

T.C.
POLİS AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ
ULUSLARARASI GÜVENLİK ANABİLİM DALI

GÖÇ KONTROL MEKANİZMASI OLARAK BİYOMETRİK
SİSTEMLERİN ETKİNLİĞİ:
AVRUPA BİRLİĞİ VE AMERİKA BİRLEŞİK DEVLETLERİ
UYGULAMALARININ TÜRKİYE'YE ETKİSİ

DOKTORA TEZİ

Osman Nihat ŞEN

Danışman

Prof. Dr. Arif KÖKTAŞ

Ankara - 2012

T.C.
POLİS AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ
ULUSLARARASI GÜVENLİK ANABİLİM DALI

GÖÇ KONTROL MEKANİZMASI OLARAK BİYOMETRİK
SİSTEMLERİN ETKİNLİĞİ:
AVRUPA BİRLİĞİ VE AMERİKA BİRLEŞİK DEVLETLERİ
UYGULAMALARININ TÜRKİYE'YE ETKİSİ

DOKTORA TEZİ

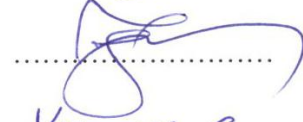
Osman Nihat ŞEN

Bu tez 04 / 06 / 2012 tarihinde aşağıdaki jüri tarafından **Oybirliği**/Oyçokluğu ile kabul edilmiştir.

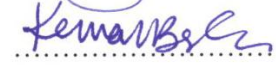
Jüri Başkanı: Prof. Dr. Arif KÖKTAŞ



Üye: Prof. Dr. Mehmet ÖZCAN



Üye: Prof. Dr. Kemal BAŞLAR



Üye: Doç. Dr. Sema BUZ



Üye: Yrd. Doç. Dr. Mustafa DÖNMEZ



T.C.
POLİS AKADEMİSİ BAŞKANLIĞI
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Doktora tezi olarak sunduğum bu çalışmayı bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde yollama yaparak yararlandığımı belirtir; bunu şerefimle beyan ederim.

Enstitü veya başka herhangi bir mercii tarafından belli bir zamana bağlı kalmaksızın, tezimle ilgili bu beyana aykırı bir durumun tespit edilmesi durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

21/04/2012

Osman Nihat ŞEN

ÖNSÖZ

Bu çalışmayı yapma konusunda bana fikir veren ve yol gösteren hocam Prof. Dr.Sn.Bülent ÇİÇEKLİ'ye teşekkür ederim. Çalışma sırasında bana her türlü yardım ve danışmanlıkta bulunarak desteğini ve zamanını hiç bir zaman esirgemeyen Danışmanım Prof. Dr. Sn.Arif KÖKTAŞ ile çeşitli konularda öneri ve fikir desteğinde bulunarak özgün bir çalışma olmasında yol gösteren tez danışmanlarım Prof. Dr. Sn.Mehmet ÖZCAN ve Prof. Dr. Sn.Kemal BAŞLAR hocalarıma engin saygılarımla teşekkürlerimi sunarım.

Kaynak olarak yardımcı olan Emniyet Genel Müdürlüğü Pasaport Daire Başkanı 1. Sınıf Emniyet Müdürü Sn. Metin AŞIK ve Emniyet Genel Müdürlüğü Pasaport Daire Başkanlığı çalışanları ile Dr. Nuri TEMUR, Mehmet Bedii KAYA ve Ahmet ÇUBUKÇU'ya teşekkür ederim.

Bu çalışmayı yapma konusunda bana önderlik eden Bilgi Teknolojileri ve İletişim Kurumu Başkanı Sn. Dr. Tayfun ACARER'e ve çalışmayı yaparken moral ve motivasyon desteği veren Telekomünikasyon İletişim Başkanı Sn. Fethi ŞİMŞEK'e teşekkürlerimi takdim ederim. Çalışma arkadaşlarım Sn. Basri AKTEPE, Sn. Mustafa AKAR, Sn. Abdulkadir MAHMUTOĞLU, Sn. Barış YASLAN ve Sn. İlhan ELİEYİÖĞLU'na da destekleri için teşekkür ederim. Tezimin yazımında bazı düzeltmeler yaparak katkı sunan arkadaşlarıma özellikle teşekkür ederim.

Eşim Hikmet ve çocuklarım Nedret, Nimet ve Sedat'ın maddi ve manevi destekleri, bu çalışmayı yaparken bana tahammülleri sonsuz müteşekkiri olduğum önemli bir ailevi destek olmuştur. Son olarak, büyük fedakarlıklarla yetiştirmemi sağlayan sevgili annem Gülseren ŞEN ve sevgili babam Hasan ŞEN'e şükranlarımı sunarım.

ÖZET

Şen, Osman Nihat, (2012), Göç Kontrol Mekanizması Olarak Biyometrik Sistemlerin Etkinliği: Avrupa Birliği ve Amerika Birleşik Devletleri Uygulamalarının Türkiye'ye Etkisi, Doktora Tezi, Danışman: Prof. Dr. Arif Köktaş, 171 sayfa.

Göç ve güvenlik kavramları arasındaki ilişki 11 Eylül 2001 tarihinde ABD’de yaşanan terör olayı ve bu olaya karışan teröristlerin yabancı olmaları ile birlikte önemli bir konu haline gelmiştir. Ülkeler, hem yasadışı göçü engellemek hem de sınır güvenliğini daha etkin hale getirmek için farklı önlemler almaktadır. Göç yönetiminde uygulamaya konan tedbirlerden bir tanesi biyometrik sistemlerin kullanılmasıdır. Günümüzde birçok ülkede pasaportlarda, vize işlemlerinde ve sınır kapılarında biyometrik sistemler kullanılmaktadır. Biyometrik sistemler güvenliği artırmak ve sık seyahat eden yolcuların işlemlerini hızlandırmak üzere kullanılmaktadır. AB ve ABD uygulamaları, bu kapsamda detaylı olarak tartışılmaktadır. Bahsedilen iki uygulama, diğer ülkelerle birlikte Türkiye’ye de etki etmiştir. Bu çalışmada, göç kontrol mekanizması olarak biyometrik sistemlerin, uluslararası sınır kontrol uygulamalarında kullanımı ve etkinliği incelenmektedir. Göç kontrol yönetiminde kullanılan biyometrik sistemlerin avantajları ile dezavantajları etkinlik kapsamında tartışılmaktadır. Çalışma kapsamında varılan sonuç; göç yönetiminde biyometrik sistem kullanımının yasadışı göçü önleme ve sınırların güvenliğini artırma bağlamında katkısının somut verilerle ispatlanmadığı gerçeğidir.

Anahtar Kelimeler: Biyometrik pasaport, biyometrik sistemlerin avantajları, biyometrik sistemlerin dezavantajları, biyometrik sistemlerin etkinliği.

ABSTRACT

Şen, Osman Nihat, (2012), Effectiveness of Biometric Systems as an Immigration Control Mechanism: European Union and United States of America Implementations' Influence on Turkey, PhD Thesis, Supervisor: Prof. Dr. Arif Köktaş, 171 pages.

With the terrorist attacks occurred in USA in 11 September 2001 and as the terrorists who have committed to these attacks were foreigners, the relation between immigration and security notions became an important topic. Both to prevent illegal immigration and to ensure more effective border security, countries take different precautions. One of the measures that put into practice is usage of biometric systems. Nowadays biometric systems are used in a lot of countries for passports, visa processes and at border gates. Biometric systems are used to improve safety and accelerate frequently traveling passengers' border processes. EU and USA implementations, within this scope, are discussed in detail. These two implementations, affected Turkey including with other countries. In this study, the usage and effectiveness of biometric systems as control mechanism of migration in international border control is reviewed. Advantages and disadvantages of biometric systems are discussed in the scope of effectiveness. The conclusion of this study is; contribution of usage of biometric systems to prevent illegal migration and improvement of border security in administration of migration cannot be shown concretely.

Key Words: Biometric passport, advantages of biometric systems, disadvantages of biometric systems, effectiveness of biometric systems.

İÇİNDEKİLER

Sayfa

ÖNSÖZ.....	IV
ÖZET.....	V
ABSTRACT	VI
İÇİNDEKİLER	VII
KISALTMALAR	X
TABLolar	XII
ŞEKİLLER	XIII
RESİMLER	XIV
GİRİŞ	1

BİRİNCİ BÖLÜM

BİYOMETRİ

1.1. TANIM.....	12
1.2. BİYOMETRİK TARAMA AŞAMALARI	13
1.3. TANIMA VE DOĞRULAMA	15
1.4. BİYOMETRİK SİSTEM TÜRLERİ	17
1.4.1. Parmak İzi Tanıma (<i>Fingerprint Recognition</i>)	17
1.4.2. Yüz Tanıma (<i>Facial Recognition</i>)	19
1.4.3. İris ve Retina Tarama (<i>Iris and Retina Recognition</i>).....	20
1.4.4. Ses Tanıma (<i>Voice Recognition</i>)	23
1.4.5. El ve Parmak Geometrisi Tanıma (<i>Hand Geometry Recognition</i>).....	24
1.4.6. İmza Tanıma (<i>Signature Recognition</i>)	27
1.5. BİYOMETRİK SİSTEMLERİN BAŞARISI	28
1.6. BİYOMETRİK SİSTEMLERİN KULLANIM ALANLARI ve AMAÇLARI	31
1.7. BİYOMETRİ DEĞERLENDİRMESİ VE BİYOMETRİNİN GELECEĞİ33	
1.8. BÖLÜM ÖZETİ	36

İKİNCİ BÖLÜM

GÖÇ POLİTİKALARI

2.1. AVRUPA BİRLİĞİ GÖÇ POLİTİKASI	41
2.1.1. AB Ortak Göç Politikası	43
2.1.2. AB Göç Politikasında Son Gelişmeler	45
2.2. AMERİKA BİRLEŞİK DEVLETLERİ GÖÇ POLİTİKASI	48
2.2.1. Vatanseverlik Yasası (<i>USA Patriot Act, 2001</i>)	52
2.2.2. Sınır Güvenliğinin Artırılması ve Vize Reform Yasası (<i>The Enhanced Border Security and Visa Entry Reform Act of 2002</i>)	53
2.2.3. İç Güvenlik Örgütü Yasası (<i>Homeland Security Act, 2002</i>)	54
2.3. AB VE ABD GÖÇ POLİTİKALARININ DEĞERLENDİRİLMESİ	55
2.4. TÜRKİYE GÖÇ POLİTİKASI	56
2.5. BÖLÜM ÖZETİ	61

ÜÇÜNCÜ BÖLÜM

BİYOMETRİNİN GÖÇ KONTROL MEKANİZMASINDA KULLANILMASI

3.1. YASA DIŞI GÖÇLE MÜCADELE	65
3.2. BİYOMETRİK PASAPORT	67
3.2.1. Uluslararası Sivil Havacılık Örgütü (<i>International Civil Aviation Organization - ICAO</i>)	67
3.2.2. Makine Tarafından Okunabilen Seyahat Belgeleri (<i>Machine-Readable Travel Documents - MRTD</i>)	68
3.2.3. Elektronik Pasaport	70
3.2.4. Biyometrik Pasaport	71
3.3. VİZE İŞLEMLERİNDE VE SINIR KONTROLLERİNDE BİYOMETRİ UYGULAMALARI	72
3.3.1. Avrupa Birliği Uygulaması	75
3.3.1.1. AB Biyometrik Pasaport Düzenlemeleri	76
3.3.1.2. AB Göç Yönetiminde Kurumsal Düzenlemeler	82
3.3.1.3. Avrupa Birliği'nin ABD ile Yolcu Bilgilerini Paylaşması	84
3.3.2. Amerika Birleşik Devletleri Uygulaması	85

3.3.2.1. ABD Ziyaretçi ve Göçmen Statüsünü Gösterge Teknolojisi Programı (The United States Visitor and Immigrant Status Indicator Technology - US- VISIT).....	86
3.3.2.2. ABD Vize Feragat Programı (Visa Waiver Program - VWP).....	89
3.3.2.3. Elektronik Seyahat Yetkilendirmesi (The Electronic System for Travel Authorization - ESTA).....	89
3.3.3. AB ve ABD Uygulamalarının Değerlendirilmesi.....	90
3.3.4. Türkiye Uygulaması	92
3.5. BÖLÜM ÖZETİ	98

