya, haber medyası ve pek çok açık kaynaktan biyometrik veriler toplayan şirket, ABD Sayıştayı'nın raporuna göre ülkenin kamu otoriteleri tarafından en çok başvurulan çözümü geliştirilmiştir[74]. Clearview AI hesabına sahip emniyet güçleri, Clearview AI'ın yüz tanıma sistemine bilinmeyen bir kişinin fotoğrafını yüklemek için bir bilgisayar veya akıllı telefon kullanabilmektedir. Sistem, bilinmeyen kişinin potansiyel fotoğraflarını gösteren arama sonuçlarının yanı sıra fotoğrafların elde edildiği siteye (ör. Facebook) bağlantılar verebilir. ABD ordusunun bazı birimlerinin de Clearview IT yazılımını kullandığı belirtilmektedir[79].

Clearview AI, savunma ve güvenlik açısından hayli işlevsel olmakla birlikte ABD ve Avrupa'da büyük tartışma yaratmıştır. Clearview AI'ın sosyal medyadaki fotoğrafları kullanıcı ve platformlardan izin almadan taradığı ortaya çıkmıştır[80]. Sosyal medya şirketlerinin yanı sıra Avrupa'dan pek çok kuruluş; söz konusu şirket aleyhine, kişisel veri güvenliğini ihlal ettiği ve izinsiz kitlesel takip yaptığı gerekçesiyle davalar açmıştır[79].

ABD'de özellikle savunma ve güvenlik alanında YTT teknolojisine kamuoyunda güvensizlik üst seviyededir. 2020 yılında George Floyd'un gözaltına alınırken gördüğü muamele sonucu yaşamını yitirmesinden sonra başlayan "Siyahilerin Hayatı Önemlidir" (#Black Lives Matter) eylemleri eyalet yönetimleri üzerinde büyük baskı yaratmış ve pek çoğunun emniyet teşkilatları yüz tanıma teknolojisini terk etme emri vermek zorunda kalmıştır.

2019'da ardı ardına çıkarılan çok sayıda yerel yasayla ABD'nin Kaliforniya eyaletindeki San Francisco ve Oakland kentleri[81] ile Massachusetts eyaletindeki Somerville ve Brookline kentleri[82] de dahil olmak üzere birçok kentte YTT'nin kolluk faaliyetlerinde kullanımına yönelik sınırlandırmalar getirilmiştir. San Diego, Ocak 2020'den itibaren YTT'nin kolluk faaliyetlerinde kullanılmasını askıya almıştır[83]. Oregon eyaletinde yer alan Portland, eyalet birimleri ve özel kuruluşların YTT kullanımına yönelik ileriye dönük bir yasak çıkarmayı planladığını açıklamıştır[84]. Massachusetts eyalet meclisi üyeleri ise YTT'nin hükümet tarafından kullanımını eyalet genelinde yasaklayan bir yasa gündeme getirmiştir.

Tepkilere rağmen ABD ordusu ve bazı güvenlik teşkilatları, yüz tanıma teknolojisine yatırım yapmaya ve Ar-Ge çalışmalarına kaynak ayırmaya devam etmektedir. Örneğin ABD Kara Kuvvetleri, terör şüphelilerinin ve askeri casusluk yapanların tespiti için bir yüz tanıma programı üzerinde çalışmaktadır[85].

ABD ordusu Araştırma Laboratuvarı Mart 2021'de, yapay zekâya karanlıkta bile yüzleri tanımasını öğretecek bir programa başlamıştır[86]. Söz konusu programın kızılötesi termal kameralarla gece yüz tanıma çalışmasının bir sonraki aşaması olduğu kaydedilmektedir. Program ve sistemin askeri uçaklar, insansız hava araçları, kara araçları, gözetleme kuleleri ve kontrol noktalarının yanı sıra gelecekte piyade üniformalarına monte edilebilecek yüz tanımalı ve kızılötesi görüşlü kameralardan elde edilecek görüntülerin anlık analizini ve bir alarm sisteminin kurulmasını amaçladığı belirtilmektedir.

ABD Kara Kuvvetleri ayrıca Nisan 2021'de üslerin güvenliğinin artırılması için "Yaklaşan araçlarda ön camların arkasındaki kişilerin kimliğini tespit edebilecek" biyometrik yüz tanıma sistemi geliştirilmesi projesi için bir çağrı yayınlamıştır[87].

3.5.2 Çin

Çin'in diğer yapay zekâ uygulamalarında olduğu gibi yüz tanıma teknolojisinde de dünyada lider konumda olduğu sıklıkla dile getirilmektedir. Bu önermeyi destekleyen gelişmeler bulunmaktadır. Bunlardan birincisi YTT şirketlerinin piyasa değerleridir. Huawei, Hikvision, Dahua ve ZTE gibi büyük şirketler, yapay zekâ tabanlı video gözetiminden tam teşekküllü akıllı şehir paketlerine kadar çeşitli çözümler geliştirmektedir. Piyasa değeri 7,5 milyar doları aşan SenseTime[88], 4,5 milyar dolarlık Megvii[89] ve her ikisi de 2 milyar doların üzerinde değeri bulunan CloudWalk ile Yitu[89] adlı start-up şirketleri yüz tanıma teknolojisinde önde gelen küresel oyunculardır. Çinli şirketlerin, 2023 yılına kadar küresel yüz tanıma pazar payının % 44,59'una sahip olacağı tahmin edilmektedir[90]. Çinli şirketler YTT entegre yapay zekâlı gözetim teknolojilerini 63 ülkeye ihraç etmektedir[1] ve sadece Huawei en az 50 ülkeye bu sistemleri satmaktadır.

Çin'de hükümetin başta yüz tanıma olmak üzere, yapay zekâlı gözetleme sistemlerini teşvik etmesi de bu alanda çalışma yapan şirketlerini cesaretlendirmektedir. Hatta Çin'in "sosyal kredi sistemi"[91] adı altında, vatandaşların davranışlarını izlemek ve her birine çeşitli sonuçları olacak bir sosyal puan vermek için yüz tanıma ve 200 milyon kamera da dahil olmak üzere emrindeki tüm gözetim sistemini kullanmaya başladığı ileri sürülmektedir. Sistemle toplumsal kurallara bağlılığın göstergesi olduğu ileri sürülen bir puanlamayla kişilerin kamu hizmetleri ve bankalardan yararlanma koşullarının düzenlenebileceği ifade edilmektedir[92].

Özellikle Sincan Uygur Özerk Bölgesi'nin gözetleme sistemleri açısından bir "laboratuvar" hâline geldiği iddia edilmektedir[93]. Huawei'nin Uygurlu Müslüman azınlık grubuna mensup kişileri tespit edebilen ve Sincan'daki Çinli yetkilileri uyarabilen yapay zekâ tabanlı bir yüz tarama kamera sistemi olan "Uygur alarmı" olarak adlandırılan bir sistem geliştirdiği ve test ettiği iddia edilmiştir[94].

Genel olarak teknoloji alanında yaptığı çalışmalarla bu alanı şekillendirmeyi ve kontrolü altına almayı amaçlayan ülkelerden biri olan Çin, kent güvenliğini sağlamada güvenlik güçleri için vazgeçilmez bir teknoloji olacağı öngörülen YTT alanında da ilerleyişini sürdürmektedir.

YTT pek çok şehirde güvenlik başta olmak üzere çeşitli amaçlar için kullanılmaktadır. Çin'in Henan eyaletinin başkenti Çengçou şehrinin tren istasyonlarında güvenlik görevlileri yolcuların kimlik bilgisini doğrulamak ve şüphelileri teşhis etmek için Google Glass benzeri yüz tanıma gözlükleri kullanmaya başlamıştır[95]. Bu gözlükler merkezi Pekin'de bulunan LLVisionTechnology şirketi tarafından geliştirilmiştir[96].

Bugün Çin'de sadece tren istasyonlarında değil ülkenin birçok farklı yerinde polis karakollarıyla koordinasyon hâlinde kullanılan bu yüz tanıma teknolojisiyle suçlular tespit edilebilmektedir. Bu teknolojiyle örneğin Şanghay'da trafik kurallarını ihlal edenlerin kimlikleri tespit edilip ceza kesilmektedir[97].

3.5.3 Japonya

Japonya 20'nci yüzyılın son çeyreğinde dünya teknolojisine yön veren ülkeler arasında ilk sıralarda anılmıştır. Uzakdoğu ülkesi bugün bu görünümden oldukça uzak olmakla birlikte bazı alanlarda liderliğini sürdürmektedir. Örneğin, yüz tanıma teknolojisinde Çin ile yarışa girebilen tek ülke Japonya gibi görünmektedir. Japonya'nın bu alanın liderleri arasında yer almasını sağlayan ise teknoloji firması NEC'tir. 1980'li yıllardan bu yana bu alanda çalışan NEC, dünyanın en düşük hata oranına sahip yüz tanıma çözümlerini üretmektedir.

2013	2018	2021
NEC (Japonya)	NEC (Japonya)	SenseTime (Çin)
Morpho (Şimdi Idemia - Fransa)	YituTech (Çin)	Idemia (Fransa)
Toshiba (Japonya)	Microsoft (ABD)	NEC (Japonya)
Cognitec (Almanya)	Shenzen Institute (Çin)	CloudWalk (Çin)
3M (ABD)	SenseTime (Çin)	Xforward (Çin)

Tablo 2: Dünyanın en düşük hata oranına sahip yüz tanıma yazılımlarını geliştiren firmalar[98], [99].