DÖRDÜNCÜ BÖLÜM

BİYOMETRİNİN AVANTAJ VE DEZAVANTAJLARI

4.1. AVANTAJLAR	103
4.2. DEZAVANTAJLAR.....	106
4.3. İNSAN HAKLARINA ETKİSİ.....	113
4.3.1. Mahremiyet Hakkı (Right to Privacy).....	114
4.3.2. Kişisel Verilerin Korunması.....	118
4.3.2.1. Kişisel Veri Düzenlemeleri	125
4.3.2.2. Kişisel Veri İlkeleri	129
4.3.2.3. Kişisel Verilerin Korunması Konusunun Değerlendirilmesi.....	132
4.4. ETKİNLİK	133
4.5. AVANTAJLAR İLE DEZAVANTAJLARIN DEĞERLENDİRİLMESİ ve ÖNERİLER	144
4.6. BÖLÜM ÖZETİ.....	148
SONUÇ VE ÖNERİLER.....	151
KAYNAKÇA	159

KISALTMALAR

3D	: Üç Boyutlu
AB	: Avrupa Birliđi
ABD	: Amerika Birleşik Devletleri
AFIS	: Otomatik Parmak İzi Tanıma Sistemi
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AR-GE	: Araştırma Geliştirme
ATM	: Otomatik Banka Makinesi
BM	: Birleşmiş Milletler
DHS	: ABD İç Güvenlik Örgütü
DNA	: Deoksiribo Nükleik Asit
EDPS	: AB Veri Koruma Gözetmeni
ESTA	: ABD Elektronik Seyahat Yetkilendirmesi
EURODAC	: AB Mülteci Bilgi Sistemi
EUROPOL	: Avrupa Polis Ofisi
EUROSUR	: Avrupa Sınır Gözetleme Sistemi
FAR	: Yanlış Kabul Oranı
FNMR	: Yanlışlıkla Kabul Etmeme Oranı
FRONTEX	: Avrupa Birliđi Bütünleşmiş Sınır Yönetimi Birimi
FRR	: Yanlış Ret Oranı
ICAO	: Uluslararası Sivil Havacılık Örgütü
IDENT	: ABD Otomatik Biyometrik Tanımlama Sistemi
IOM	: Uluslararası Göç Örgütü
IRCA	: Göç ve Reform Kontrol Yasası
IRIRA	: Yasa Dışı Göç Reformu ve Göçmen Sorumluluđu Kanunu
MRTD	: Makine Tarafından Otomatik Olarak Okunabilen Seyahat Belgesi
MRZ	: Makine Tarafından Okunabilen Bölge
OECD	: Ekonomik Kalkınma ve İşbirliđi Örgütü
PC	: Kişisel Bilgisayar
PKI	: Açık Anahtar Altyapısı

PNR	: Yolcu Bilgileri
RFID	: Radyo Frekans Tanımlama
SGK	: Sosyal Güvenlik Kurumu
SIRENE	: Ulusal Birimler Üzerinden Ek Bilgi Talebi
SIS	: Schengen Bilgi Sistemi
SIS II	: Geliştirilmiş II. Kademe Schengen Bilgi Sistemi
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
US-VISIT	: ABD Ziyaretçi ve Göçmen Statüsü Gösterge Teknolojisi Programı
VIS	: AB Vize Bilgi Sistemi
VWP	: ABD Vize Feragat Programı

TABLÖLER

Sayfa

Tablo 1: Biyometri Türlerinin Doğrulama Özelliklerinin Karşılaştırılması	16
Tablo 2: Biyometri Türlerinin Genel Özelliklerinin Karşılaştırılması.....	31
Tablo 3: AB Üyesi Bazı Ülkelerin Biyometrik Pasaport Uygulama Tarihleri	81
Tablo 4: Türkiye’de 06 Mart 2012 Tarihi İtibariyle Mevcut Geçerli Pasaport Sayısı	96
Tablo 5: ABD Sınır Görevlilerince Yakalanan Yasa Dışı Göçmenler.....	138
Tablo 6: AB Sınır Kapılarında Yakalanan Yasa Dışı Göçmenler.....	142
Tablo 7: AB Sınır Kapılarında Yakalanan Sahte Seyahat Belgeleri	143

ŞEKİLLER

Sayfa

Şekil 1: Genel Bir Biyometrik Sistemin Elemanları.....	13
Şekil 2: Biyometrik Sistem Tarama Aşamaları	14
Şekil 3: Yüz Tanımada Kullanılan Yüzün Yapısal Bölgeleri.....	20
Şekil 4: Biyometrik Sistem Hata Payı Denge Eğrisi	30
Şekil 5: 2000-2040 Yılları Arasında 25 AB Ülkesinde Nüfus Artışı ve İş Gücü İhtiyacı Grafiği	42
Şekil 6: ICAO 9303 Sayılı Dokümanın Bölümleri.....	68
Şekil 7: 1930-2000 Yılları Arası ABD’de Yakalanan Yasa Dışı Göçmenler	139
Şekil 8: ABD Devletinin 1960-2000 Yılları Arası Göç Harcamaları.....	140
Şekil 9: ABD Devletinin 2004-2009 Yılları Arası Göç Harcamaları.....	141

RESİMLER

Sayfa

Resim 1: Parmak İzi Tanıma Cihazı.....	18
Resim 2: Parmak İzinin Özellikleri	19
Resim 3: İris Resmi	20
Resim 4: İrisin Yapısı.....	21
Resim 5: İris Taramalı Kapı Kontrolü Uygulaması	22
Resim 6: İris Tarama Ünitesi.....	22
Resim 7: Ses Spektrogramı.....	24
Resim 8: Avuç İçi Tarama Sistemi.....	25
Resim 9: Damar Geometrisi Tanıma Cihazı	26
Resim 10: Damar Geometrisi Tanıma Resmi.....	27
Resim 11: İmza Tanıma Tableti Resmi	27
Resim 12: Genel Biyometrik Sistem İşlemleri.....	29
Resim 13: El ve Parmak Geometrisi Tanıma İle Ödeme Sistemi	35
Resim 14: Parmak İzi Tanıma İle Mobil Ödeme Sistemi.....	35
Resim 15: Makine tarafından otomatik olarak okunabilen pasaport (ABD pasaportu)	69
Resim 16: Finlandiya Biyometrik Pasaportu.....	71
Resim 17: Schiphol Havalimanı PRIVIUM İris Tarama Otomatik Geçiş Kapısı.....	73
Resim 18: Frankfurt Havalimanı ABG İris Tarama Otomatik Geçiş Kapısı	73
Resim 19: Charles de Gaulle Havalimanı PEGASE Parmak İzi Tanıma Otomatik Geçiş Kapısı	74
Resim 20: Londra Heathrow Havalimanı IRIS İris Kayıt Bölümü	75
Resim 21: AB Sınır Kapısında Vize Kontrolü Uygulaması	83
Resim 22: US-VISIT Programı Açılış Resmi	87
Resim 23: ABD Sınır Kapısında Vize Kontrolü Uygulaması	88

GİRİŞ

Göç, sınır güvenliği, vize işlemleri ve biyometrik sistemler arasındaki ilişki, 11 Eylül 2001 tarihinde Amerika Birleşik Devletleri'nde yaşanan terör olayları ile İspanya ve İngiltere'de yaşanan terör olayları kapsamında daha önemli bir konu haline gelmiştir. Amerika Birleşik Devletleri'nde 2001 yılında ve Avrupa'da 2004 ile 2005 yıllarında yaşanan terör olayları ülkelerin göç, güvenlik ve özellikle ulusal güvenlik kavramlarına bakış açılarını ciddi oranda etkilemiştir (Aslan, 2010: 50).

Amerika Birleşik Devletleri'nde 11 Eylül 2001 tarihinde yaşanan terör olaylarına karışan teröristlerin yabancı olmaları göç yönetiminin ve sınır kontrollerinin ulusal güvenliğe nasıl etki edebileceğine bir örnek olmuştur (JRC, 2005: 19). Amerika Birleşik Devletleri'nde 11 Eylül 2001 tarihinde yaşanan terör olaylarında uçakları kaçıran teröristler yabancısıdır. Bu kişiler Amerika Birleşik Devletleri'ne yasal vizeler ile girmişlerdir (Stock, 2006: 119; Khanat, 2008: 48). Bununla birlikte, vizelerinin tarihleri geçmiş olmasına rağmen ülkede yasal olmayan bir şekilde kaldıkları (McGowan, 2003: 1) düşünüldüğünde göç yönetiminin ulusal güvenliğe etkisi daha somut olarak anlaşılabilmektedir. Örneğin, 11 Eylül 2001 terör olaylarına karışan yirmi teröristin dördünün yasadışı göçmen, on üçünün Amerika Birleşik Devletleri'ne turist vizesi ile giren ve üçünün ise arananlar listesinde bulunan kişiler olduğu bilinmektedir (Kajevic, 2006: 35).

Amerika Birleşik Devletleri'nde ve Avrupa'da yaşanan terör olayları, zayıf göç yönetiminin, seyahat belgelerindeki güvenlik eksiklerinin ve sınır kontrollerindeki zafiyetlerin ulusal güvenliği ne ölçüde tehdit edebileceğini dikkat çekici bir şekilde göstermiştir. Nitekim 11 Eylül terör olayları ile ilgili hazırlanan ve Amerikan Kongresi'ne sunulan raporda (*9/11 National Commission Report on Terrorist Attacks-2004*¹), Amerika Birleşik Devletleri göç yönetimindeki ve sınır kontrollerindeki eksikliklere dikkat çekilmektedir (Khanat, 2008: 54).

Ulusal güvenliği artırmak maksadıyla, sınır kontrollerinde biyometrik sistemlerin kullanımı ve konuya ilişkin uluslararası işbirliği, hem Amerika Birleşik Devletleri'nin hem de Avrupa Birliği'nin iç ve dış politikada önemli bir gündem

¹ The National Commission on Terrorist Attacks upon the United States, (2004), (<http://www.9-11commission.gov/>, Erişim Tarihi: 25 Aralık 2010).

maddesi haline gelmiştir. Biyometrik sistem kullanılarak sınırların güvenliğinin artırılması ve yasadışı göçle daha etkin mücadele edilmesi, bütün ülkelerin politik gündemidir. Biyometrik sistemlerin sınır kontrollerinde güvenliği artırmak amacıyla kullanılması her geçen gün yaygınlaşmaktadır (Redpath, 2005: 8). Göç yönetiminde biyometrik sistemlerin kullanımının arttığına ve yakın gelecekte daha da artacağına şüphe bulunmamaktadır.

Yasadışı göçü engellemek, sınır güvenliğini daha etkin hale getirmek, vize işlemlerinde hızı artırmak ve doğruluğu sağlamak, nitelikli işçi göçünü kolaylaştırmak ve iyi niyetli seyahat edenler için sınır geçiş işlemlerini kolaylaştırmak amaçlarıyla biyometrik sistemler kullanılmaktadır. Uluslararası göç yönetiminde biyometrik sistemler sınır kapılarında güvenliğin artırılması için uluslararası havacılığın, seyahat belgelerinin ve hedef ülkelerin güvenliğinin geliştirilmesi amaçlarıyla kullanılmaktadır.

Avrupa ülkelerinde ekonomik gelişmeden dolayı birçok sektör için nüfus artış hızı yavaşlığından dolayı nitelikli işçi ihtiyacı duyulmakta ve bu ihtiyacın da her geçen gün artması beklenmektedir. Nitelikli işçi ihtiyacı, üçüncü ülkelere yapılan vasıflı yasal işçi göçü ile karşılanabilmektedir. İlave olarak iyi niyetli ve sık seyahat edenlerin sınır geçiş işlemlerinin kolaylaştırılması da birçok ülkenin gündemindedir. Bütün bu işlemler sınır kontrollerinde biyometrik sistemlerin kullanılmasıyla gerçekleştirilmektedir. Avrupa Birliği'nde kullanılan mavi kart uygulaması bu kapsamda değerlendirilebilen bir uygulamadır. Diğer yandan Fransa, Hollanda, Almanya ve İngiltere gibi ülkelerde kullanılan otomatik sınır geçiş kapıları iyi niyetli seyahat eden yolcuların daha güvenli ve daha hızlı bir şekilde sınır kontrol işlemlerini gerçekleştirmelerine imkân sağlamaktadır (Frontex, 2007: 6). Örneğin, İngiltere'de Heathrow Havalimanında 2006 yılı Ocak ayından bu yana kullanılan iris tanıma sistemi ile kayıtlı yolcular sınır görevlilerine uğramadan gözlerini cihazlara tanıtarak sınır kontrol işlemlerini hızlıca yapabilmektedirler (JRC, 2008: 59). Üstelik İngiltere'deki iris tanıma sisteminde üye olmayı talep eden yolcuların kayıt olma süresi ortalama 5 dakikadır (JRC, 2008: 116).