NEC'in YTT çözümleri, Çin ile ABD arasındaki ticari savaş kapsamında Çinli teknoloji firmalarına uygulanan yaptırımlar nedeniyle uluslararası alanda daha yaygın biçimde kullanılmaktadır[99]. COVID-19 pandemisi sürerken maskeli kişilerin tanınmasına olanak sağlayan iyileştirmeler getiren NEC[100], havaalanları için de temassız işlem yapılabilen sistemler geliştirmiştir[101].

3.5.4 Rusya

Rusya'nın teknoloji şirketleri, potansiyel olarak askeri rollere hizmet edebilecek yüz tanıma ve konuşma tanıma teknolojileri üzerinde çalışmaktadır. Rusya'nın önde gelen yüz tanıma AI girişimlerinden biri olan NtechLab, geliştiricilerin Rusya'nın popüler sosyal medya ağı VKontakte'de profilleri gözden geçirmek ve fotoğraflardaki insanları tanımak için tasarladığı FindFace

uygulamasıyla ABD ordusunun araştırma kuruluşlarından biri olan IARPA'nın 2017 Yüz Tanıma Ödül Yarışmasını bile kazanmıştır[102].

Şirketin geliştirdiği FindFace aldı yüz tanıma sistemi 0,3 saniye tanıma hızı ve yüzde 99 başarıyla dünyanın en gelişmiş YTT uygulamalarından biridir ve 30 ülkeden kullanım onayı almıştır[103].

NtechLab, Moskova'nın kapsamlı kentsel gözetim ağının bir parçası olarak yapay zekâ destekli yüz tanıma programları geliştirmek üzere harekete geçmiştir. Uygulama, 12 milyon insanın günlük hareketlerinin izlenmesine imkân sağlayacaktır[104].

Nteclab, ayrıca Tevian ve VisionLabs ile birlikte kişilerin ırklarını da tespit edebilen bir YTT geliştirmiştir[105]. Sistem insan haklarını ihlal ettiği için eleştirilmektedir. Öte yandan sistem, özellikle COVID-19 pandemisi sırasında kapanma kurallarını ihlal edenleri tespit ederken kamu otoritelerine oldukça yardımcı olmuştur. Sistem aynı zamanda enfekte olan kişilerin temas ettiklerini de tespit edebilmiştir[106].

NtecLab ile Rusya'nın kamu kuruluşu Rostec ülkenin silahlı kuvvetleri için de YTT geliştirmek üzere anlaşmaya varmıştır. Geliştirilecek sistemler arasında otonom ve yarı otonom silah sistemlerine yüz tanıma kabiliyeti kazandırmak da bulunmaktadır[107].

3.5.5 Hindistan

Hindistan'da dünyanın en büyük biyometrik programlarından biri yürütülmektedir. Aadhaar adlı dev bir ulusal kimlik kartı sistemi oluşturmak için yüz tanıma da kullanılmaktadır. Hindistan'da yaşayan herkes bir Aadhaar merkezine gidip fotoğraflarını çektirebilmektedir. Sistem, başvuranın hâlihazırda farklı bir adla kaydolmadığından emin olmak için fotoğrafı 1,3 milyar kişinin mevcut kayıtlarıyla karşılaştırır. Ancak sistem, kart sahibi olmayanları ikinci sınıf vatandaşlara dönüştürdüğü ve seçme hakkını elinden almaya yönelik olduğu gerekçeleriyle eleştirilmektedir.

Hindistan'da bankalar, ATM'lerde dolandırıcılığı önlemek için bu yüz tanıma teknolojisini kullanmaktadır[108]. Sistem aynı zamanda mükerrer seçmenlerin bildirilmesi, pasaport ve vizenin doğrulanması, ehliyet vb. için de kullanılmaktadır. Ülkenin eyaletlerindeki emniyet teşkilatları da yaygın biçimde YTT kullanmaktadır. Bir araştırmaya göre 32 eyalette bu sistemler kullanılmaktadır[109].

Hindistan ordusu da yüz tanıma sistemlerine yatırımlarını artırmıştır. Ordunun araştırma birimi DRDO, Pakistan sınırında yaşayan çiftçilerin ara bölgedeki tarlalarına kolaylıkla erişebilmesi için üç boyutlu bir YTT sistemini devreye almıştır. Aynı sistemin çatışma alanlarında dost ve düşman kuvvetlerinin birbirinden ayırt edilmesinde kullanılabileceği kaydedilmektedir[110].

3.5.6 İsrail

21'inci yüzyılın teknolojilerinde gerçekleştirdiği atılımlarla kendine has bir yer edinen İsrail'de diğer bütün yapay zekâ bağlantılı teknolojilerde olduğu gibi biyometrik tanıma teknolojilerinde önemli atılımlar gözlemlenmektedir. Ülkede üniversitelerle bağlantılı çok sayıda startup, biyometrik çözümler geliştirmektedir. Örneğin Corsight AI, yüzlerinin bir kısmı kapalıyken bile kişileri gerçek zamanlı olarak tanımlayabilen bir yüz tanıma aracı geliştirmiştir[111]. IsitYou ise yüz tanıma ile bankacılık hizmeti vermek isteyen mali kuruluşlara sunduğu hizmetinde, cep telefonunun kamerasına gösterilen yüzün bir fotoğraftaki kişiye mi yoksa kameranın karşısına geçmiş "canlı" bir kişiye mi ait olduğunu tespit edebilmektedir[112].

YTT açısından İsrail'de en çok ses getiren firma ise AnyVision olmuştur. Merkezi Tel Aviv'de olan ancak 43 ülkede 350'den fazla kentte faaliyet yürüten şirket, emniyet teşkilatlarına, akıllı kent uygulaması olan dünyanın çeşitli şehirlerinin yönetimlerine, havalimanı, otel ve şirketlere yapay zekâ destekli yüz tanıma teknolojisi sağlamaktadır. Şirketin Batı Şeria'nın işgal edilmiş topraklarına kurduğu YTT sisteminin "terör saldırısı düzenleme olasılığı olanları" bile tespit edebildiği ileri sürülmektedir. İsrail'in Filistin topraklarında dünyanın büyük kitlesel gözetleme faaliyeti yürütmesi[113] insan hakları savunucularının tepkisini çekmekte, dünya genelinde firmanın çözümlerini satın alan kamu kuruluşları ve özel şirketler itham altında kalmaktadır[114].

4. GELECEĞİN YÜZ TANIMA SİSTEMLERİ SAVUNMA VE GÜVENLİK ALANINI NASIL ETKİLEYECEK?

Birçok biyometrik teknoloji gibi yüz tanıma çözümleri de hâlen geliştirme ve test aşamasındadır. Ancak birkaç yıl içinde bu teknolojilerin kamusal alanların çoğunda görüleceğini tahmin etmek zor değildir. Sadece savunma ve güvenlik alanındaki yatırımlar ile araştırma ve geliştirme çalışmalarına ayrılan kaynaklar bile bu alanın gelişime son derece açık olduğunu göstermektedir. Bu bölümde savunma ve güvenlik alanı ağırlıklı olarak YTT'nde yakın gelecekte olası gelişmelere ışık tutulmaya çalışılacaktır.

4.1 Uzun Mesafeden Kimlik Tespiti

Yüz tanımanın gelecekte savunma ve güvenlik alanında çığır açıcı etkileri olabilir. Çalışmalar özellikle uzun mesafeden kimlik tespiti üzerine odaklanmıştır. Örneğin ABD'nin istihbarat örgütleri için araştırma ve geliştirme çalışmaları yürüten IARPA, Ocak 2021'de 300 m ila 1.000 m arasında uzun mesafeden ve yüksek irtifadan (hava aracı, kule veya yüksek bina) kişilerin kimliklerinin her türlü hava koşulunda tespitini sağlayacak sistem geliştirme çağrısında bulunmuştur. Söz konusu sistemin geliştirilmesi için zorlu atmosferik ve görüş koşulları altında uzak mesafeden yakalanan görünür bant video görüntülerinde biyometrik doğrulama, tanıma ve kişilerin tanımlanmasını gerçekleştirebilen algoritmalar geliştirilmesi gerekecektir[115]. Sistemin geliştirilmesi hâlinde, terörle mücadele, kritik altyapı ve ulaşım tesislerinin korunması, askeri gücün korunması ve sınır güvenliği gibi görevlerde önemli katkı sağlanacağı beklenmektedir.

ABD Özel Operasyon Komutanlığı (SOCOM) da benzeri bir proje üzerinde çalışmaktadır. Kişilerin kimliklerini bir kilometre öteden tespit edebilmek için 2016'da başlatılan çalışmalarda 2019'da taşınabilir bir sistemin prototipinin geliştirilmesi aşamasına gelindiği kaydedilmektedir[116].

YTT'ne sahip insansız hava araçları ile, uzun mesafeden kimlik tespiti de yakında mümkün olabilir. Türkiye'de Papilon Savunma, İHA ile kullanabilecek bir yüz tanıma sistemi geliştirmiştir. Çevresel faktörlerin yarattığı dezavantajlardan (gün ışığı, ters ışık, kamera açısı vb.) minimum şekilde etkilenen algoritmalar sayesinde yüksek doğruluk oranı ile çalışan yüz tanıma sisteminin havadan tespit yapabildiği belirtilmektedir[117]. İsrailli teknoloji firması AnyVision, benzeri bir teknoloji için ABD'den patent almıştır[118]. Birleşik Arap Emirlikleri'nin Şarjah kentinde emniyet güçleri yüz tanıma özellikli kameralarla donatılmış yaklaşık 200 İHA'yı test etmeye başlamıştır[119]. Açık kaynaklarda, 30 kilograma kadar görev yükü taşıyabildiği ifade edilen söz konusu İHA'ların şüphelileri tespit ettiğinde alçalıp açısını düzelterek kişinin aranılanlar listesinde olduğunu kesinleştirdiği ve yetkili birimlere anında haber verebildiği kaydedilmektedir. Sistemin COVID-19 kapanma kurallarına aykırı davranışları tespit ettiği; kazalar ve olay yeri incelemesine katkı sağladığı; kayıp kişileri aradığı, yasadışı faaliyetleri izlediği, hassas ve tehlikeli endüstriyel bölgelerde güvenliği sağladığı ve pek çok güvenlik görevi üstlenebildiği belirtilmektedir[119].

4.2 5G ve Nesnelerin İnterneti Destekli Yüz Tanıma İle Muharebe Sahasında Artırılan Durumsal Farkındalık

5G mobil teknolojisinin yaygınlaşmasıyla nesnelerin interneti uygulamalarının daha da yaygınlaşması beklenmektedir. Bu gelişme YTT açısından da önemli atılımlara kapı aralayabilir.

5G teknolojisinin hızı günümüzde birkaç saniyede sonuç verebilen YTT gibi biyometrik çözümlerinin hızını neredeyse anlık hâle getirebilir[120]. 5G'nin mobil bir teknoloji olması YTT uygulamalarının taşınabilir cihazlar ve giyilebilir elektronik ürünleriyle birlikte daha da yaygınlaşması bir diğer beklentidir. Bu beklentiyle çalışmalar başlamıştır. Örneğin ABD Kara Kuvvetleri Araştırma Laboratuvarı, yeni tahmine dayalı savaş alanı analitiği geliştirmek için Gelişen Akıllı Hedefe Dayalı Ağlar (IoBT REIGN) için Savaş Alanı Nesnelerinin İnterneti Araştırması konsorsiyumuna 25 milyon dolar kaynak tahsis etmiştir[121]. Askeri Nesnelerin İnterneti'nde (IoMT) veya Savaş Alanı Nesnelerinin İnterneti'nde (IoBT), askerler tarafından giyilen ve savaş kıyafetlerine, miğferlerine, silah sistemlerine ve diğer ekipmanlara gömülü sensörler; yüz, iris, perioküler boşluk, parmak izleri, kalp atış hızı, yürüyüş, jestler ve yüz ifadeleri gibi dinamik biyometri verilerinin anlık izlenmesini sağlayabilir[122]. Öte yandan nesnelerin interneti uygulamalarının gelecekte güvenliğinin sağlanması için YTT gibi biyometrik teknolojilerden yararlanması gerekeceği sıkça dile getirilmektedir[123].

4.3 "Akıllı Polislik" Uygulamaları (Smart Policing)

Akıllı polislik, suçu önlemek, suç eylemlerine yanıt vermek ve hatta gelecekteki suç faaliyetleri hakkında tahminlerde bulunmak için coğrafi konum, tutuklama istatistikleri, işlenen suç türleri, biyometrik veriler, sosyal medya gönderileri ve benzerlerinden elde edilen muazzam miktarda veriyi bir algoritmayla analiz etmektir. Bu anlamda büyük veriyi suçu önlemek amacıyla kullanmaya dayanmaktadır ve öngörüsel amaçlı veri analizinin bir başka örneğidir[124].

Akıllı şehir uygulamaları, şehir güvenlik kameraları, YTT, sosyal medya dahil açık kaynaklardan elde edilen verilerle emniyet güçleri artık çok daha büyük miktarda veriye erişim imkânına sahip olmuştur. Bu nedenle, akıllı polisliğin ana bileşenlerinden biri, çok büyük miktarda materyali ayrıştırabilen, birden fazla kaynaktan gelen verileri kolaylaştıran ve bireysel bilgilerin ince ayarlı toplanmasına izin veren otomatik platformlar oluşturmaktır.

Bu alandaki çalışmalar henüz emekleme safhasındadır. Ancak teknolojideki ilerlemeler ve güvenlik konusunda karar alıcıların teşvikiyle söz konusu alandaki atılımların hız kazanması beklenebilir. Özünde bu programlar, gelecekteki suçların nerede işleneceğini, büyük miktarda veri toplamaya dayalı olarak dikkate değer bir doğrulukla tahmin ettiğini iddia etmektedir. ABD'de "Predpol" adı verilen öngörüye dayalı sistem 60'tan fazla yerel polis teşkilatı tarafından kullanılmaya başlanmıştır. Ancak söz konusu uygulama, taraflı girdilere dayandığı ve hatalı öngörüleri nedeniyle[125] yanlış muamelelere yol açtığı için eleştirilmektedir. Nitekim Los Angeles Polis Teşkilatı Nisan 2020'de uygulamayı kullanmaya son vermiştir[126].

4.4 Otomatik Sınır Kontrol Sistemleri

Sınır teşkilatları birçok zorlukla karşı karşıyadır ve bugün benzeri görülmemiş bir değişim çağında faaliyet göstermektedirler. Giderek daha değişken hâle gelen küresel seyahat ve ticaret ortamı, yeni güvenlik ve halk sağlığı tehditleriyle birleşmiş ve süreçlerin yönetimini daha da zorlu hâle getirmiştir.

Bu istikrarsızlık ve hızlı değişim çağında başarılı olmak için sınır teşkilatlarının süreçlerini, çalışanlarını ve teknolojilerini geliştirmeleri gerekmektedir. Sınır deneyimlerinin ve süreçlerinin tamamen dijitalleştirilmesi ve temassız hâle getirilmesi önerilerin başında gelmektedir. Bu gelişmeler ışığında yüz tanıma teknolojisinin sınır kontrollerinde geleceğin en önemli öğelerinden biri olmayı sürdüreceğini tahmin etmek güç değildir.

Sınır kapıları ve havaalanlarında yolcu kontrollerinin yarattığı zaman kaybının azaltılmasına yönelik biyometrik çözümler günümüzde hayli yaygınlık kazanmıştır. Bu sürecin daha da hızlanması için çalışmalar sürmektedir. Örneğin, Avrupa Birliği "iBorderCtrl" adlı bir teknolojiyi üç ülkede test etmektedir. Akıllı Taşınabilir Sınır Kontrolü'nün kısaltması olan iBorderCtrl, pilot proje kapsamında Yunanistan, Macaristan ve Letonya'da denenmektedir. Bu sistemde yolculara menşe ülkeleri ve hareket koşulları hakkında sorular sorulmakta ve yolcuların yüz

görüntüleri alınmaktadır. Alınan cevaplar ve yüz ifadeleri daha sonra AI tabanlı bir yalan tespit sistemi tarafından değerlendirilmektedir. Soruları dürüstçe yanıtladığı tespit edilen yolculara, geçmelerine izin veren bir kod verilmektedir. Diğerleri ise gözaltına alınmaktadır. Sistem daha şimdiden tartışma yaratmıştır ve iptali için Avrupa Adalet Divanı'nda dava açılmıştır[127].

4.5 Yüz Tanıma İle Duygu Analizi

Yüz tanıma teknolojisinin en tartışmalı ancak gelişime en açık alanlarından biri yüz tanıma ile duygu analizidir. Yüz-duygu tanıma, yüz ifadelerinden insan duygularını algılama sürecidir. Araştırmalar, iletişimimizin yüzde 90'ından fazlasının sözsüz olduğunu göstermektedir[128]. İnsan beyni duyguları otomatik olarak tanır ama günümüze kadar bunları tanıyabilecek algoritmalar geliştirilememiştir. Duyguların yüzde yarattığı jestlere dayanan tahminler yapabilen bu algoritmalar henüz emekleme aşamasındadır ve büyük tartışma yaratmaktadır.

Yüz tanıma ile duygu analizini savunanlar bu teknolojinin kişinin kaza yapmasını, saldırı düzenlemesini veya intihar etmesini engelleyebileceğini ileri sürmektedir. Bu amaçla çalışmalar da bulunmaktadır. Örneğin; Çin'in araç paylaşım platformu Didi, daha önce kendisiyle anlaşmalı sürücüleri tanımak için kullandığı YTT sistemini, sürücülerin uykulu olup olmadığını tespit etmek için kullanabileceğini açıklamıştır[129]. Sosyal medyada paylaşılan fotoğraflarda kimin intihar eğilimli olup olmadığının tespit edilmesine dair çok sayıda bilimsel çalışma bulunmaktadır[130].

Duygu analizinin kullanım alanı olarak önerilenler arasında kişiye özel mesajlar[131] gönderilmesi, ruh hâline göre müzik, film ürün vb. önerisinde bulunulması[132], kişilerin sanat etkinlikleri ve filmlere tepkilerinin ölçülmesi[133], işe alımlarda karar vermeye yardımcı olunması[134], öğrencilerin derse ilgisinin ölçülmesi[135], terör saldırısı düzenleme potansiyeli olanlarının tespiti[136] ve hatta siyasi tavırların belirlenmesi[137] bulunmaktadır.

Bu alanda çözümler üreten firmaların sayısı gün gittikçe artmaktadır. NEC veya Google gibi teknoloji devlerinden Affectiva veya Eyeris gibi daha küçük şirketlere kadar birçok şirket bu teknolojiye yatırım yapmaktadır. Ayrıca AB'nin araştırma ve inovasyon programı Horizon 2020 kapsamında da çalışmalar yürütülmektedir[138]. Bu alanda startup firmaları da ortaya çıkmaktadır. Örneğin İsrail'de 2011 yılında bir grup sinirbilimci tarafından kurulan BioCatch adındaki firma, biyometrik kimlik doğrulama hizmeti sunmaktadır. Cep telefonu ve internet uygulaması olan BioCatch tek bir kullanıcı profili oluşturmak için 500'den fazla bilişsel parametre kullanmaktadır[112].