Sovyetler Birliği'nin 1989 yılında dağılmasından sonra uluslararası göç Avrupa Birliği'nde önemli bir politika gündemi olmuştur. Yaşanan 11 Eylül 2001 terör olayları da Amerika Birleşik Devletleri'nin göç politikasında bazı değişiklikleri

gündeme getirmiştir. Göç kontrol yönetiminin güvenliğini artırmak amacıyla hem Avrupa Birliği'nde hem de Amerika Birleşik Devletleri'nde biyometrik sistemlerin göç yönetiminde kullanılması ve ülkeler arasında bu alanda yapılan işbirliği, ülkelerin hem iç hem de dış politika gündemine alınmıştır.

Gelişmiş ülkeler, biyometrik sistemleri sadece sınır güvenliği için kullanmakla kalmayıp aynı zamanda biyometrik verinin uluslararası alanda değişimini de öngörmektedir (Redpath, 2005: 5). Göç, sınır güvenliği ve vize işlemlerinde biyometrik sistemlerin kullanılmaya başlaması ile biyometrik verilerin toplanması ve paylaşılması sonucu özellikle insan hakları savunucuları tarafından yapılan mahremiyetin ihlali tartışmaları yoğunluk kazanmıştır. Örneğin, Avrupa Birliği ile Amerika Birleşik Devletleri arasında yolcu bilgilerinin değişimini öngören 17 Mayıs 2004 tarihli Avrupa Konseyi kararı kamuoyunda yoğun tepki çekmiş ve Avrupa Parlamentosu'nun başvurusu üzerine Avrupa Adalet Divanı tarafından kararın yürütmesi durdurulmuştur. Konsey kararı Avrupa Adalet Divanı tarafından 30 Mayıs 2006 tarihinde iptal edilmiştir (Özcan ve Yılmaz, 2007: 108).

Gelişmiş ülkeler, biyometrik sistemleri ülkelerine giriş yapmak isteyen üçüncü ülke vatandaşlarının vize işlemlerinde kullanmakta oldukları gibi kendi vatandaşlarının seyahat belgelerinin düzenlenmesinde de kullanmaktadır. Bu durum bazı vatandaşlar tarafından mahremiyete müdahale olarak değerlendirilmektedir.

Özgürlük ve insan hakları savunucuları, göç yönetiminde biyometrik sistemlerin kullanılması ile devletin güvenlik sağlama hakkının kişilerin mahremiyet ve kişisel haklarını ihlal edebileceğini ve devlet hakkı ile kişisel hak arasında dengenin sağlanamayacağını iddia etmektedir (Redpath, 2005: 6).

Biyometri teknolojisinin birçok avantajlı ve dezavantajlı yanı olduğu gibi göç yönetiminde kullanılan biyometrik sistemlerin ilave bazı avantaj ve dezavantajları bulunmaktadır. Avantaj ve dezavantajı çok olan biyometrik sistemlerin kullanımında devletin güvenlik talebi ile kişilerin mahremiyetlerinin ihlali arasında bir denge sağlanmalıdır.

Biyometrik sistemlerin göç kontrol mekanizmasına katkı sağlayıp sağlamadığı tartışılan başka bir konudur. Hem Avrupa Birliği'nde hem de Amerika Birleşik Devletleri'nde göç yönetiminde kullanılan biyometrik sistemlerin yasadışı göçü önlediğine ilişkin somut bir veri bulunmamaktadır.

Diğer taraftan, biyometrik sistem kullanımının güvenlik sağlama ve göç yönetimine ciddi katkıları bulunmadığı ve yasadışı göçü önlemede önemli başarılar sağlamadığı da iddia edilmektedir. Avrupa Parlamentosu Liberal Demokrat Parlamenti aynı zamanda Adalet ve İnsan Hakları Sözcüsü olan Londra Milletvekili Sarah Ludford, Avrupa Birliği'nin biyometrik veri tabanı olan Avrupa Birliği Vize Bilgi Sistemi VIS veri tabanının kuruluş tartışmalarında, Avrupa Birliği'ne gelen göçmenlerin %99,99'unun yasal göçmenler olduğunu, kurulmakta olan biyometrik veri tabanının Avrupa Birliği'ne gelen göçmenlerin sadece %0,01'ini oluşturan yasadışı göçmenler ve suçlular için kurulduğunu belirtmiştir (Euractiv, 2007). Diğer taraftan yasadışı göçmenlerin çoğunlukla yasadışı yollarla ülkeye girdiği belirtilmektedir (McGowan, 2003: 1). Görülmektedir ki, göçmenlerin çok az bir kısmını oluşturan yasadışı göçmenlerden dolayı bu kişilerin daha az kullandıkları yasal sınır kapılarında bütün göçmenlere biyometrik sistem yükümlülüğü getirilmektedir.

I. TEZİN KONUSU VE PROBLEM

Bu çalışmada, göç politikaları, sınır güvenliği ile vize işlemlerinde ve sınır kontrollerinde biyometrik sistemler göz önünde bulundurularak uygulamalar ve tutulan kişisel verilerin güvenliğinin sağlanması değerlendirilmektedir. Ayrıca uluslararası sınır kontrol uygulamalarında biyometrik sistemlerin kullanımı ve göç kontrol sistemi olarak kullanılan biyometrik sistemlerin etkinliği ile göç yönetimine katkısı tartışılmaktadır. Avrupa Birliği ve Amerika Birleşik Devletleri göç politikaları ile Avrupa Birliği ve Amerika Birleşik Devletleri'nde uygulamaya konan biyometrik sistemler bu kapsamda tartışılmaktadır.

Bu tartışmalar yapılırken göç yönetiminde biyometrik sistemlerin kullanılması için Avrupa Birliği ile Amerika Birleşik Devletleri'nde yapılan düzenlemeler ve bu düzenlemeleri uygulamaya koymakla görevlendirilen kurumsal yapılar ve uygulamaların yapısı incelenmektedir. Uygulamalardaki sorunlar ile biyometrik sistemlerin göç yönetiminde kullanılmasının avantajları ve dezavantajları tespit edilmektedir.

Sosyal arařtırmalar genel olarak sosyal problemlere çözüm aramaktadır. Bazı durumlarda bir konunun detaylarının anlaşılması için yapılan çalışma herhangi bir sosyal probleme çözüm aramaktan daha önemli olabilmektedir (Ertem, 2007: 27–28).

Bu tezde, Avrupa Birlięi ve Amerika Birleşik Devletleri’nde uygulamaya konan biyometrik sistemlerin etkinlięi tartışılmaktadır. Etkinlik sorusuna cevap aranırken ilk olarak, göç yönetiminde biyometrik sistemlerin kullanımını gündeme getiren yasadışı göçle mücadele ve sınır kontrollerinin daha etkin yapılması açısından biyometrik sistemlerin katkısı değerlendirilmektedir. Etkinlik arařtırması için bir başka yöntem olarak, biyometrik sistemlerin kullanımının getirdięi avantaj ve dezavantajlar incelenmektedir. Teoride başarılı olarak gözüken biyometrik sistemler uygulamada ne tür avantajlar sağlamakta; dięer yandan biyometrik sistem kullanımının doęurduęu sorunlar ve sistemin dezavantajları avantajları ile kıyaslandığında nasıl bir durumun ortaya çıktığı tartışılmaktadır. İlk bakışta biyometrik sistemlerin avantajlarının dezavantajlarından daha fazla olduęu düşünölebilmektedir. İtiraf etmek gerekir ki bu çalışmaya başlarken yazarın kişisel kanaati de bu şekildeydi.

II. TEZİN AMACI VE ÖNEMİ

Bu konuları incelemek hem teorik hem de pratik boyutta katkılar sağlamaktadır. Teorik boyuttaki katkı hem Avrupa Birlięi hem de Amerika Birleşik Devletleri’ndeki yasal düzenlemeleri ve sorumlu aktörlerin görevlerini bilmemize ve anlamamıza yardımcı olma şeklindedir. Pratik boyutta ise hem Avrupa Birlięi hem de Amerika Birleşik Devletleri’ndeki uygulamaların nasıl olduęunu ve uygulamaların etkinlięi ile zayıf yanlarını daha iyi anlamamızı sağlama şeklindedir.

Bütün bu tartışmalar, 1 Haziran 2010 tarihinde Türkiye’de başlayan elektronik pasaport uygulamasına ve yapılacak düzenlemelere destek sağlaması, dięer ölkelerdeki durumu göz önüne koyması amacıyla ve genel olarak uygulanan sistemlerdeki açıklıkların tespiti göz önünde bulundurularak yapılmaktadır. Avrupa Birlięi aday ölkesi konumunda olan Türkiye’nin göç yönetiminde biyometrik sistemlerin kullanımına ilişkin yapılan düzenlemeleri olduęu gibi uygulamak isteyeceęi veya uygulamak zorunda kalacaęı yapılar da olacaktır. Çünkü Avrupa Birlięi, sınır kontrol sistemlerinin güçlendirmesine ilişkin 2019 yılına kadar devam

edecek yeni planlamalar yapmaktadır.² Örneğin, Bolu ilinde pilot bölge olarak uygulanan akıllı kimlik kartı projesi önümüzdeki süreçte Türkiye’de uygulanacak bir sistemdir. TÜBİTAK tarafından üretilen akıllı kimlik kartı üzerindeki bütünleşmiş devreye kişilere ait kimlik bilgileri kaydedilebilecektir.

Ayrıca, Türkiye bu sürece yeni girmiştir ve bu alanda yeterli akademik çalışma bulunmamaktadır. İlave olarak, bu çalışma akademik çalışmalara katkı sunabilecektir. Biyometrik sistemlerin göç kontrol mekanizmasında kullanılması bağlamında akademisyenlerin en çok tartıştığı konulardan birisi kişisel verilerin korunması konusudur. Kişisel verilerin yeterli düzeyde korunamadığı durumlarda kişilerin temel haklarından olan mahremiyete müdahale edilmiş olmaktadır. Bu çalışmada kısa da olsa birçok konuya değinilmekte ve böylece biyometrik sistemlerin göç kontrol mekanizmasında kullanımına ilişkin yapılacak sonraki çalışmalara referans olabilecek durumdadır.

Tezde cevap aranan temel soru göç kontrol mekanizması veya sınır kontrollerinde güvenliğin artırılmasında ilk akla gelen ve son yıllarda uygulanmakta olan biyometrik sistemlerin Avrupa Birliği ve Amerika Birleşik Devletleri uygulamaları ışığında başarısının ve güvenliği artırmaya etkisinin olup olmadığının tartışılıp incelenmesidir. Bu soruya cevap aranırken biyometrik sistemlerin dezavantajları ve özellikle kişisel verilerin korunması değerlendirme kapsamında bulundurulmaktadır.

III. MATERYAL ve METOD

Bu çalışmada dokümanlara dayalı araştırma metodu kullanılmıştır. Kaynak olarak birincil ve ikincil kaynaklar kullanılmıştır. Birincil kaynak olarak Avrupa Birliği ve Amerika Birleşik Devletleri düzenlemeleri ile Ekonomik Kalkınma ve İşbirliği Örgütü ve Uluslararası Sivil Havacılık Örgütü gibi uzman kuruluşların çeşitli raporları kullanılmıştır. Biyometrik sistemlerin standartlarını belirleyen Uluslararası Sivil Havacılık Örgütü’nün raporları öncelikli olarak referans verilen kaynaklardandır. Uluslararası Göç Örgütü’nün yayınladığı ve göç yönetiminde

² EU Press Release, (2011), “EUROSUR: ‘connecting the dots’ in border surveillance (Eurosur Sınır Kontrol Sistemi Kuruluyor)”, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1528>, (Erişim Tarihi: 1 Mart 2012).

biyometrik sistemlerin kullanımını inceleyen makaleler çalışmanın çerçevesini belirleyen önemli kaynaklardır. Türkiye’de iltica ve göç konularında yapılan tez çalışmaları bu çalışmanın bazı alt başlıklarına katkı sağlamak üzere kullanılmıştır. Olaylara ve tarihlere referans vermek üzere güvenilir internet kaynakları da kullanılmıştır.

IV. KAPSAM VE SINIRLILIKLAR

Biyometrik sistemler ve ülkelerdeki uygulamalar, nispeten yeni olduğundan dolayı konuya ilişkin yeterli Türkçe kaynak bulunmadığından genelde İngilizce kaynaklar kullanılmıştır. İngilizce kaynaklar, çoğunlukla internetteki akademik bilgi havuzlarından derlenmiştir. Başlar’ın (2005) da ifade ettiği gibi, internetin sunduğu akademik imkânlar yeterince değerlendirilirse, Türkiye’de yüksek lisans eğitimi yapan öğrenciler, İngiltere’de veya Amerika’da eğitim yapanlara eş değer akademik yayınlar üretebilme şansına sahiptir (Başlar, 2005: 42). Bu çalışmada, bahsedilen hassasiyet gösterilmeye çalışılmıştır.