Buna karşılık söz konusu teknolojinin karşısında olanlar başta kültürel ve etnik farklılıklar olmak üzere pek çok açıdan güvenilir standart duygu algılamasının geliştirilemeyeceğini ileri sürerek bu teknolojiye kuşkuyla baktıklarını ifade etmektedir[139].

4.6 Biyometri Karması

Biyometri sektörü, dünya çapında kimlik hırsızlığı, veri hack'leme ve güvenlik ihlallerine dair endişeler nedeniyle hızlı bir şekilde büyümektedir. Hem şirketler hem de devletler, verilerini rahatça emanet edebilecekleri güvenilir biyometrik teknolojiler konusunda çalışmaktadır. Yüz tanıma teknolojisinin, mobil ödeme ve perakende uygulamalarında sıklıkla kullanılması beklenebilir.

Yüz tanıma teknolojisi gelecek diğer biyometri araçlarıyla birlikte daha düşük hata oranlı olarak ayrıntılı analiz sunabilecektir. Kişinin yüzü, parmak izi, konuşması, yürüyüşü ve hatta kişiye özel kalp atış ritmi gibi özelliklerinden kimlik tespitine yönelik çalışmalar artmaktadır. Tüm bu sistemlerin en düşük hata oranıyla kimlik tespiti veya kimlik doğrulamasına yol açacak biçimde birleştirilme yoluna gideceği yönündeki öngörüleri beraberinde getirmektedir.

Biyometride ayırt edici özellik olarak kullanılan verilerden biri de kişinin sesidir. Konuşmacı (speaker) veya ses tanıma (voice recognition), konuşma tanıma teknolojisinden farklıdır, çünkü bir kişi ses biyometrisini kullanarak bir konuşmacıyı tanır, tanımlar ve söylenenleri analiz eder. Ses biyometrisi ise, ritim ve ton gibi davranışsal özellikleri içerir.

Parmak izi ve parmak damar izi tanımlama da bilinen ve kullanılan yöntemlerdendir. Son yıllarda ağırlıklı olarak kimlik ve pasaportta kullanılan parmak izi/parmak damar izi teknolojisi artık ofis, hastane vb. mekânlarda kişi doğrulama için tercih edilen bir yöntem olarak karşımıza çıkmaktadır.

Henüz yaygınlaşmamış olsa da; iris tarama, el geometrisi tanımlama, beyin dalgalarıyla kişiyi tanımlama, vücut kokusu ve DNA profillemesi de biyometrik teknolojilerde kullanılabilecek diğer kişiye has fiziksel özellikler arasındadır.

Kişinin kalp ritminin en az parmak izi ve yüz biçimi kadar kendisine has olduğu bilinmektedir. Yapılan çalışmalar kalp biyometrisinin yüz tanımadan yüzde 98 daha güvenli olduğunu ortaya çıkarmıştır[140]. Bu gerçekten yola çıkan ABD Özel Kuvvetler Komutanlığı, kızılötesi lazer kullanarak 200 metre öteden kalp atışının yarattığı küçük titreşimleri algılayabilecek bir cihaz üzerinde çalışmaktadır[141]. Sistemin, kişinin üzerindeki kıyafetlere rağmen kalp ritmini yakalayabileceği ileri sürülmektedir[141]. Ancak bu teknolojinin en büyük zaafı kalp ritmini yakalayıp kimliklerle ilişkilendirmek için en az 30 saniyeye ihtiyaç duymasıdır.

Kişinin davranışsal özellikleri de biyometrinin ilgi alanına girmiştir. Örneğin Çinli startup Watrix, video görüntülerinden yürüyüş şeklini tespit ederek eğer veritabanında varsa bu kişinin kimliğini 50 metreye kadar mesafeden tespit edebilen bir sistem geliştirdiğini duyurmuştur[142].

Tüm bu biyometrik verileri bir arada kullanan sistemler geliştirilmeye başlanmıştır. Örneğin İsrail ordusundan emekli bir general tarafından kurulan FST Biometrics şirketinin geliştirdiği "Hareket Hâlinde Kimlik Tespiti Yönetimi (In Motion Identification -IMID) bunlardan biridir. Sistem biyometrik ve analitik teknolojilerini kullanarak sınır geçişleri ve kontrol noktalarından geçen kişilerin yüz, yürüyüş tarzı ve vücut hareketlerini analiz ederek sesiyle eşleştirmekte ve kimlik tespiti yapabilmektedir. Üstelik tüm bu süreçler kişilerin suçluluk hissine kapılmasına izin vermeden saniyeler içinde olmaktadır[112].

5. SONUÇ

Yüz tanıma teknolojisi ve genel olarak biyometri teknolojisi, günümüzde hem bireysel hem de ulusal seviyede güvenlik endişelerinin arttığı bir çağda önerilen en iyi çözümlerden biri olarak ortaya çıkmaktadır. Kişiye has fiziksel ve davranışsal özellikleri bulup kimlik tespiti ve doğrulama yapan sistemler kişi ve kurumları istismar etmek isteyenlere karşı etkin bir yöntemdir. Ancak bu yöntemlerin yeni istismarlara, adli hatalara ve ihlallere yol açmaması için düzenleme yapılması gerektiği de açıktır.

Yüz tanıma, görece yeni bir teknolojidir. Başarısı ardındaki yapay zekâ uygulamalarının gelişmişliğine bağlıdır. Bu yüzden diğer yapay zekâ uygulamalarında olduğu gibi Çin'in bu alanda dünyada lider konuma gelmesi şaşırtıcı değildir.

YTT teknolojisi hakkında göz ardı edilemeyecek eleştiriler yöneltilmektedir. Ancak eleştirilerin büyük bir kısmı henüz bu teknolojinin tam olarak olgunlaşmaması ve teknolojinin kullanımına ilişkin düzenlemeler konusunda somut adımların sınırlı kalmasıdır.

Emniyet teşkilatları yüz tanımada belli bir deneyim sahibi olmasına rağmen askeri alanda bu teknolojinin kullanımı daha yeni yeni başlamıştır. Ancak orduların, gece yüz tanıma ve uzaktan yüz tanıma gibi alanlarda yaptığı araştırmalar, sivil sektörde de yansımasını bulabilecek niteliktedir ve sektöre ivme kazandıracaktır.

Türkiye'de yüz tanıma teknolojisi alanında çalışmaların sınırlı düzeyde kaldığı görülmektedir. Diğer alanlarda 21'inci yüzyıl teknolojilerini başarıyla kullanarak TSK'ye gelişmiş çözümler sunan Türk savunma sanayii, bu alanda da çalışmalarını yoğunlaştırarak hem TSK'ye yeni kabiliyetler kazandırabilir hem de bu geleceği açık sektörde özel sektör firmalarına ilham kaynağı olabilir.

KAYNAKÇA

[1] Feldstein, Steven; (2019), "The Global Expansion of AI Surveillance", Carnegie Endowment For International Peace, (Eylül 2019), https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf. (Erişim Tarihi: 2 Ekim 2021)

[2] Crumpler, William; (2020), "How Accurate are Facial Recognition Systems – and Why Does It Matter?", *Center for Strategic and International Studies*, (14 Nisan 2020), https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter. (Erişim Tarihi: 2 Ekim 2021)

[3] Symanovich, Steve; (2021), "What is facial recognition? How facial recognition works", *Norton*, (20 Ağustos 2021), https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html. (Erişim Tarihi: 2 Ekim 2021)

[4] Lunan, Mark; (2018), "Biometrics", *NATO*, https://www.jwc.nato.int/images/stories/threeswords/Biometrics_2018.pdf. (Erişim Tarihi: 2 Ekim 2021)

[5] *Joint Chiefs of Staff*, (2013), "Joint Intelligence", (22 Ekim 2013), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf. (Erişim Tarihi: 2 Ekim 2021)

[6] *Council of Europe*, (2021), "Guidelines on Facial Recognition", (28 Ocak 2021), https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. (Erişim Tarihi: 2 Ekim 2021)

[7] *Electronic Frontier Foundation*, "Face Recognition", https://www.eff.org/tr/pages/face-recognition. (Erişim Tarihi: 2 Ekim 2021)

[8] Lee, Giacomo; (2021), "Face recognition is just the tip of the AI Computer Vision iceberg", *Verdict*, (4 Haziran 2021), https://www.verdict.co.uk/face-recognition-is-just-the-tip-of-the-ai-computer-vision-iceberg/. (Erişim Tarihi: 2 Ekim 2021)

[9] *AJL*, "WHAT IS FACIAL RECOGNITION TECHNOLOGY?", https://www.ajl.org/facial-recognition-technology. (Erişim Tarihi: 2 Ekim 2021)

[10] *STM ThinkTech*, (2018), "Derin Farklar: Yapay Zekâ, Makine Öğrenmesi ve Derin Öğrenme", (14 Kasım 2018), https://thinktech.stm.com.tr/detay.aspx?id=182. (Erişim Tarihi: 2 Ekim 2021)

[11] *Kaspersky*, "What is Facial Recognition – Definition and Explanation", https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition. (Erişim Tarihi: 2 Ekim 2021)

[12] Yang, Ming-Hsuan; (2002), "Detecting Face in Images: A Survey", *Research Gate*, (Şubat 2002), https://www.researchgate.net/profile/Ming-Hsuan-Yang-2/publication/3193340_Detecting_Faces_in_Images_A_Survey/links/0912f50adc53724402000000/Detecting-Faces-in-Images-A-Survey.pdf. (Erişim Tarihi: 2 Ekim 2021)

[13] Dwivedi, Divyansh; (2018), "Face Detection For Beginners", *towards data science*, (27 Nisan 2018), https://towardsdatascience.com/face-detection-for-beginners-e58e8f21aad9. (Erişim Tarihi: 2 Ekim 2021)

[14] *Markets and Markets*, "Facial Recognition Market worth $8.5 billion by 2025", https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp. (Erişim Tarihi: 2 Ekim 2021)

[15] Gallagher, Chris; (2021), "Masks no obstacle for new NEC facial recognition system", *Reuters*, (7 Ocak 2021), https://www.reuters.com/article/us-health-coronavirus-japan-facial-recog-idUSKBN29C0JZ. (Erişim Tarihi: 2 Ekim 2021)

[16] Hodson, Hal; (2012), "Face recognition finds lost pilgrims in Mecca", *ScienceDirect*, (9 Haziran 2012), https://www.sciencedirect.com/science/article/pii/S0262407912614729. (Erişim Tarihi: 2 Ekim 2021)

[17] Deb, Sopan; Singer, Natasha; (2018), "Taylor Swift Said to Use Facial Recognition to Identify Stalkers", *New York Times*, (13 Aralık 2018), https://www.nytimes.com/2018/12/13/arts/music/taylor-swift-facial-recognition.html. (Erişim Tarihi: 2 Ekim 2021)

[18] *Banfacialrecognition*, "BAN FACIAL RECOGNITION IN STORES", https://www.banfacialrecognition.com/stores/. (Erişim Tarihi: 2 Ekim 2021)

[19] Dua, Tanya; (2017), "DiGiorno pizza used facial recognition to show how much people love pizza", *DIGIDAY*, (3 Mayıs 2017), https://digiday.com/marketing/digiorno-pizza-used-facial-recognition-show-much-people-love-pizza/. (Erişim Tarihi: 2 Ekim 2021)

[20] Mullen, Jethro; Wang, Serenitie; (2017), "Pay with your face at this KFC in China", *CNN*, (1 Eylül 2017), https://money.cnn.com/2017/09/01/technology/china-alipay-kfc-facial-recognition/index.html. (Erişim Tarihi: 2 Ekim 2021)

[21] Seker, Ensar; (2020), "Deepfake to Bypass Facial Recognition by Using Generative Adversarial Networks (GANs)", *towards data science*, (17 Mayıs 2020), https://towardsdatascience.com/deep-

fake-to-bypass-facial-recognition-by-using-generative-adversarial-networks-gans-37a8194a87b1. (Erişim Tarihi: 2 Ekim 2021)

[22] Cheshire, Tom; (2017), "Piccadilly Circus lights facial detection system 'incredibly intrusive'", *Sky News*, (18 Ekim 2017), https://news.sky.com/story/piccadilly-circus-lights-facial-detection-system-incredibly-intrusive-11087020. (Erişim Tarihi: 2 Ekim 2021)

[23] Zhu, Melissa; (2020), "What is facial recognition, and why is it more relevant than ever during the coronavirus pandemic?", *South China Morning Post*, (18 Kasım 2020), https://www.scmp.com/tech/policy/article/3108742/what-facial-recognition-and-why-more-relevant-ever-during-covid-19?module=perpetual_scroll&pgtype=article&campaign=3108742. (Erişim Tarihi: 2 Ekim 2021)

[24] Getz, Ken; (2021), "Using AI to Provide New Insights into Intentional Dose Non-Adherence", *AiCure*, (12 Mayıs 2021), https://aicure.com/blog/opinion/using-ai-to-provide-new-insights-into-intentional-dose-non-adherence/. (Erişim Tarihi: 2 Ekim 2021)

[25] *STM ThinkTech*, (2019), "İLERİ SAĞLIK TEKNOLOJİLERİ III: Sağlıkta Dijitalleşmenin Önündeki Yol Haritası", (29 Kasım 2019), https://thinktech.stm.com.tr/detay.aspx?id=290. (Erişim Tarihi: 2 Ekim 2021)

[26] *Omnicom Health Group*, (2017), "The Face as the Key to Unlocking Health Information", (Kasım 2017), https://omnicomhealthgroup.com/pdfs/OHG-Facial-Recognition.pdf. (Erişim Tarihi: 2 Ekim 2021)

[27] *Face-six*, "FA6 MED – FACE RECOGNITON FOR HOSPITALS. PATIENT IDENTIFICATION. REINVENTED!", https://www.face-six.com/patient-identification/. (Erişim Tarihi: 2 Ekim 2021)

[28] Chen, Zhanli; (2018), "Automated Pain Detection from Facial Expressions using FACS: A Review", *arxiv*, (13 Kasım 2018), https://arxiv.org/pdf/1811.07988. (Erişim Tarihi: 2 Ekim 2021)

[29] Dolgin, Elie; (2019), "AI face-scanning app spots signs of rare genetic disorders", *Nature*, (7 Ocak 2019), https://www.nature.com/articles/d41586-019-00027-x. (Erişim Tarihi: 2 Ekim 2021)

[30] Pascu, Luana; (2019), "West Virginia Secretary of State vows security of biometric mobile voting process", *Biometric Update*, (7 Ekim 2019), https://www.biometricupdate.com/201910/west-virginia-secretary-of-state-vows-security-of-biometric-mobile-voting-process. (Erişim Tarihi: 2 Ekim 2021)

[31] *ellucian*, "Facial recognition can give students better service (and security)", https://www.ellucian.com/blog/facial-recognition-campus-benefits-security-risks. (Erişim Tarihi: 2 Ekim 2021)

[32] Herold, Benjamin; (2018), "Facial-Recognition Systems Pitched as School-Safety Solutions, Raising Alarms", *Education Week*, (18 Temmuz 2018), https://www.edweek.org/ew/articles/2018/07/18/facial-recognition-systems-pitched-as-school-safety-solutions-ra.html. (Erişim Tarihi: 2 Ekim 2021)

[33] Yi, Yang; (2017), "Chinese university uses facial recognition to track student attendance", *Xinhuanet*, (25 Ekim 2017), http://news.xinhuanet.com/english/2017-10/25/c_136704562.htm. (Erişim Tarihi: 2 Ekim 2021)

[34] Karoub, Jeff; (2020), "U-M study finds facial recognition technology in schools presents many problems, recommends ban", *University of Michigan*, (10 Ağustos 2020), https://news.umich.edu/u-m-study-finds-facial-recognition-technology-in-schools-presents-many-problems-recommends-ban/. (Erişim Tarihi: 2 Ekim 2021)

[35] Misra, Tanvi; (2019), "The Tenants Fighting Back Against Facial Recognition Technology", *Bloomberg*, (7 Mayıs 2019), https://www.bloomberg.com/news/articles/2019-05-07/when-facial-recognition-tech-comes-to-housing. (Erişim Tarihi: 2 Ekim 2021)

[36] Davies, Marie; (2018), "These Moscow apartments are replacing keys with face recognition tech", *The Calvert Journal*, (9 Nisan 2018), https://www.calvertjournal.com/articles/show/9853/these-moscow-apartments-are-replacing-keys-with-face-recognition-tech. (Erişim Tarihi: 2 Ekim 2021)

[37] Oakley, Philip; (2019), "Porsche Develops Facial Recognition Vehicle Access", *TU-Automotive* (1 Ağustos 2019), https://www.tu-auto.com/porsche-develops-facial-recognition-vehicle-access/. (Erişim Tarihi: 2 Ekim 2021)

[38] Hollister, Sean; (2021), "How Tencent's sweeping new facial scans will catch Chinese kids playing past curfew ", *The Verge*, (9 Temmuz 2021), https://www.theverge.com/2021/7/9/22567029/tencent-china-facial-recognition-honor-of-kings-game-for-peace. (Erişim Tarihi: 2 Ekim 2021)

[39] *FindBiometrics*, (2021), "South Australia Clamps Down On Problem Gambling With Facial Recognition Tech", (28 Mayıs 2021), https://findbiometrics.com/south-australia-clamps-down-on-problem-gambling-with-facial-recognition-tech-052809/. (Erişim Tarihi: 2 Ekim 2021)

[40] Dai, Sarah; (2020), "Shanghai introduces facial recognition drug collection terminals to combat abuse by patients and pharmacists", *South China Morning Post*, (17 Ocak 2020), https://www.scmp.com/tech/policy/article/3046346/shanghai-introduces-facial-recognition-drug-collection-terminals-combat. (Erişim Tarihi: 2 Ekim 2021)

[41] Milne, Sandy; (2020), "Facial recognition for pigs: Is it helping Chinese farmers or hurting the poorest?", *The Guardian*, (10 Aralık 2020), https://www.theguardian.com/environment/2020/dec/10/facial-recognition-for-pigs-is-it-helping-chinese-farmers-or-hurting-the-poorest. (Erişim Tarihi: 2 Ekim 2021)

[42] Southey, Flora; (2021), "Real-time facial recognition tech developed for cows and pigs: 'Animal emotions directly impact meat quality'", *Food Navigator*, (12 Mayıs 2021), https://www.foodnavigator.com/Article/2021/05/12/Real-time-facial-recognition-tech-developed-for-cows-and-pigs-Animal-emotions-directly-impact-meat-quality. (Erişim Tarihi: 2 Ekim 2021)

[43] *Simbt*, "ÜRÜNLER Takbul Gözlük", http://www.simbt.com.tr/urunler/id/28/takbul_gozluk. (Erişim Tarihi: 2 Ekim 2021)

[44] Heilweil, Rebecca; (2020), "Masks can fool facial recognition systems, but the algorithms are learning fast", *Vox*, (28 Temmuz 2020), https://www.vox.com/recode/2020/7/28/21340674/face-masks-facial-recognition-surveillance-nist. (Erişim Tarihi: 2 Ekim 2021)

[45] Haskell-Dowland, Paul; (2020), "Face masks and facial recognition will both be common in the future. How will they co-exist?", *The Conversation*, (6 Eylül 2020), https://theconversation.com/face-masks-and-facial-recognition-will-both-be-common-in-the-future-how-will-they-co-exist-144417. (Erişim Tarihi: 2 Ekim 2021)