Avrupa Birliğine aday ülke konumunda olan Türkiye’nin, Birliğin mevzuatına uyum çalışmaları önemli bir hükümet politikasıdır. Bu sebeple, bir göç kontrol mekanizması olarak biyometrik sistemlerin kullanımda Avrupa Birliği mevzuatı ve uygulaması detaylı olarak tartışılmaktadır. Türkiye haricindeki Avrupa Birliği üye ve aday ülkeleri çalışma kapsamına dâhil edilmemiştir. Avrupa Birliği’nin genel politikası, mevzuatı ve uygulaması çalışma çerçevesinde incelenmektedir. Diğer taraftan, Amerika Birleşik Devletleri biyometrik sistemlerin sınır kontrollerinde ve seyahat belgelerinde kullanılması konusunda bütün ülkelerin politika ve uygulamalarına dolaylı olarak yönlendirmede bulunmaktadır. Bir anlamda dünyada göçün güvenlikleştirilmesi politikasına yön veren Amerika Birleşik Devletleri göç politikası, hem Avrupa Birliği’ni hem de dolaylı olarak Türkiye mevzuatını etkilemektedir. Aynı zamanda, Amerika Birleşik Devletleri, biyometrik sistem uygulamalarına ve teknolojiye önderlik etmesinden dolayı, mevzuatı ve uygulaması detaylı olarak incelenmektedir.

IV. TEZİN BÖLÜMLERİ

Teze ilk olarak giriş bölümü ile başlanmaktadır. Giriş bölümünde, göç kontrol mekanizması olarak biyometrik sistemlerin kullanımının yaygınlaşması sebeplerinden gösterilen Amerika Birleşik Devletleri, İspanya ve İngiltere’de meydana gelen terör olayları ile konuya giriş yapılmaktadır. Daha sonradan biyometrik sistemlerin kullanımına ilişkin yaşanan tecrübeler ve yapılan tartışmalara değinilmektedir. Tezde cevap aranan sorular, tezin metodolojisi ve kaynaklar ve son olarak çalışmada var olan kısıtların tanıtımı yapılarak giriş bölümü bitirilmektedir.

Giriş bölümünden sonra birinci bölümde biyometrinin ve biyometrik sistemin ne olduğu, türleri, biyometrik sistemlerin işleyişi, başarısı, kullanım amaçları ve kullanım alanlarından bahsedilmektedir. Bu çalışma teknik bir çalışma olmaması itibariyle biyometrik sistemlerin teknik detayları anlatılmamakta, konunun anlaşılması için sadece gerekli minimum teknik detay dâhil edilmektedir.

İkinci bölümde göç olgusu, uluslararası göç, Avrupa Birliği’nin ve Amerika Birleşik Devletleri’nin göç politikaları ve en son Türkiye’nin göç politikası ile mevzuatı anlatılmaktadır. Avrupa Birliği ve Amerika Birleşik Devletleri göç politikaları çalışmanın konusuyla ilgisi kadar genel olarak ve kısaca açıklanmaktadır. Avrupa Birliği ve Amerika Birleşik Devletleri göç politikalarının detayı sadece göç politikaları konusunda yapılmış birçok detaylı çalışmaya bırakılmaktadır.

Üçüncü bölümde, biyometrinin göç kontrol mekanizmasında kullanılması tartışılmaktadır. Yasadışı göçle mücadele, sınır güvenliği, vize işlemlerinde ve sınır kontrollerinde biyometrik pasaport uygulamaları tartışılmaktadır. Göç kontrol sistemi olarak biyometrik sistemlerin Avrupa Birliği ve Amerika Birleşik Devletleri uygulamaları açıklanmaktadır. Avrupa Birliği ve Amerika Birleşik Devletleri uygulamalarının etkisi ile Türkiye’de son dönemde ortaya çıkan elektronik pasaport uygulaması ile bölüm bitirilmektedir.

Dördüncü bölümde, biyometrik sistemlerin avantaj ve dezavantajları ile kullanılan biyometrik sistemlerin kişilere ilişkin özel bilgileri kullanmaları sebebiyle ortaya çıkma ihtimali olan insan hakları ihlalleri, mahremiyete müdahale ve bu müdahalenin en aza indirilmesi için dikkat edilmesi gerekenler tartışılmaktadır. Özellikle bu tür bilgilerin kişisel bilgiler olduğu göz önünde bulundurularak kişisel bilgilerin korunması kapsamında uyulması gereken ilkeler sıralanmaktadır. Diğer

tarafından kolaylaştırma amaçlı olarak seyahat belgelerinde biyometri kullanımında ortaya çıkabilecek hatalar, iyi niyetli seyahat edenlerin özgürlüklerini kısıtlayabilecek etkiler doğurabilmektedir. Bu konuların da sistemlerin tasarlanmasında dikkat edilecek önemli konular olduğu vurgulanmaktadır. Biyometrik sistemlerin göç kontrol mekanizmasında kullanımının etkinliği incelenmektedir. Özellikle yasadışı göçmenlerin sayısının azaltılmasına ilişkin Amerika Birleşik Devletleri'nde uygulamanın başlarında olmakla birlikte somut bir katkı gösterilememektedir. Bu yüzden, biyometrik sistemlerin kullanımının kurallarını belirlemek için yapılması gerekenler bulunmaktadır. Yapılması gerekenler özelinde uluslararası alanda çerçeve kuralların oluşturulması gerekliliği tartışılmaktadır.

Sonuç bölümünde, biyometrik sistemlerin güvenlik veya kolaylaştırma amaçlı kullanımının arttığı, hatta biyometrik pasaportun kaçınılmaz hale geldiği kabul edilerek öneriler ile çalışma bitirilmektedir. Kişisel verilerin kullanılması ve mahremiyete müdahale ile ülke güvenliğinin sağlanması arasındaki dengenin özenle nasıl kurulabileceği önerilmektedir.

BİRİNCİ BÖLÜM

BIYOMETRİ

Kişilerin tanımlanması veya doğrulanması üç farklı yöntemle yapılmaktadır (Kumar, Sirinvasan ve Narendran, 2012: 18). Birincisi, kişinin kimlik kartı gibi sahip olduğu bir şey kullanılarak yapılmaktadır. Diğer, kişinin parola gibi bildiği bir şey ile ve sonuncusu ise biyometrik özellikler gibi sadece o kişide bulunan bir özellik ile kişiler birçok kişi arasından tanımlanmakta veya kişinin sistemde daha önceden kaydedilmiş biyometrik verisi ile karşılaştırılarak doğrulanmaktadır.

Biyometri, güvenlik ve doğrulama gibi amaçlarla kişileri biyolojik özellikleri aracılığıyla otomatik olarak tanımlamaktır (Drygajlo, 2009: 1). Kişilere ait tekil özelliklerin sistemdeki veriler ile kıyaslanması sonucu sistemin karşısında doğru kişi olduğunun teyit edilmesidir. Biyometride, her insanda farklılık gösteren, parmak izi, iris ve retina şekli, yüz yapısı, el geometrisi, el yazısı ve ses gibi farklı özellikler kullanılmaktadır.

Biyometri, kişinin fizyolojik veya davranışsal özellikleri ile tanınmasıdır (JRC, 2005: 31). Parmak izi, el geometrisi, iris, yüz yapısı, ses, kulak yapısı ve vücut kokusu gibi özellikler fizyolojik özelliklere, el yazısı ve yürüyüş gibi özellikler de davranışsal özelliklere örnektir (Thomas, 2005: 377).

Artan güvenlik ihtiyacı kapsamında birçok alanda biyometri kullanılmaya başlanmıştır (T-PD, 2005: 2). Dizüstü bilgisayarların başkaları tarafından kullanılmasını engellemekten bankamatiklerden para çekmeye kadar pek çok uygulama için biyometri standart güvenlik uygulaması olarak kabul edilmektedir.

Dünyanın birçok önde gelen bankası ATM kullanımı ve genel anlamda kart sahteciliği ile savaşmak için biyometriyi kullanmaktadır. Sahteciliğin boyutları göz önüne alındığında bankaların bu sorunla biyometri gibi bir teknolojiyi kullanarak baş etmesi uygun bir çözüm olarak ön plana çıkmaktadır.

Uçak bileti, otel odası, araç kiralama gibi çeşitli turizm hizmetlerinde ve giriş kontrol sistemlerinde kullanılabilecek biyometrik işlevleri olan bir akıllı kart tasarlanması önerisi biyometri endüstrisinde en çok tartışılan konulardan birisidir. Teknik olarak bu fikrin icra edilmesi mümkün olmasına rağmen, politik ve ticari açıdan bakıldığında, çözülmesi gereken birçok sorun ortaya çıkarmaktadır. Bu

kartlara kimlerin sahip olacağı sorusu bir yana, bu uygulamanın kimler tarafından ve nasıl yönetileceği de önem arz etmektedir. Uzmanlar, bu alanda kullanılacak biyometrik akıllı kartların bir pilot uygulamasının yapılarak kullanıcılara cazip gösterilmesini önermektedirler. Biyometrik sistemlerin ve akıllı kart teknolojisinin birleştirilmesi ile oluşan biyometrik tanımlama ve doğrulama sistemleri hem kullanıcıları hem de devletin güvenlik ihtiyacını karşılar durumdadır (Uzun, 2006: 52).

Biyometrinin etkin bir şekilde kullanılabileceği alanlardan birisi de internet işlemleridir. Biyometrik bir okuyucunun standart PC'lere bütünleşmiş edilerek cihaz maliyetinin düşürülmesi bu alanı diğerlerine göre daha cazip kılsa da, tartışılan bazı konulardan dolayı biyometrik sistemlerin internet işlemlerinde kullanılması henüz yaygınlaşmamıştır. Kredi kartlarına biyometrik sistemlerin bütünleşmesi sağlanarak müşteriye sunulması bu süreci kolaylaştıracak çözümlerden biri olmaktadır.

Sınır kontrol işlemlerinde de biyometri kullanılmaktadır (Frontex, 2007: 8). Biyometrik pasaport ve otomatik geçiş sistemleri gibi sınır kontrol işlemlerinde biyometrik sistemler kullanılmaktadır. Vize işlemlerinde de biyometrik sistemler kullanılmaktadır.

Telefonla satış yapan ya da çağrı merkezinde çalışan birçok kişi iş süreçlerinin en az bir bölümünde biyometri kullanımını düşünmüştür. Biyometri kullanımı özellikle otomatik geçişler için cazip bir alternatif olmaktadır. Yine de ses tanıma, biyometrinin problemlili alanlarından biri olarak gözükmektedir. Telefon cihazlarının, telefon hatlarının ve kullanıcı ortamlarının sabit olmayıp çeşitlilik göstermesi bu alanı zor kılan faktörlerden birisi olmaktadır.

Biyometrinin birçok alanda farklı amaçlarla kullanıldığı görülmektedir. Diğer yandan hangi biyometrik uygulama türünün hangi alanda kullanımının daha uygun olacağı henüz netlik kazanmamıştır (Ashbourn, 2004: 3).

Biyometrik sistemlerin (Redpath, 2007: 663), yüksek maliyeti ve ileri teknoloji olması itibariyle uygulamalarının kalifiye personel tarafından yürütülmesi gerekliliği biyometrinin birçok avantajına rağmen henüz tartışmasız kabul edilebilir bir teknoloji haline gelmesini engellemekte, bu sistemin başarı oranının yüzde yüzlere hala varamamış olması da bunu doğrulamaktadır.

Bu bölümde, biyometri tanımlanmaktadır. Biyometrinin kullanım aşamaları, fonksiyonları, türleri, başarı oranları ile kullanım alan ve amaçları anlatılıp, geleceğinden bahsedilerek bölüm bitirilmektedir.