[46] Murdock, Jason; (2018), "Amazon Face Recognition Tech Matches 28 Members of Congress With Mugshots", *Newsweek*, (27 Temmuz 2018), https://www.newsweek.com/amazons-face-recognition-tool-matches-28-members-congress-criminal-mugshots-1044850. (Erişim Tarihi: 2 Ekim 2021)

[47] Grother, Patrick; (2021), "Amazon Face Recognition Tech Matches 28 Members of Congress With Mugshots", *National Institute of Standards and Technology*, (21 Eylül 2021), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf. (Erişim Tarihi: 2 Ekim 2021)

[48] *University of Essex*, (2019), "New report raises concerns over Met Police trials of live facial recognition technology", (3 Temmuz 2019), https://www.essex.ac.uk/news/2019/07/03/met-police-live-facial-recognition-trial-concerns. (Erişim Tarihi: 2 Ekim 2021)

[49] Parker, Jake; (2021), "What Science Really Says About Facial Recognition Accuracy and Bias Concerns", *Security Industry Association*, (23 Temmuz 2021), https://www.securityindustry.org/2021/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/. (Erişim Tarihi: 2 Ekim 2021)

[50] Dastin, Jeffrey; (2021), "Amazon extends moratorium on police use of facial recognition software", *Reuters*, (18 Mayıs 2021), https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/. (Erişim Tarihi: 2 Ekim 2021)

[51] Chee, Foo Yun; (2020), "EU mulls five-year ban on facial recognition tech in public areas", *Reuters*, (16 Ocak 2020), https://www.

reuters.com/article/uk-eu-ai/eu-mulls-five-year-ban-on-facial-recognition-tech-in-public-areas-idUKKBN1ZF2QN?edition-redirect=uk. (Erişim Tarihi: 2 Ekim 2021)

[52] *Uluslararası Af Örgütü*, (2020), "ABD: Yüz tanıma teknolojisinin kitlesel gözetimde kullanılması yasaklansın", (17 Haziran 2020), https://www.amnesty.org.tr/icerik/abd-yuz-tanima-teknolojisinin-kitlesel-gozetimde-kullanilmasi-yasaklansin. (Erişim Tarihi: 2 Ekim 2021)

[53] Grother, Patrick; (2021), "Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification", (10 Eylül 2021), *National Institute of Standards and Technology*, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf. (Erişim Tarihi: 2 Ekim 2021)

[54] Dirini, İlden; (2021), "Yüz ve uzaktan biyometrik tanıma kullanımları küresel olarak yasaklanmalıdır!", Alternatif Bilişim, (7 Haziran 2021), https://alternatifbilisim.org/yuz-ve-uzaktan-biyometrik-tanima-kullanimlari-kuresel-olarak-yasaklanmalidir/. (Erişim Tarihi: 2 Ekim 2021)

[55] O'Donnell, Lindsey; (2019), "Researchers Bypass Apple FaceID Using Biometrics 'Achilles Heel'", *threat post*, (8 Ağustos 2019), https://threatpost.com/researchers-bypass-apple-faceid-using-biometrics-achilles-heel/147109/. (Erişim Tarihi: 2 Ekim 2021)

[56] Biometric Technology Today, (2013), "Researchers show facial recognition could ID Boston bombers from CCTV", *Science Direct*, (Haziran 2013), https://www.sciencedirect.com/science/article/abs/pii/S0969476513700973. (Erişim Tarihi: 2 Ekim 2021)

[57] *The Wall Street Journal*, (2016), "Chinese Researchers Invent New Police Car That Can Scan Criminals' Faces", (25 Mart 2016), https://www.wsj.com/articles/BL-CJB-28938. (Erişim Tarihi: 2 Ekim 2021)

[58] Tao, Li; (2018), "Malaysian police wear Chinese start-up's AI camera to identify suspected criminals", *South China Morning Post*, (20 Nisan 2018), https://www.scmp.com/tech/social-gadgets/article/2142497/malaysian-police-wear-chinese-start-ups-ai-camera-identify. (Erişim Tarihi: 2 Ekim 2021)

[59] *Interpol*, "Facial Recognition", https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition. (Erişim Tarihi: 2 Ekim 2021)

[60] *Istanbul Airport*, "Hızlı Pasaport Geçiş Sistemi", https://www.istairport.com/tr/yolcu/havalimani-rehberi/havalimani-hizmetleri/hizli-pasaport-gecis-sistemi. (Erişim Tarihi: 2 Ekim 2021)

[61] *World Travel & Tourism Council*, (2021), "Global Guidelines For Safe & Seamless Traveller Journey", https://wttc.org/Portals/0/Documents/Reports/2021/SSTJ-Biometrics%20and%20Digital%20Identity%20Global%20Guidelines.pdf?ver=2021-02-27-120737-970. (Erişim Tarihi: 2 Ekim 2021)

[62] Porter, Jon; (2019), "US facial recognition will cover 97 percent of departing airline passengers within four years", *The Verge*, (18 Nisan 2019), https://www.theverge.com/2019/4/18/18484581/us-airport-facial-recognition-departing-flights-biometric-exit. (Erişim Tarihi: 2 Ekim 2021)

[63] Abadicio, Millicent; (2020) "Facial Recognition in the Military – Current Applications", *EMERJ*, (17 Şubat 2020), https://emerj.com/ai-sector-overviews/facial-recognition-in-the-military-current-applications/. (Erişim Tarihi: 2 Ekim 2021)

[64] Mitchell, Billy; (2020), "DDS launches biometric app to identify friends, foes on battlefield", *FEDSCOOP*, (14 Temmuz 2020), https://www.fedscoop.com/dds-biometric-battlefield-app/. (Erişim Tarihi: 2 Ekim 2021)

[65] *Tech Link*, "Adaptive facial recognition software requires little training data", https://techlinkcenter.org/technologies/adaptive-facial-recognition-software-requires-little-training-data/c89f8eee-61b6-444d-813a-943540727f42. (Erişim Tarihi: 2 Ekim 2021)

[66] Cox, Matthew; (2019), "Army's Next Infantry Weapon Could Have Facial-Recognition Technology", *Military.com*, (1 Haziran 2019), https://www.military.com/daily-news/2019/06/01/armys-next-infantry-weapon-could-have-facial-recognition-technology.html. (Erişim Tarihi: 2 Ekim 2021)

[67] *Interpol*, "Identifying terrorist suspects", https://www.interpol.int/Crimes/Terrorism/Identifying-terrorist-suspects. (Erişim Tarihi: 2 Ekim 2021)

[68] Steinhauer, Joshua; (2014), "US Biometric and Identity Intelligence Programme", *KEESING PLATFORM*, (1 Ekim 2014), https://platform.keesingtechnologies.com/us-biometric-and-identity-intelligence-programme-3/. (Erişim Tarihi: 2 Ekim 2021)

[69] *Wired*, (2011), "CSI bin Laden: Commandos Use Thumb, Eye Scans to Track Terrorists", (2 Mayıs 2011), https://www.wired.com/2011/05/csi-bin-laden-commandos-use-thumb-eye-scans-to-track-terrorists/. (Erişim Tarihi: 2 Ekim 2021)

[70] Greene, Tristan; (2021), "The US Army is developing a nightmarish thermal facial recognition system", *The next web,* (11 Ocak 2021), https://thenextweb.com/news/the-us-army-is-developing-a-nightmarish-thermal-facial-recognition-system. (Erişim Tarihi: 2 Ekim 2021)

[71] *STM ThinkTech*, (2019), "Biyometri ve Kimlik Teknolojisine En Çok Yatırım Yapan Ülkeler, (21 Ocak 2019), https://thinktech.stm.com.tr/detay.aspx?id=198. (Erişim Tarihi: 2 Ekim 2021)

[72] Garvie, Clare; (2016), "A. DEPLOYMENT", *THE PERPETUAL LINE-UP*, (18 Ekim 2016), https://www.perpetuallineup.org/findings/deployment. (Erişim Tarihi: 2 Ekim 2021)

[73] Schuppe, Jon; (2019), "How facial recognition became a routine policing tool in America", *NBC News*, (11 Mayıs 2019), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251. (Erişim Tarihi: 2 Ekim 2021)

[74] *United States Government Accountability Office*, (2021), "FACIAL RECOGNITION TECHNOLOGY Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks", (Haziran 2021), https://www.gao.gov/assets/gao-21-518.pdf. (Erişim Tarihi: 2 Ekim 2021)

[75] Gershgorn, Dave; (2020), "The DHS Is Working to Access 300 Million More Facial Recognition Photos", *Onezero*, (29 Mayıs 2020), https://onezero.medium.com/the-dhs-is-working-to-access-300-million-more-facial-recognition-photos-eef02e3ccb4b. (Erişim Tarihi: 2 Ekim 2021)

[76] Risen, James; Poitras, Laura; (2014), "N.S.A. Collecting Millions of Faces From Web Images", *The New York Times*, (1 Haziran 2014), http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html?_r=1. (Erişim Tarihi: 2 Ekim 2021)

[77] *U.S. Customs and Border Protection*, "CBP Introduces Simplified Arrival at GUM in Guam, CNMI",

https://www.cbp.gov/newsroom/local-media-release/cbp-introduces-simplified-arrival-gum-guam-cnmi. (Erişim Tarihi: 2 Ekim 2021)

[78] *Clearview.ai*, "WE ARE CLEARVIEW AI", https://clearview.ai/overview. (Erişim Tarihi: 2 Ekim 2021)

[79] Reyes, Hercules; (2021), "US Army Using Controversial Facial Recognition AI: Report", *The Defense Post*, (25 Ağustos 2021), https://www.thedefensepost.com/2021/08/25/us-army-clearview-ai/. (Erişim Tarihi: 2 Ekim 2021)

[80] Hill, Kashmir;, (2020), "The Secretive Company That Might End Privacy as We Know It", *The New York Times*, (18 Kasım 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. (Erişim Tarihi: 2 Ekim 2021)

[81] Fowler, Patrick; (2019), "Facing the Issue: San Francisco Bans City Use of Facial Recognition Technology", JDSUPRA, (15 Temmuz 2019), https://www.jdsupra.com/legalnews/facing-the-issue-san-francisco-bans-35144/#:~:text=On%20May%2021%2C%202019%2C%20the,police%20and%20other%20city%20agencies.&text=The%20ordinance%20bans%20facial%20recognition,including%20police%20and%20transit%20authorities. (Erişim Tarihi: 2 Ekim 2021)

[82] Lannan, Katie; (2019), "Somerville Bans Government Use Of Facial Recognition Tech", wbur, (28 Haziran 2019), https://www.wbur.

org/news/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech . (Erişim Tarihi: 2 Ekim 2021)

[83] Maass, Dave; (2019), "Victory: San Diego to Suspend Face Recognition Program, Limits ICE Access To Criminal Justice Data", *Electronic Frontier Foundation*, (11 Aralık 2019), https://www.eff.org/deeplinks/2019/12/victory-san-diego-suspend-face-recognition-program-cuts-some-ice-access. (Erişim Tarihi: 2 Ekim 2021)

[84] Hamilton, Brent; Berry, Kate; (2021), "Portland Becomes First Jurisdiction to Ban Certain Uses of Facial Recognition by Private Businesses" , *Davis Wright Tremaine LLP*, (21 Ocak 2021), https://www.dwt.com/blogs/privacy--security-law-blog/2021/01/portland-facial-recognition-ban. (Erişim Tarihi: 2 Ekim 2021)

[85] *Lifars*, (2019), "Army is advancing facial recognition technology", (2 Eylül 2019), https://lifars.com/2019/09/army-is-advancing-facial-recognition-technology/. (Erişim Tarihi: 2 Ekim 2021)

[86] Hsu, Jeremy; (2021), "Army Trains AI to Identify Faces in the Dark", *IEEE Spectrum*, (9 Mart 2021), https://spectrum.ieee.org/army-trains-ai-to-identify-faces-in-the-dark. (Erişim Tarihi: 2 Ekim 2021)

[87] SINGH BISHT, INDER; (2021), "US Army Calls for Facial Recognition Tech to Secure Bases", *The Defense Post*, (6 Nisan 2021), https://www.thedefensepost.com/2021/04/06/us-army-facial-recognition-bases/. (Erişim Tarihi: 2 Ekim 2021)

[88] Jingli, Song; (2019), "Chinese AI giant SenseTime sees valuation surge above USD 7.5 billion", *KrASIA*, (5 Eylül 2019), https://kr-asia.com/sensetime-says-its-valued-at-usd-7-5-billion-and-in-no-ipo-rush. (Erişim Tarihi: 2 Ekim 2021)

[89] Xiang, Nina; (2018), "China's AI Industry Has Given Birth To 14 Unicorns: Is It A Bubble Waiting To Burst?", *The Forbes*, (5 Ekim 2018), https://www.forbes.com/sites/ninaxiang/2018/10/05/chinas-ai-industry-has-given-birth-to-14-unicorns-is-it-a-bubble-waiting-to-pop/?sh=150721ae46c3. (Erişim Tarihi: 2 Ekim 2021)

[90] Wang, Eudora; (2018), "China To Take Nearly Half Of Global Face Recognition Device Market By 2023", *China Money Network*, (23 Ağustos 2018), https://www.chinamoneynetwork.com/2018/08/23/china-to-take-nearly-half-of-global-face-recognition-device-market-by-2023. (Erişim Tarihi: 2 Ekim 2021)

[91] Donnelly, Drew; (2021), "An Introduction to the China Social Credit System", *New Horizons*, (15 Eylül 2021), https://nhglobalpartners.com/china-social-credit-system-explained/. (Erişim Tarihi: 2 Ekim 2021)

[92] *MERICS*, "China's Social Credit System in 2021: From fragmentation towards integration", https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration. (Erişim Tarihi: 2 Ekim 2021)

[93] *Atlantic Council*, (2020), "The West, China, and AI surveillance", (18 Aralık 2020), https://www.atlanticcouncil.org/blogs/geotech-cues/the-west-china-and-ai-surveillance/. (Erişim Tarihi: 2 Ekim 2021)

[94] *The Washington Post*, (2020), "Huawei tested AI software that tould recognize Uighur minorities alert police report says", (8 Aralık 2020), https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/. (Erişim Tarihi: 2 Ekim 2021)

[95] Bhandari, Bibek; (2018), "Face Recognition Glasses Augment China's Railway Cops", Sixth Tone, (6 Şubat 2018), https://www.sixthtone.com/news/1001676/face-recognition-glasses-augment-chinas-railway-cops. (Erişim Tarihi: 2 Ekim 2021)

[96] Francis Chan, Tara; (2018), "Beijing police are using facial-recognition glasses to identify car passengers and number plates", Business Insider, (12 Mart 2018), https://www.businessinsider.com/china-police-using-smart-glasses-facial-recognition-2018-3. (Erişim Tarihi: 2 Ekim 2021)

[97] Yiwei, Wang; (2017), "Shanghai Traffic Violators Identified With Facial Recognition", (20 Eylül 2017), https://www.sixthtone.com/news/1000882/shanghai-traffic-violators-identified-with-facial-recognition. (Erişim Tarihi: 2 Ekim 2021)

[98] *National Institute of Standards and Technology*, (2021), "FRVT 1:N Identification", (21 Eylül 2021), https://pages.nist.gov/frvt/html/frvt1N.html. (Erişim Tarihi: 2 Ekim 2021)

[99] SHIMIZU, KOSUKE; (2019), "Japan in race with China for facial-recognition supremacy", *Nikkei Asia*, (20 Aralık 2019), https://asia.nikkei.com/Business/Business-trends/Japan-in-race-with-China-for-facial-recognition-supremacy. (Erişim Tarihi: 2 Ekim 2021)

[100] *BBC*, "Facial recognition identifies people wearing masks", https://www.bbc.com/news/technology-55573802. (Erişim Tarihi: 2 Ekim 2021)

[101] *NEC*, (2021), "NEC to provide facial recognition system for new "Face Express" check-in to boarding process at Narita and Haneda Airports", (25 Mart 2021), https://www.nec.com/en/press/202103/global_20210325_02.html. (Erişim Tarihi: 2 Ekim 2021)

[102] Mayhew, Stephen; (2017), "Ntechlab wins two categories at Face Recognition Prize Challenge", *Biometric Update*, (7 Kasım 2017), https://www.biometricupdate.com/201711/ntechlab-wins-two-categories-at-face-recognition-prize-challenge. (Erişim Tarihi: 2 Ekim 2021)

[103] *Rostec*, (2019), "Rostec Will Start Exporting Face Recognition Technology to the Armed Forces", (25 Nisan 2019), https://rostec.ru/en/news/rostec-will-start-exporting-face-recognition-technology-to-the-armed-forces/. (Erişim Tarihi: 2 Ekim 2021)

[104] Bendett, Samuel; (2019), "Moscow to Weave AI Face Recognition into Its Urban Surveillance Net", *Defense One*, (14 Mayıs 2019), https://www.defenseone.com/technology/2019/05/moscow-weave-ai-face-recognition-its-urban-surveillance-net/156994/. (Erişim Tarihi: 2 Ekim 2021)

[105] *VOA*, (2021), "'Racist' Facial Recognition Sparks Ethical Concerns in Russia, Analysts Say", (5 Temmuz 2021), https://www.voanews.com/europe/racist-facial-recognition-sparks-ethical-concerns-russia-analysts-say. (Erişim Tarihi: 2 Ekim 2021)

[106] Reevell, Patrick; (2020), "How Russia is using facial recognition to police its coronavirus lockdown", *ABC News*, (30 Nisan 2020), https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736. (Erişim Tarihi: 2 Ekim 2021)

[107] *Rostec*, (2019), "Rostec Introduces BrainReader Neuro Interface to the International Market", (25 Nisan 2019), https://rostec.ru/en/news/rostec-introduces-brainreader-neuro-interface-to-the-international-market/. (Erişim Tarihi: 2 Ekim 2021)

[108] *Readwrite*, (2020), "Does Artificial Intelligence Help Fight Financial Fraud?", (16 Ocak 2020), https://readwrite.com/2020/01/16/does-artificial-intelligence-help-fight-financial-fraud/?__cf_chl_managed_tk__=pmd_nmWoIBB3OROLJH0VioEd0Pf5BqReEMVT._fDyIQ7kt0-1633168626-0-gqNtZGzNAzujcnBszRQ9. (Erişim Tarihi: 2 Ekim 2021)

[109] Ajmal, Anam; (2020), "Ministries & several states deploying facial recognition tech systems: Study", *Times of India*, (28 Kasım 2020), https://timesofindia.indiatimes.com/india/ministries-several-states-deploying-facial-recognition-tech-systems-study/articleshow/79455779.cms. (Erişim Tarihi: 2 Ekim 2021)

[110] Mohan, Vijay; (2020), "Coronavirus: DRDO developing AI-based face recognition system for marking attendance", *The Tribune*, (20 Mayıs 2020), https://www.tribuneindia.com/news/nation/coronavirus-drdo-developing-ai-based-face-recognition-system-for-marking-attendance-87420. (Erişim Tarihi: 2 Ekim 2021)