1.1. TANIM

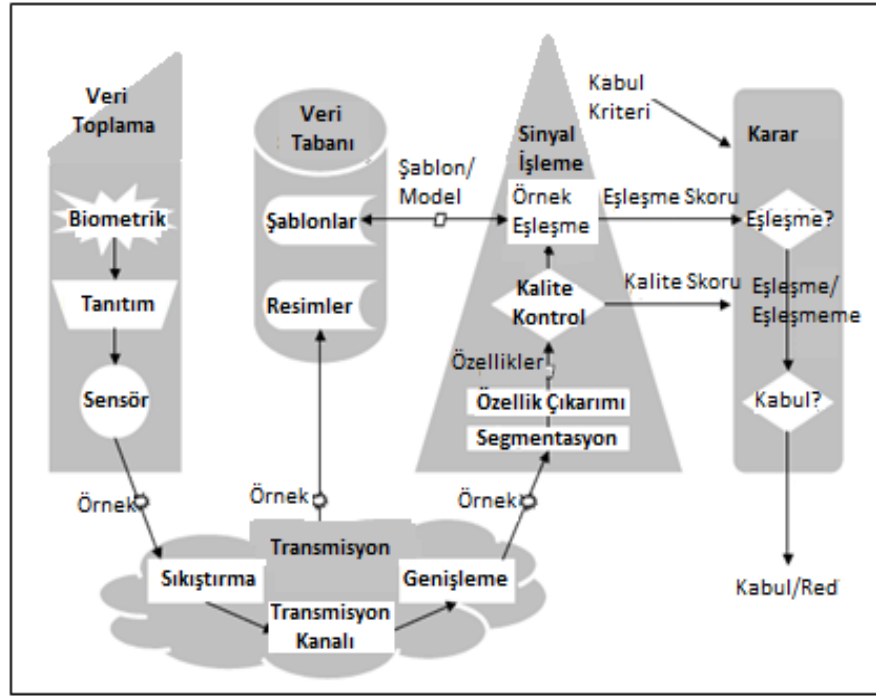
Biyometri, bir insanın otomatik olarak tekil ve özgün biyolojik özellikleri aracılığıyla tanınması ve doğrulanması demektir (ICAO, 2004: 8). Biyometrik sistem, biyometrik kayıt ve karşılaştırma aşamalarında baştan sona kadar kullanılan donanım, yazılım ve ağ cihazlarının hepsini içeren sisteme denmektedir (OECD, 2004: 11).

Biyometrik sistemler, bireyleri birbirinden ayıran ölçeklenebilir psikolojik ve/veya davranışsal karakteristiklerin kimlik tespitinde kullanıldığı bilgisayar kontrollü sistemler olarak da tanımlanmaktadır (Ashbourn, 2004: 1). Sade bir ifade olarak, biyometrik sistemler; anahtar ve parola gibi araçlar kullanmadan kişilerin kim olduğunun tanımlanması yöntemidir denebilmektedir.

Biyometrik sistemler, kişinin sadece kendisinin sahip olduğu ve kişiyi diğer kişilerden ayıran ve bilgisayar sistemine daha önceden kaydedilmiş fiziksel veya davranışsal özelliklerin kişiden tekrar alınan biyometrik özellikler ile matematiksel formüllerin kıyaslaması prensibine göre çalışmaktadır (Feldman, 2003: 653).

Bu teknolojiye parmak izi ve el geometrisinin incelenmesi, yüz özelliklerinin karşılaştırılması, ses ve konuşma analizi, iris ve retina taraması gibi alternatif biyometrik sistemler yer almaktadır.

Mansfield ve Wayman, “*Best Practices in Testing and Reporting Performance of Biometric Devices*” isimli raporlarında genel olarak bir biyometrik sistemde bulunabilecekleri grafik olarak resmetmişlerdir (Mansfield ve Wayman, 2002: 2).



Şekil 1: Genel Bir Biyometrik Sistemin Elemanları³

Şekil 1’den görüleceği üzere biyometrik sistemlerde birçok alt parça bulunmaktadır. Bunlar veri toplama, iletme, özellik çıkartılması ve veri tabanında saklanması ile sonuç karar aşamalarıdır. Şekil 1’de, aşamalar arasındaki ilişki ve işlem sırası da bulunmaktadır.

1.2. BİYOMETRİK TARAMA AŞAMALARI

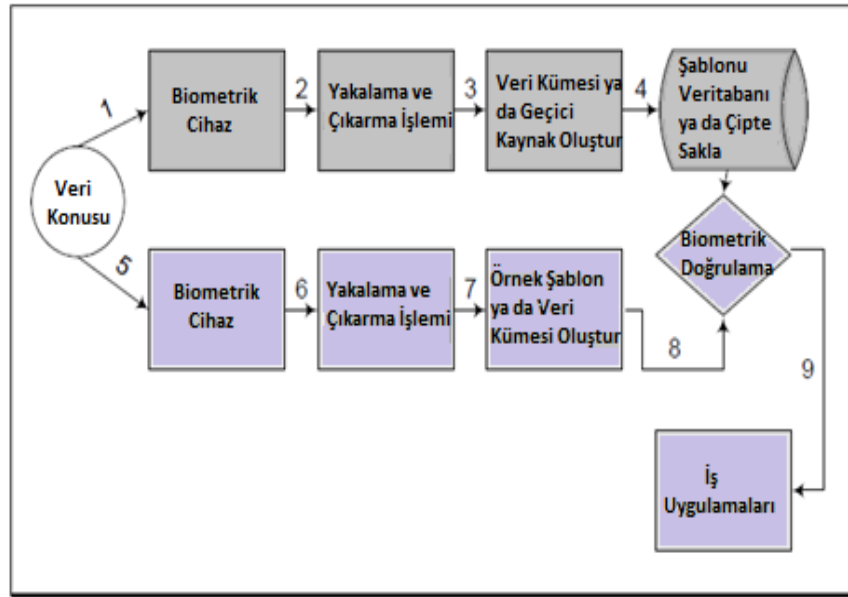
Biyometrik sistemlerin kullanımının üç aşaması bulunmaktadır. Bunlar: üyelik, kayıt ve karşılaştırmadır (Busch, 2006: 23). Biyometrik sistemlerin aşama sayısı dört diyenler de bulunmaktadır üyelik, kayıt, kaydetme, karşılaştırma (Kajevic, 2006: 16; JRC, 2005: 41). Bu çalışmada aşama sayısı üç olarak kabul edilmektedir. Biyometrik sistemlerin kullanıldığı göç kontrol mekanizmasında veri tabanı genelde her sistemde bulunmaktadır. Hatta biyometrik pasaport uygulamalarında kişisel verilerin daha iyi korunması için veri tabanının bulunmaması tercih edilmektedir.

Biyometrik sistemin türüne göre bir karakteristik özellik kaydedilir; ilk kayıt aşamasına üyelik denmektedir ve sistem bir daha kullanıldığında alınan bilgiler daha

³ Mansfield ve Wayman, 2002: 2.

önce kaydedilen örnekler ile karşılaştırılmaktadır. Karşılaştırmanın sonucuna göre, sonuç olumlu veya olumsuz olmaktadır. Üyelik aşaması, örnek olarak biyometrik verinin kaydedilip ve bu örnek veriden biyometrik özelliklerin çıkartılmasını kapsamaktadır (OECD, 2004: 16).

Biyometrik sistemlerin tarama aşamaları ve aralarındaki ilişki aşağıda şekil olarak gösterilmektedir:



Şekil 2: Biyometrik Sistem Tarama Aşamaları⁴

Şekilde 1, 2, 3 ve 4 sayıları ile gösterilen kutular üyelik ile kayıt aşamalarını ve 5, 6, 7, 8 ve 9 sayıları ile gösterilen kutular ise karşılaştırma aşamalarını temsil etmektedir, (OECD, 2004: 17).

Üyelik, yani sisteme kaydolma aşamasında bir biyometrik cihaz kullanılarak biyometrik örnek alınır (örneğin parmak izi tarayıcısı). Biyometrik sistem bu örnekten ayırt edici biyometrik özellikleri veya öznitelikleri çıkartmaktadır. Bu aşamadan sonra orijinal biyometrik örnek gizlilik kapsamında imha edilmekte veya güvenli bir şekilde saklanmaktadır. Çünkü bundan sonra artık orijinal biyometrik örnek değil biyometrik özellik veya öznitelik kullanılmaktadır. Biyometrik özellik

⁴ OECD, 2004: 17.

belirli bir formata çevrilerek merkezi bir veri tabanına veya kişide bulunan bir cihaza (akıllı kart gibi) kaydedilmektedir.

Karşılaştırma veya doğrulama aşamasında, bir biyometrik cihaz kullanılarak biyometrik örnek alınmaktadır. Biyometrik sistem bu biyometrik örnekten ayırt edici biyometrik özellikleri çıkartmaktadır. Biyometrik özellik belirli bir formata çevrilerek karşılaştırma motoruna gönderilmektedir. Karşılaştırma işlemi veri tabanında saklanan diğer biyometrik özellikler ile yapılmaktadır. Bu işlem sonucuna göre çıkan sonuç (doğru veya yanlış) biyometrinin kullanıldığı sisteme gönderilmektedir.

1.3. TANIMA VE DOĞRULAMA

Uluslararası Sivil Havacılık Örgütü (*International Civil Aviation Organization-ICAO*), biyometri için; “bir insanın otomatik olarak tekil ve özgün biyolojik özellikleri aracılığıyla tanınması ve doğrulanması demektir” diye bir tanım vermektedir (ICAO, 2004: 8). Yukarıdaki cümlede geçen tanıma ve doğrulama iki farklı işlemdir.

Biyometri terminolojisinde tanıma (*identify*), mevcut biyometrik verinin sistemde önceden kaydedilmiş veriler ile karşılaştırılmasıdır (ICAO, 2004: 8). Diğer bir deyimle bu işlem birden çoğa (*one-to-many*) kıyaslamadır. Tanıma bir anlamda teşhis etmedir. Örneğin, bir sınır kapısına gelen kişinin orada biyometrik bilgisinin canlı olarak alınıp sisteme daha önceden kaydedilen veriler ile karşılaştırılmasıdır. Yani, kişinin sistem tarafından tanınan ve önceden kaydedilmiş bir kişi olduğunun belirlenmesidir.

Biyometri terminolojisinde kullanılan diğer kavram olan doğrulama (*verify*) ise, bir insanın mevcut biyometrik özelliğinin kişinin sisteme önceden kaydedilmiş biyolojik özelliği ile karşılaştırılmasıdır (ICAO, 2004: 8). Diğer bir deyimle bu işlem bire bir (*one-to-one*) kıyaslamadır. Örneğin, seyahat belgesinde, vize belgesinde, pasaportta veya herhangi bir kimlik kartında önceden kaydedilmiş biyometrik veri var ise, ilgili belge elinde olan kişi, bu işlem esnasında canlı olarak biyometrik verisi alınıp elindeki belgedeki ile karşılaştırılarak kişi tanınmaktadır. Yani, kişinin, elindeki belgede veya sistemde kaydedilmiş olan kişi olduğunun doğrulanmasıdır.

Bire bir kıyaslama olan doğrulamada merkezi bir biyometri veri tabanının bulunması zorunluluğu yoktur, çünkü doğrulama işlemi kişinin elindeki bir cihazda kayıtlı olan biyometri örneği ile yapılabilmektedir (OECD, 2004: 16). Bire bir kıyaslama olan doğrulama birden çoğa kıyaslama olan tanıma göre daha kolay ve basit bir işlemdir. İhtiyaca ve şartlara göre doğrulama tercih edilmektedir. Fakat yüksek güvenlik beklentisi olduğu durumlarda genelde tanıma temelli biyometrik sistemler kullanılmaktadır.

Biyometrik sistemlerde tanıma ve doğrulama fonksiyonlu sistemlerin kullanımına çeşitli parametreler değerlendirilerek karar verilmektedir. Güvenlik beklentisi, doğruluk beklentisi, kişilerin haklarına yapılan müdahale ve sistemin kurulum maliyeti gibi faktörler tanıma veya doğrulama amaçlı biyometrik sistemlerin seçiminde göz önünde bulundurulacak faktörlerdir.

Aşağıda Tablo 1’de bazı biyometrik sistem türlerinin tanıma ve doğrulama fonksiyonları listelenmektedir. Tablo 1’den de görüleceği üzere biyometrik sistemler doğrulama için kullanılabildikleri gibi tanıma için de kullanılabilmektedir. Biyometrik sistemler tasarlanırken bütün bu parametreler göz önünde bulundurulmaktadır.

Biyometrik Sistemlerin Doğrulama Özellikleri

Biyometrik Tür	Doğrulama	Tanıma	Yanlış kabul	Yanlış ret	Kişiyeye Etkisi	Masrafı
Yüz	Evet	Hayır	Zor	Kolay	Çok düşük	Düşük
Parmak izi	Evet	Evet	Çok zor	Çok zor	Orta	Düşük
El geometrisi	Evet	Hayır	Çok zor	Orta	Düşük	Orta
İris	Evet	Evet	Çok zor	Çok zor	Orta	Yüksek
Retina	Evet	Evet	Çok zor	Çok zor	Yüksek	Yüksek
Ses	Bazen	Hayır	Orta	Kolay	Çok düşük	Düşük
İmza	Bazen	Hayır	Orta	Kolay	Düşük	Orta

Tablo 1: Biyometri Türlerinin Doğrulama Özelliklerinin Karşılaştırılması⁵

⁵ Pedreza, Juanita; Patricio, Miguel A.; Asis, Agustin De ve Jose, M. Molina, (2010), “Privacy and Legal Requirements for Developing Biometric Identification Software in Context-Based Applications”, *International Journal of Bio-Science and Bio-Technology*, Cilt 2, Sayı 1, Mart 2010.