[111] Pascu, Luana; (2020), "Israeli military-grade biometric facial recognition works with face masks", *Biometric Update*, (13 Nisan 2020), https://www.biometricupdate.com/202004/israeli-military-grade-biometric-facial-recognition-works-with-face-masks. (Erişim Tarihi: 2 Ekim 2021)

[112] Klein Leichman, Abigail; (2016), "6 futuristic Israeli biometric techs that will transform our lives", Israel21c, (10 Ekim 2016), https://www.israel21c.org/6-futuristic-israeli-biometric-techs-that-will-transform-our-lives/. (Erişim Tarihi: 2 Ekim 2021)

[113] *The New Arab*, (2019), "Israeli army using 'artificial intelligence, facial recognition' to track Palestinian civilians", (15 Mayıs 2019), https://english.alaraby.co.uk/news/israeli-army-using-artificial-intelligence-track-palestinian-civilians. (Erişim Tarihi: 2 Ekim 2021)

[114] *The Times of Israel*, (2021), "US firms said using Israeli tech for controversial facial recognition", (21 Nisan 2021), https://www.timesofisrael.com/us-firms-said-using-israeli-tech-for-controversial-facial-recognition/. (Erişim Tarihi: 2 Ekim 2021)

[115] Keller John; (2021), "Military researchers ask industry to develop long-range biometrics and facial recognition algorithms", *Military & Aerospace Electronics*, (8 Ocak 2021), https://www.militaryaerospace.com/sensors/article/14189954/facial-recognition-long-range-biometrics. (Erişim Tarihi: 2 Ekim 2021)

[116] Hambling, David; (2020), "US military face recognition system could work from 1 kilometre away", *New Scientist* (15 Şubat 2020), https://www.newscientist.com/article/2233639-us-military-face-recognition-system-could-work-from-1-kilometre-away/. (Erişim Tarihi: 2 Ekim 2021)

[117] *Savunmasanayi.org*, (2020), "DRONE İLE YERLİ YÜZ TANIMA SİSTEMİ", (3 Nisan 2020), https://www.savunmasanayi.org/drone-ile-yerli-yuz-tanima-sistemi/. (Erişim Tarihi: 2 Ekim 2021)

[118] R. Aguiar, Alberto; (2021), "Drones with facial recognition are closer to becoming a reality thanks to a patent from an Israeli company", *Business Insider*, (17 Şubat 2021), https://www.businessinsider.com/httpswwwbusinessinsideresdrones-reconocimiento-facial-cerca-ser-realidad-812285. (Erişim Tarihi: 2 Ekim 2021)

[119] Singh, Ishveena; (2021), "AI-powered facial recognition drones track criminals in UAE", *DroneDJ*, (26 Nisan 2021), https://dronedj.com/2021/04/26/facial-recognition-drones-sharjah-police/. (Erişim Tarihi: 2 Ekim 2021)

[120] Harper, Nicole; (2020), "5G's Impact on Financial Services Even Greater in a Post-Pandemic Society", *Credit Union Times*, (7 Ağustos 2020), https://www.cutimes.com/2020/08/07/5gs-impact-on-financial-services-even-greater-in-a-post-pandemic-society/?slreturn=20210731134937. (Erişim Tarihi: 2 Ekim 2021)

[121] Beinart, Matthew; (2018), "Army Research Lab Awards Awards $25 Million Grant For IoBT Device Network Concepts", *Defense Daily*, (21 Şubat 2021), https://www.defensedaily.com/army-research-lab-awards-awards-25-million-grant-iobt-device-network-concepts/cyber/. (Erişim Tarihi: 2 Ekim 2021)

[122] Cameron, Lori; "Internet of Things Meets the Military and Battlefield", *IEEE Computer Society*, https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt. (Erişim Tarihi: 2 Ekim 2021)

[123] *Analytics Insight*, (2020), "THE FUTURE OF BIOMETRICS IOT", (3 Nisan 2020), https://www.analyticsinsight.net/the-future-of-biometric-iot/. (Erişim Tarihi: 2 Ekim 2021)

[124] *STM ThinkTech*, (2018), "Eğilimleri Önceden Tahmin Eden Büyük Veri Platformu", (21 Mart 2018), https://thinktech.stm.com.tr/detay.aspx?id=116. (Erişim Tarihi: 2 Ekim 2021)

[125] Haskins, Caroline; (2019), "Academics Confirm Major Predictive Policing Algorithm is Fundamentally Flawed", *VICE*, (14 Şubat 2019), https://www.vice.com/en_us/article/xwbag4/academics-confirm-major-predictive-policing-algorithm-is-fundamentally-flawed. (Erişim Tarihi: 2 Ekim 2021)

[126] Haskins, Caroline; (2020), "The Los Angeles Police Department Says It Is Dumping A Controversial Predictive Policing Tool", *BuzzFeed.News*, (21 Nisan 2020), https://www.buzzfeednews.com/article/carolinehaskins1/los-angeles-police-department-dumping-predpol-predictive. (Erişim Tarihi: 2 Ekim 2021)

[127] Lomas, Natasha; (2021), "'Orwellian' AI lie detector project challenged in EU court", *Tech Crunch*, (5 Şubat 2021), https://techcrunch.com/2021/02/05/orwellian-ai-lie-detector-project-challenged-in-eu-court/. (Erişim Tarihi: 2 Ekim 2021)

[128] *Recfaces*, (2021), "Emotion Recognition: Introduction to Emotion Reading Technology", (3 Mart 2021), https://recfaces.com/articles/emotion-recognition. (Erişim Tarihi: 2 Ekim 2021)

[129] Borak, Masha; (2020), "Didi detects drowsy drivers with AI facial recognition", *South China Morning Post*, (10 Ocak 2020), https://www.scmp.com/abacus/news-bites/article/3045621/didi-detects-drowsy-drivers-ai-facial-recognition. (Erişim Tarihi: 2 Ekim 2021)

[130] Huang, Yan; (2019), "Suicidal Ideation Detection via Social Media Analytics", *Research Gate*, (Aralık 2019), https://www.researchgate.net/publication/338696833_Suicidal_Ideation_Detection_via_Social_Media_Analytics. (Erişim Tarihi: 2 Ekim 2021)

[131] Pentland, Alex; (1999), Personalization Smart Environments: Face Recognition for Human Interaction, *Massachusetts Institute of Technology*, (8 Ekim 1999),

https://dam-prod.media.mit.edu/x/files/tech-reports/TR-516.pdf. (Erişim Tarihi: 2 Ekim 2021)

[132] Ferwerda, Bruce; Schedl, Markus; (2014), "Enhancing Music Recommender Systems with Personality Information and Emotional States: A Proposal", *Johannes Kepler University*,

http://www.cp.jku.at/people/schedl/Research/Publications/pdf/ferwerda_empire_2014.pdf. (Erişim Tarihi: 2 Ekim 2021)

[133] *Caltech*, (2017), "Neural Networks Model Audience Reactions to Movies", (21 Temmuz 2017), https://www.caltech.edu/about/news/neural-networks-model-audience-reactions-movies-79098. (Erişim Tarihi: 2 Ekim 2021)

[134] *Workable*, "Workable partners with Human machine learning provider to bring AI to recruiting", https://blog.workable.com/workable-integrates-with-human/. (Erişim Tarihi: 2 Ekim 2021)

[135] *Venture Boat*, (2018), "Chinese school installs facial recognition cameras to monitor students", (17 Mayıs 2018), https://venturebeat.com/2018/05/17/chinese-school-installs-facial-recognition-cameras-to-monitor-students/. (Erişim Tarihi: 2 Ekim 2021)

[136] Thomas, Daniel; (2018), "The cameras that know if you're happy - or a threat", *BBC*, (17 Temmuz 2018), https://www.bbc.com/news/business-44799239. (Erişim Tarihi: 2 Ekim 2021)

[137] Fino, Edita; (2019), "Unfolding political attitudes through the face: facial expressions when reading emotion language of left- and right-wing political leaders", *Nature*, (30 Ekim 2019), https://www.nature.com/articles/s41598-019-51858-7. (Erişim Tarihi: 2 Ekim 2021)

[138] *European Commission*, "What is Horizon 2020?", https://ec.europa.eu/programmes/horizon2020/what-horizon-2020. (Erişim Tarihi: 2 Ekim 2021)

[139] Heaven, Douglas; (2020), "Why faces don't always tell the truth about feelings", *Nature*, (26 Şubat 2020), https://www.nature.com/articles/d41586-020-00507-5. (Erişim Tarihi: 2 Ekim 2021)

[140] Hambling, David; (2019), "The Pentagon has a laser that can identify people from a distance—by their heartbeat", *MIT Technology Review*, (27 Haziran 2019), https://www.technologyreview.com/s/613891/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/. (Erişim Tarihi: 2 Ekim 2021)

[141] DONCASTER, KEVIN; TANGERMANN, VICTOR; (2019), "NEW LASER CAN IDENTIFY PEOPLE FROM A DISTANCE BY THEIR HEARTBEAT", *Futurism*, (27 Haziran 2019), https://futurism.com/the-byte/laser-identify-distance-heartbeat. (Erişim Tarihi: 2 Ekim 2021)

[142] Dai, Sarah; (2019), "Chinese police test gait-recognition technology from AI start-up Watrix that identifies people based on how they walk", *South China Morning Post*, (26 Şubat 2019), https://www.scmp.com/tech/start-ups/article/2187600/chinese-police-surveillance-gets-boost-ai-start-watrix-technology-can. (Erişim Tarihi: 2 Ekim 2021)

thinktech
STM Teknolojik Düşünce Merkezi
http://thinktech.stm.com.tr