1.4. BİYOMETRİK SİSTEM TÜRLERİ

Biyometrik tanımlama için yüz (*facial recognition*), parmak izi (*fingerprint recognition*), iris ve retina (*iris and retina recognition*), el ve parmak geometrisi tanıma (*hand geometry recognition*) gibi fiziksel karakteristik özellikler kullanabileceği gibi, ses (*voice recognition*) ve imza tanıma (*signature recognition*) gibi davranışsal özellikler de kullanabilmektedir (Das, 2006:3–4). Bu tür karakteristik özelliklerin kopyalanması çok zordur. Bu yüzden biyometrik sistemler günümüzde anahtar ve parolalardan daha güvenli sayılmaktadırlar.

Yukarıda bahsedilen kullanımı yaygın olan biyometrik sistemler gibi, kullanımı daha az olan biyometrik sistemler de vardır. Kulak geometrisi, vücut kokusu, klavye tuş dokunuşu, DNA⁶ veya yürüyüş tanıma gibi biyometrik tanıma sistemleri örnek olarak verilebilir (OECD, 2004: 34). Bu tür sistemlerin araştırmaları henüz devam etmektedir (JRC, 2005: 56).

Biyometrik sistemlerde çeşitli yöntemlerin her birinin avantaj ve dezavantajları olduğu görülmektedir. Yüz geometrisi yöntemi başarısız bulunurken, parmak izi ve iris taramasının başarılı ve hızlı olduğu ifade edilmektedir (Çiçekli, 2003: 178; Redpath, 2007: 28). Diğer taraftan, iris taraması sisteminin daha karmaşık olmasıyla birlikte maliyetinin parmak izi tanıma sistemi maliyetinden fazla olduğunu da belirtmek gerekir (Çiçekli, 2003: 178). Kasım 2003'te *New Scientist* dergisinde yayınlanan bir habere göre, iris taraması sisteminin başarısı %99 iken yüz tanıma sisteminin başarısı %60 civarındadır (Graham-Rowe, 2003). İris taraması sisteminin başarısı yüksek olmasına rağmen, bu oran az sayıda örnek içeren veri tabanlarındaki kıyaslamalarda faydalı olabilmektedir. Fakat 60 milyon kaydın bulunduğu bir veri tabanında, %99 başarıyla çalışan bir iris taraması sisteminde, bir kişinin iris taramasında 600.000 alternatif kayıt dönecektir ki bu da uygulanamaz bir durum demektir.

1.4.1. Parmak İzi Tanıma (*Fingerprint Recognition*)

Kişilerin parmaklarının kişilere özel olduğu ve parmak çizgilerinin her insanda farklı olduğu uzunca zamandır insanlar tarafından bilinmektedir. Parmak izi tanıma,

⁶ JRC, 2005: 53.

parmakta bulunan yay, kıvrım ve helezon gibi özelliklerden faydalanılarak gerçekleştirilmektedir (OECD, 2004: 21). Helezon şeklindeki hat çizgileri ve bu çizgilerin birbiriyle ilişkisi ile parmak izleri kıyaslanmakta ve eşleştirilmektedir (OECD, 2004: 21). Parmak izi tanıma, parmak izinin bir cihaz ile resminin çekilerek önceden örnek alınmış resim ile eşleştirilmesi ile yapılmaktadır. Sisteme önceden kaydedilen parmak izleri cihazın kendisinde bulunabileceği gibi merkezi bir veri tabanında da tutulabilmektedir.

Parmak izi tanıma sistemleri, personel takip sistemleri, banka işlemlerinde ATM cihazlarında, dizüstü bilgisayarlarda parola doğrulamasında, üyelik takip ve giriş çıkış kontrol sistemlerinde yaygın olarak kullanılmaktadır. Parmak izi tanıma, insanı en çabuk ayırt edebilmek ve bulmak için yaygın olarak kullanılan bir yöntemdir. Parmak izi tanıma sisteminin başarı oranı yüksektir, kullanımı kolaydır ve kurulum maliyeti düşüktür. Bütün bu sebeplerden dolayı kullanımı yaygındır (OECD, 2004: 22).

Aşağıdaki resimlerde bir parmak izi tanıma cihazı resmi ve parmak izi okuyucusu tarafından çekilmiş örnek bir parmak izi resmi ile parmak izinin kıyaslama yapılabilecek özellikleri bulunmaktadır.



Resim 1:Parmak İzi Tanıma Cihazı

Resim 1’de örnek bir parmak izi tanıma cihazının resmi bulunmaktadır. Parmak izi tanıma cihazının üzerine kişi daha önceden sisteme kaydetmiş olduğu parmağını koymakta ve tanıma işlemi yapılmaktadır. Tanıma işlem yapılırken kişinin parmağının resmi çekilmektedir. Resim 2’de öz nitelikleri nokta olarak belirlenen taranmış bir parmak izi resmi bulunmaktadır.



Resim 2:Parmak İzinin Özellikleri

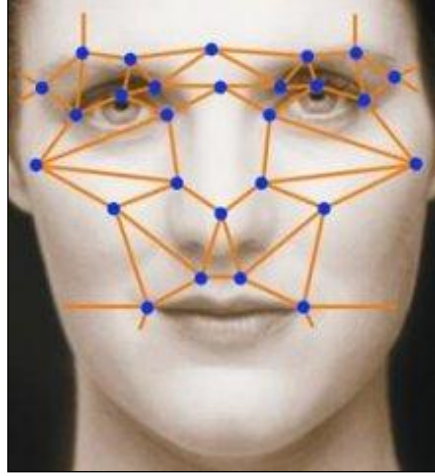
Parmak izi tanıma sistemleri belki onlarca yıldır kullanılmakla birlikte bilgisayarlı parmak izi otomatik tanıma sistemleri (*Automated Fingerprint Identification System-AFIS*) ile işlemler hızlandırılmıştır (Busch, 2006: 23; Liu, 2011: 36). Kullanımı kolay ve hızlı olduğu üstelik kurulum ve işletim maliyeti yüksek olmadığı için yaygın bir şekilde kullanılmaktadır. Otomatik parmak izi tanıma sistemleri Türkiye’de de kullanılmaktadır. Örneğin, Emniyet Genel Müdürlüğü’nde Otomatik parmak izi tanıma sistemi AFIS⁷ 1997 yılından beri kullanılmaktadır (Tetik, 2004: 45).

1.4.2. Yüz Tanıma (*Facial Recognition*)

Yüz tanıma, çekilen bir yüz resminin ayırt edici özelliklerinin çıkartılıp eşleştirmede kullanılması olarak tanımlanabilmektedir (Ashbourn, 2004: 2). İnsan yüzünün ayırt edici özelliklerinin bulunduğu yapısal bölgeler bulunmaktadır (Çelebi, 2008: 6). Yapısal örnek olarak, gözün birbirinden uzaklığı, burnun uzunluğu, göz çukurlarının derinliği ve elmacık kemiklerinin çıkıklığı sayılabilir. Yapısal bölgeler aranıp, aralarındaki ilişki tespit edilerek yüz bölgesi belirlenmektedir (Çelebi, 2008: 6). Yüz kıyaslamada birden fazla yöntem-algoritma (eigenface, özellik analizi, yapay sinir ağları, otomatik yüz tanımlama gibi) kullanılabilmektedir (OECD, 2004: 25). Yüz tanıma insanın biyometrik özelliklerine en az müdahale eden sistemlerden birisi olduğundan kişiler tarafından tercih edilmektedir. Yüz tanıma sistemleri; devlet

⁷ AFIS: Automated Fingerprint Identification System (Otomatik Parmak İzi Tanıma Sistemi).

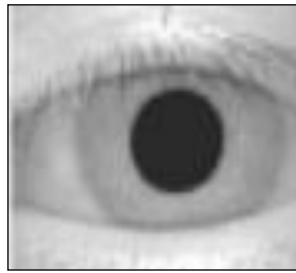
kurumlarında, bankalarda, seyahat acentelerinde ve birçok alanda kullanılmaktadır. Yüz tanıma-tarama sistemlerinin yüz resminde işlem yaptıkları düğüm noktalarına örnekler aşağıdaki şekilde verilmiştir.



Şekil 3: Yüz Tanımada Kullanılan Yüzün Yapısal Bölgeleri

1.4.3. İris ve Retina Tarama (*Iris and Retina Recognition*)

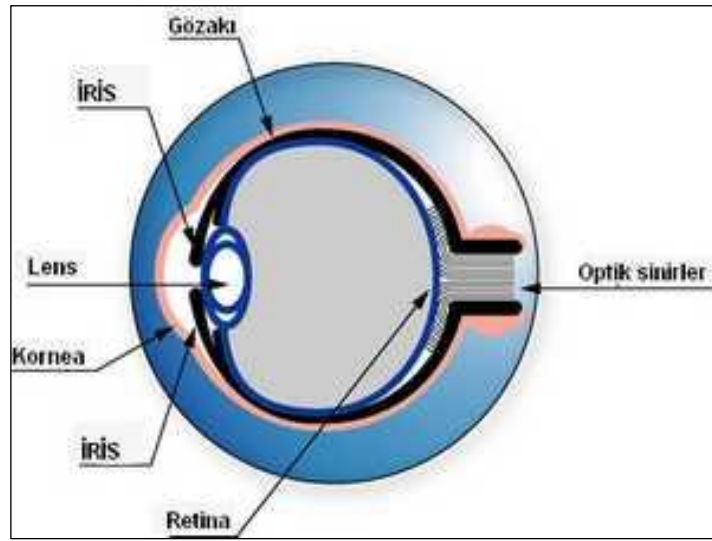
İris, gözün içinde mavi, kahverengi gibi renklerle çizilmiş yuvarlak bölümüdür. İris tarama, bir dijital kamera ile alınan iris resminin daha önceden alınan iris resmi kaydıyla tekil özellikler itibarıyla kıyaslama yapılmasıdır (Ashbourn, 2004: 2).



Resim 3:İris Resmi

Kamera, görünen ışığı ve infrared aralığına çok yakın ışığı alarak kişinin irisinin temiz ve yüksek çözünürlüklü bir resmini alır. İnfrared aralığa yakın ışıktaki kişinin gözbebeği çok siyahtır. Bu sayede kişinin gözbebeği ve irisi bilgisayar

tarafından kolaylıkla ayır edilebilir. Bir iris tarayıcıya bakıldığında sistem öncelikle gözün doğru pozisyon alıp almadığını test etmektedir. Göz kameraya genellikle 7.62 cm ile 25–40 cm uzaklıktadır. Daha sonra iris modelini analiz eder ve bunları bir koda çevirir. İris tarayıcıları yüksek güvenlik taraması gereken yerlerde oldukça popüler bir hale gelmiştir. Çünkü her insanın irisi birbirinden farklı eşsiz özellikler taşır. İki kişinin aynı iris koduna sahip olma olasılığı 10^{78} ' de 1'dir.



Resim 4:İrisin Yapısı

İris dışarıdan görülebilir ancak korumalı bir yapıya sahiptir. Özellikleri zamanla değişmediği için kimlik tanımlama için idealdir. Göz ameliyatı olan birçok kişide bile iriste herhangi bir değişiklik olmamaktadır. Güneş gözlüğü, iris tarama için problem oluşturmamaktadır. Tek yumurta ikizleri aynı DNA yapısına fakat farklı iris yapısına sahiptir. Göz irisi genetik oluşumlardan en az derecede etkilenir. Göz irisi kalıtsal hastalıklardan etkilenmez. Ömür boyu değişmeyen tek organdır. İnsanın doğumundan sonra 12. ayından itibaren ölümüne kadar değişmez. Göz, insanın yaşamını yitirmesinin ardından canlılığını en çabuk kaybeden organdır.



Resim 5: İris Taramalı Kapı Kontrolü Uygulaması

Resim 5’te iris tarama kontrolü uygulaması var olan bir giriş kontrol sistemi bulunmaktadır.



Resim 6: İris Tarama Ünitesi

Resim 6’da kapı giriş çıkış kontrol sistemi olarak kullanılan örnek bir iris tarama ünitesinin resmi vardır. Kullanıcılar iris tarama ünitelerinin 25-40 cm uzağında durarak sistemi kullanmaktadırlar.

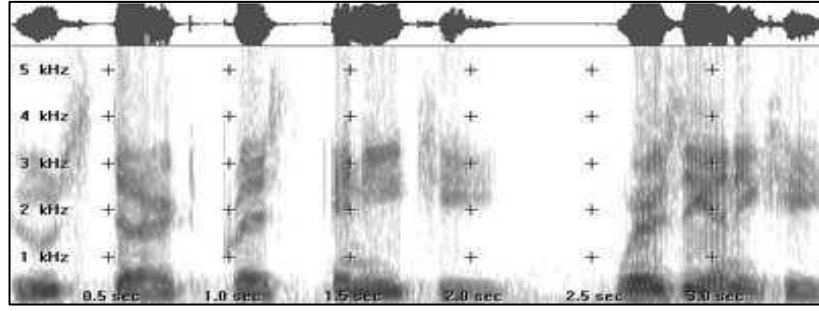
İris tarama sistemi, Türkiye’de birçok alanda uygulanmaya başlanmıştır. Bugün asansörlerde, çelik kapı, akıllı ev uygulamaları, ceza evleri, ziyaretçi ve personel takipleri, üniversite, otomotiv, kamu sektörü, bilgi işlem odaları girişleri, spor ve yaşam merkezleri alanlarında üye takip sistemi, hastanelerin tüp bebek

odaları gibi birçok alanlarda yapılan AR-GE çalışmalarında iris tarama kendini göstermiştir. Iris tarama sistemi daha çok yüksek güvenlik gerektiren durumlarda kullanılmaktadır (Akçay ve Çetinkaya, 2012: 4). Dünyada iris tarama sistemlerinde yazılım ve donanım olarak AR-GE, havaalanları ve pasaport uygulamaları üzerine kendini gösterirken, Türkiye’de bu uygulama yok denecek kadar az seviyededir.

Göz tanıma sistemleri denildiğinde genelde “Retina tarama ve Iris tarama” sistemleri, aynı sistemin iki farklı isimlendirilmesi gibi düşünülmektedir. Fakat bu iki teknoloji birbirinden tamamen farklı iki teknolojidir. Iris, göz bebeğinin etrafında yer alan göz rengini veren halkaya verilen isimdir. Retina tarama sistemleri, göz çeperinin arka yüzeyde bulunan kan damarlarının düşük yoğunluklu optik bir kaynak tarafından taranması sonucu biyometrik tanımlama bilgisinin elde edilmesi prensibiyle çalışmaktadır (JRC, 2005: 44). Retina tarama sistemlerinin potansiyel olarak göz sağlığına zararlı olduğuna dair yaygın inanış sebebiyle retina tarama sistemlerinin kullanımı çok yaygınlaşmamıştır (JRC, 2005: 44).

1.4.4. Ses Tanıma (*Voice Recognition*)

Ses tanıma veya ses doğrulama kişinin genel özelliklerinden olarak kabul edilen sesin karakteristik özelliklerinin önceden kaydedilen örnek ile karşılaştırılmasıdır (Ashbourn, 2004: 2).Herkesin sesi ağız yapısına göre farklılık göstermektedir. Ses karakteristiği kullanılarak yapılan biyometrik sistemlerde kullanıcılar sisteme belli bir sözcük veya kelime grubu söyleyerek kaydolmaktadır. Daha sonraki tanımlama işlemlerinde bu sözcük veya kelime grubu kullanılmaktadır. Ses karakteristiği belirlenirken ses spektrogramına bakılmaktadır. Farklı konuşma tonları grafikte farklı şekillerin oluşmasını sağlamaktadır. Resim 7’de örnek bir ses spektrogramı bulunmaktadır.



Resim 7: Ses Spektrogramı

Bu sistemde onaylama ve tanımlama işlemleri için iris tarayıcı, el geometrisi okuyucu gibi aletlere gerek yoktur. Tanımlama için cep telefonundan konuşma bile yeterli olabilmektedir. Ancak bu sistemlerin kötü niyetli kişiler tarafından diğer sistemlere nazaran daha kolay bir şekilde devreden çıkarılabilmek tehlikesi bulunmaktadır. Yetkili kişinin ses kaydı telefon vb. bir kaynaktan kaydedildiğinde sistem güvenilirliği azalmaktadır. Bunun önüne geçmek için ses tanıma sistemlerinde rastgele seçilen parolalar kullanılmaktadır. Parola oluşturmak için yetkili kişi tarafından bazı anahtar kelimeler önceden söylenip kaydedilmektedir. Parola olarak belirlenecek anahtar kelime rastgele olarak seçilip kullanılmaktadır.

1.4.5. El ve Parmak Geometrisi Tanıma (*Hand Geometry Recognition*)

Elin üç boyutlu olarak alınan görüntüsünün daha önceden kaydedilen örnek ile karşılaştırılmasıdır (Ashbourn, 2004: 2). Her insanın elleri ve parmakları farklıdır ve kendine has özellikler taşımaktadır. Ancak parmak izi veya iris kadar benzersiz bir yapıya sahip değildir. Bu yüzden parmak ve el geometrisi ile biyometrik tanımlama yöntemi kimlik tanımlamadan ziyade kimlik doğrulamak için kullanılmaktadır. Sistem el ve parmak geometrisini dijital bir kamera ve ışık kullanarak ölçmektedir. Basitçe el ölçüm yuvasına konulur ve parmaklar ölçüm yuvasına uygun şekilde hizalanmaktadır. Bundan sonra kamera bir veya birden fazla resim almaktadır. Resimler üç boyutlu olarak da çekilebilmektedir. Alınan bu bilgilerden ele ait uzunluk, kalınlık, eğrilik bilgileri tespit edilir ve bu bilgiler sayısal bilgiye çevrilmektedir. El ve parmak geometrisi, parmak izi veya iris gibi çok ayır edici bir özellik değildir. Bununla birlikte, insan elinde sakatlanma vb. şeylerden dolayı değişimler olabilir. El ve parmak geometrisindeki bu değişimler de tanıma

doğruluğunu azaltmaktadır. Bu yüzden, bilgilerin belirli periyotlarda güncellenmesi gerekmektedir.

Diğer taraftan daha az masraflı olması ve uygulaması kolay olduğundan çok yüksek doğruluk oranı beklenmeyen bina girişlerinde, havalimanlarında veya üniversitelerde kullanılmaktadır (OECD, 2004: 23). El ve parmak geometrisi tanıma, daha çok bire bir doğrulama uygulamalarında kullanılmaktadır. El ve parmak geometrisi tanıma sistemleri, pazarda en az paya sahip fakat en çok kullanılan biyometrik tanıma sistemleri arasındadır (Akçay ve Çetinkaya, 2012: 4).

Örneğin, Sosyal Güvenlik Kurumu SGK'ya bağlı hastaların muayenelerinde kimlik doğrulaması, el ve parmak geometrisi tanıma yöntemi ile 2012 yılının ikinci yarısından itibaren yapılacaktır (Çehreli, 2011). Bilindiği gibi Sosyal Güvenlik Kurumu bünyesindeki hastaların kimlik doğrulama yöntemi mevcut durumda T.C. kimlik numarası doğrulaması ile yapılmaktadır. Yeni uygulama ile hastaneye gitmeden fatura üretilmesi gibi suiistimallerin ortadan kaldırılması amaçlanmaktadır (Çehreli, 2011). Kamunun önemli ve büyük bir harcama kalemi olan sağlık harcamalarını, düzenlemek üzere kurulan bu sistem ile sağlık hizmetinden yararlanan bütün vatandaşların avuç içi taramaları yapılarak sağlık işlemleri yürütülecektir.

Hastanelerde Uygulanacak Olan Avuç İçi Tarama Sisteminin Kullanılışı



Resim 8: Avuç İçi Tarama Sistemi

Sosyal Güvenlik Kurumu'ndan yapılan açıklamaya göre, avuç içi tarama sisteminden yararlanacak 73,7 milyon vatandaş, ilk önce sisteme ilk kayıt işlemlerini yapacaklar ve kendi avuç içlerinin sisteme tanıtımını sağlayacaklardır (Gülten, 2011). Yeni sistemin ilk pilot uygulaması, Ankara'da bir özel hastanede yapılmıştır

(SGK, 2011). Sosyal Güvenlik Kurumu Başkanı, biyometrik doğrulama sisteminin 1 Temmuz 2012 tarihinden itibaren, özel hastanelerde uygulamaya başlayacağını ifade etmiştir (Posta, 2012).

Yeni uygulamanın getireceği bir başka yenilik de elektronik reçete sistemidir. Elektronik reçete uygulaması olan MEDULA sistemi ile doktorlar reçeteyi elektronik ortamda düzenleyecek ve eczaneler de elektronik ortamdaki reçeteye göre hastalara ilaçlarını vereceklerdir (Sağlık Aktüel, 2012).

İris ve parmak izinde olduğu gibi kişilerin damar yapıları da herkeste farklıdır. Birçok damar deri üzerinden görünür değildir, bu da kopyalanmasını oldukça zorlaştırır. Damar tanımlama sistemini kullanmak için bir parmak, bilek, el ayası veya elin tersi tarayıcı üzerine veya yakınına konmaktadır. Kamera infrarede yakın bir ışıqla dijital resim çekmektedir. Kandaki hemoglobinin ışığı emer ve damarlar siyah resimde görünür hale gelmektedir. Diğer biyometrik tanıma sistemlerinde olduğu gibi yazılım için önceden bir referans şablonu hazırlanmaktadır.

Aşağıdaki resimde damar geometrisi cihazlarına bir örnek verilmiştir:



Resim 9: Damar Geometrisi Tanıma Cihazı

Resim 9'daki damar geometrisi tanıma cihazına kişiler ellerini uzatmaktadırlar ve damar geometrisi cihazları tanımlama için Resim 10'daki gibi üç boyutlu bir resim çekmektedir.



Resim 10: Damar Geometrisi Tanıma Resmi

1.4.6. İmza Tanıma (*Signature Recognition*)

İmza tanıma, kişinin attığı imzanın özelliklerine göre kıyaslama yapılmasıdır (Ashbourn, 2004: 2). İmza, bir davranışsal özelliktir. İmza tanıma işlemlerinde, kişinin attığı imzanın şekli kadar, imza atış şekli, kalemi tuttuğu açı, yaptığı baskı, imza atış hızı ve kalemi havaya kaldırdığı sayı gibi diğer parametreler de değerlendirilmektedir.



Resim 11: İmza Tanıma Tableti Resmi

İmza, Resim 11'deki gibi özel olarak tasarlanmış bir platforma (tablete) ona uygun kalemle atılmaktadır. Platform, nihai olarak atılan imza ile birlikte yukarıda sayılan diğer parametreleri de kaydetmektedir.

İmza tanımada kişinin attığı imzanın özellikleri yani öznitelikleri çıkartılmaktadır. Öznitelik çıkartılması imza tanımının sonuç başarısına en çok etki eden aşamasıdır (Kaymaz, 2010: 2). İmza tanıma, orta düzey bir doğruluk sağlamaktadır. İmza tanıma, birden çoğa işlemlerde kullanılmaya uygun değildir (OECD, 2004: 33).

1.5. BİYOMETRİK SİSTEMLERİN BAŞARISI

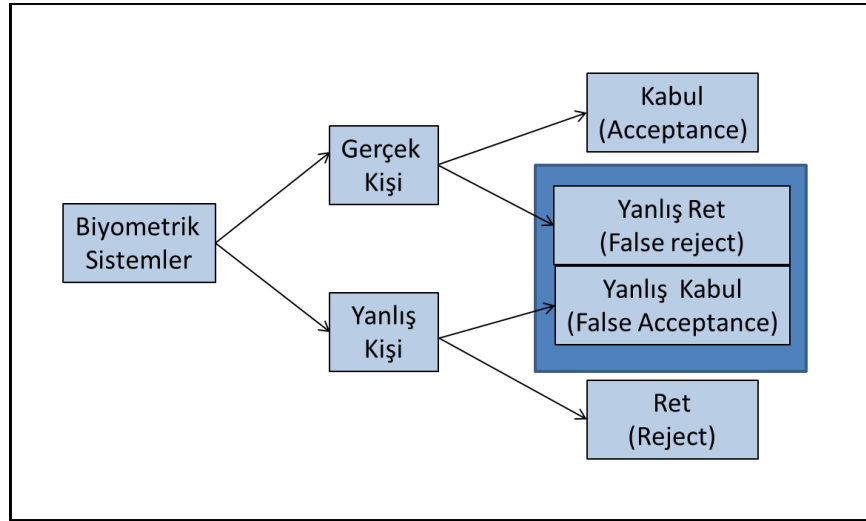
Hiçbir biyometrik sistem her zaman yüzde yüz başarılı değildir (Redpath, 2007: 33; JRC, 2005: 10). Başarı değeri biyometrik türlere göre değişmektedir. Başarı kıyaslaması yapılırken yanlış kabul (*false positive*), yanlış ret (*false negative*) gibi değerler göz önünde bulundurulmaktadır (Çelebi, 2008: 40).

Biyometrik sistemler, bir nesne ve o nesnenin daha önceden alınmış biyometrik verisinin matematiksel olarak kıyaslanması ve kıyaslama sonucu çıkan korelasyonun insanın seçimine sunulmasıdır (OECD, 2004: 10; Redpath, 2007: 33). Korelasyon için bir standart değer belirlenmesi (*threshold value*) ve bu değeri aşan sonuçların gösterilmesi işlemi, sürecin otomatikleştirilmesi demektir. Yani, önceden belirlenen standart değer üstündeki sonuçlar başarılı, standart değer altındaki sonuçlar ise başarısız kıyaslama olarak kabul edilmektedir. Korelasyon için kullanılan standart değer değişmekte; bu değer, kullanılan biyometri türü, donanım, yazılım, algoritma ve biyometrik sistemin yapılandırma ayarlarının istatistiksel fonksiyonu sonucu elde edilmektedir (OECD, 2004: 18).

Korelasyon değerinin otomatik olarak kıyaslanması sonucu, yanlış kabul (*false acceptance*) ve yanlış ret (*false reject*) gibi iki ayrı durum ortaya çıkabilmektedir (Redpath, 2007: 33). Yanlış kabul durumunda, biyometrik taraması yapılan kişinin biyometrik verisi, sistemde kayıtlı olan bir başka kişinin biyometrik verisi ile eşleştirilmektedir (Redapth, 2005: 15; OECD, 2004: 19). Bu durumda tanıma yapılan kişi doğrulanmakta ama yanlışlıkla bir başka kişi adına sistem tarafından kabul edilmektedir. Aslında doğrulanan kişinin sistemde kaydı bulunmamaktadır. Sistem yanlış kabul ile yanlış bir işlem yapmaktadır. Yanlış kabul ile yetkisiz kişiler sistemden giriş onayı alabilmektedir.

Diğer bir sonuç olan yanlış ret durumunda, sisteme kayıtlı bir kişi biyometrik verisi doğrulanmamış olarak kabul edilmektedir. Fakat biyometrik verisi doğrulanmayan kişiye ait, sistemde biyometrik kayıt bulunmaktadır. Sistem yanlış bir işlem yapmıştır. Yetkisi olan bir kişi sistem tarafından ret edilmektedir. Yanlış ret durumunda, sistem tarafından, biyometrik taraması yapılan kişinin sistemde biyometrik kaydı olmasına rağmen yok gibi değerlendirilerek kişi kabul edilmemektedir (Redapth, 2005: 15; OECD, 2004: 19). Yanlış kabul durumunda, kişiye ait biyometrik veri sistemde olmasına, kişi de doğru kişi olmasına rağmen, sistem doğru kişiye yanlış kişi muamelesi yapmaktadır.

Yanlış kabul ve yanlış ret sonuçlarının bütün ihtimalleri, Avrupa Birliği Komisyonu tarafından 2005 yılında yaptırılan bir çalışmada, Resim 12'deki gibi görselleştirilmiştir. Özetle, bir biyometrik sistemde kabul, ret, yanlış kabul ve yanlış ret gibi dört farklı sonuç çıkma durumu bulunmaktadır.



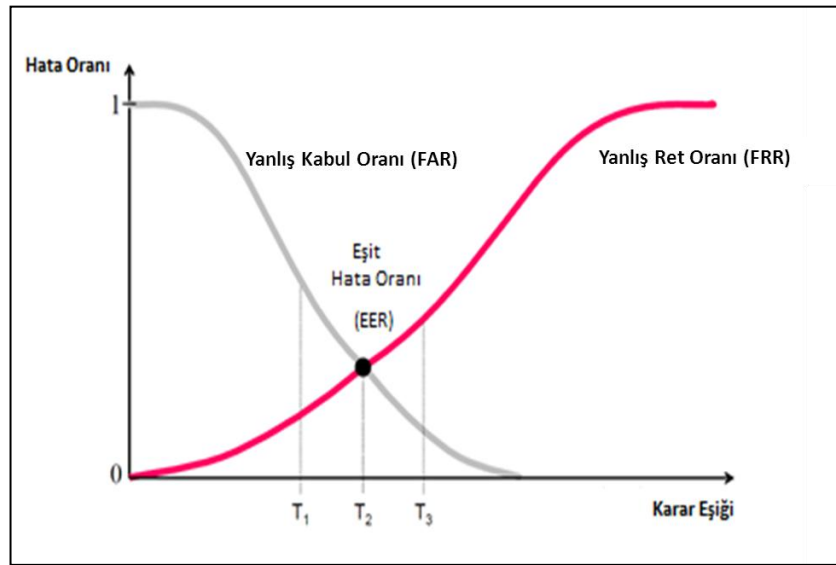
Resim 12: Genel Biyometrik Sistem İşlemleri⁸

Yanlış kabul oranı yüksek olan sistemler, güvenlik riski taşıdığı gibi yanlış ret oranı yüksek olan sistemler ise, yanlışlıkla doğru kişileri kabul etmeyerek kişilere haksızlık yapmaktadır. Göç yönetiminde kullanılan biyometrik sistemlerin çok düşük oranda yanlış kabul sonuçlar doğurması beklenmektedir. Böylece, doğru kişi

⁸ JRC, 2005: 34, Generic Biometric System Process.

olmamasına rağmen sistemin doğru kabul ettiği kişi/göçmen sayısının çok az olması durumuyla karşılaşılmaktadır.

Yanlış kabul ve yanlış ret oranları arasında ters orantı bulunmaktadır (Çelebi, 2008: 40). Yanlış kabul (*False Acceptance Rate-FAR*) ve yanlış ret (*False Reject Rate-FRR*) oranları arasında bir denge noktası olan karar eşiği bulunmaktadır. Sistem denge noktası bulunana kadar ayarlanmaktadır. Yanlış kabul ve yanlış ret oranları arasındaki ilişki ve denge noktası aşağıdaki şekilde gösterilmektedir.



Şekil 4: Biyometrik Sistem Hata Payı Denge Eğrisi⁹

Yanlış kabul, yanlış ret durumlarına ilaveten, biyometrik sistemler bazen biyometrik veriyi tarayıp sisteme yüklemekte hata yapabildiği gibi, bazen de üyelik aşamasında yani ilk kayıt aşamasında hata yapabilmektedirler. Karşılaştırma aşamasında ise resim kalitesi, ışık eksikliği gibi sebeplerle hatalar ortaya çıkabilmektedir. Biyometrik sistemlerde, yanlış kabul ve yanlış ret haricinde başka hata türleri de bulunmaktadır. Fakat karar verme açısından en önemli hata türleri, yanlış kabul ve yanlış ret sonuçlarıdır.

⁹ Dr. Andrzej Drygajlo, "Speech Processing and Biometrics Group, Biometrics Course 2009 Lecture Presentation, Lecture2 Part2", <http://scgwww.epfl.ch/courses> (Erişim Tarihi: 19 Aralık 2010).

1.6. BİYOMETRİK SİSTEMLERİN KULLANIM ALANLARI ve AMAÇLARI

Biyometrik sistemler: doğruluk, güvenlik ve kolaylaştırma amacıyla kullanılmaktadırlar (Redpath, 2005: 11). Güvenlik ve kolaylaştırma en önemli kullanım amaçlarıdır. Biyometrik sistemlerin doğruluk oranı henüz yüzde yüz olmaması sebebiyle¹⁰ kesin doğruluk beklenmeyen durumlarda kullanılmaktadır. Zaten her biyometrik türün farklı oranlarda doğruluğu bulunmaktadır. Biyometrik sistem seçimi yapılırken bütün bunlar göz önünde bulundurulacak parametrelerdir. Biyometrik sistem türlerinin çeşitli özelliklere göre kıyaslanması Tablo 2’de sunulmaktadır.

Biyometrik Sistem Özellikleri

Biyometrik Özellik	Yaygınlık	Eşsizlik	Kalıcılık	Toplanabilirlik	Performans	Kabul Edilebilirlik	Atlatma
Yüz	Yüksek	Düşük	Orta	Yüksek	Düşük	Yüksek	Düşük
Parmak İzi	Orta	Yüksek	Yüksek	Orta	Yüksek	Orta	Yüksek
El Geometrisi	Orta	Orta	Orta	Yüksek	Orta	Orta	Orta
İris	Yüksek	Yüksek	Yüksek	Orta	Yüksek	Düşük	Yüksek
Retina	Yüksek	Yüksek	Orta	Düşük	Yüksek	Düşük	Yüksek
İmza	Düşük	Düşük	Düşük	Yüksek	Düşük	Yüksek	Düşük
Ses	Orta	Düşük	Düşük	Orta	Düşük	Yüksek	Düşük
DNA	Yüksek	Yüksek	Yüksek	Düşük	Yüksek	Düşük	Düşük
Vücut Kokusu	Yüksek	Yüksek	Yüksek	Düşük	Düşük	Orta	Düşük

Tablo 2: Biyometri Türlerinin Genel Özelliklerinin Karşılaştırılması¹¹

Kullanılacak biyometrik sistem türü seçimi yapılırken Tablo 2’de görüleceği üzere birçok faktör göz önünde bulundurulmaktadır. Doğruluk oranı, kullanım yaygınlığı, kişiler tarafından sorunsuz olarak kabul edilmesi, biyometrik özelliklerin kişilerde farklı şekilde yani eşsiz düzeyde bulunması ve uzun süre boyunca

¹⁰ Redpath, 2007: 33.

¹¹ Kaymaz, 2010: 7.

biyometrik özelliğın kalıcı olması gibi birçok faktör kullanım alanına ve kullanım amacına göre değeriendirilmekte ve karar verilmektedir.

Biyometrik sistemler, geğış kontrol sistemlerinde (kısıtlı alanlara giriş kontrolünde), sınır güvenliğinde, bankacılık işlemlerinde, uluslararası sivil havacılıkta ve ülke güvenliğı gibi birçok alanda kullanılmaktadır. Biyometrik sistemlerin kullanım alanları her geğıen gün artmaktadır. Kullanım alanlarına örnekler bir liste olarak aşığıda sıralanmaktadır (Ashbourn, 2004: 3; Durmuş, 2010: 3):

- Geğış kontrol sistemleri ile kolay entegrasyon
- Akıllı binalarda göz iris ile çelik kapı uygulaması
- Asansör uygulamalarında iris okuyucu kamera
- Daha hızlı ve daha iyi sınır kontrolleri
- Havaalanlarındaki giriş ve çıkış işlemleri
- Sağlık alanında veri koruması
- Güvenlik işlemlerinde hassas verilerin korunması
- İnternet bankacılığında kullanıcı tanımlama
- ATM'lerde kullanıcı tanımlama
- Çağırı merkezlerinde kimlik tespiti
- Personel takibi
- Hastanelerde hasta takibi
- Sigorta şirketlerinde kimlik tespiti
- Masaüstü ve dizüstü bilgisayarların güvenliğı
- Kurumsal ağların güvenliğı
- Kiosklarda kullanıcı tanımlama
- Sigorta, vergi süreçleri gibi kamu hizmetleri
- Evlere, ofislere ve binalara erişim

- E-ticaret işlemleri
- Oy kullanma işlemleri

Biyometrik sistemler sınır güvenliği amacıyla, seyahat belgelerinde, sınır kapılarında veya göçmenlere ülke içinde hizmetleri ulaştırma gibi amaçlarla kullanılmaktadır. Örneğin, Hollanda ve İngiltere’de biyometrik sistemler sınır kontrollerinde kullanıldığı gibi göç yönetiminde, yani göçmenlere hizmet ulaştırmada da kullanılmaktadır (Redpath, 2007: 29).

1.7. BİYOMETRİ DEĞERLENDİRMESİ VE BİYOMETRİNİN GELECEĞİ

Biyometri uzunca zamandır bilinen ve geleneksel olarak tanımlamada kullanılan bir teknoloji (Kajevic, 2006: 25; T-PD, 2005: 2) olmasına rağmen; göç kontrol mekanizmasında yani pasaport veya seyahat belgelerinde ya da sınır kontrollerinde kullanımının yaygınlaşması 11 Eylül 2001 tarihinde Amerika Birleşik Devletleri’ne yapılan terör saldırılarından sonra olmuştur (Kajevic, 2006: 25).

Dr. Andrzej Drygajlo tarafından 2009 yılında yapılan sade bir tanıma göre biyometri: güvenlik ve doğrulama gibi amaçlarla kişileri biyolojik özellikleri aracılığıyla otomatik olarak tanımlamaktır (Drygajlo, 2009: 1).

Biyometrik sistemler: üyelik, kayıt ve karşılaştırma gibi aşamalarla çalışmaktadır. Biyometri terminolojisinde tanıma, yani birden çoğa kıyaslama ve doğrulama yani bire bir kıyaslama iki farklı işlemdir. Biyometrik sistemler, farklı türler olarak kullanıcıların karşısına çıkmaktadır. Bunlardan en yaygınları parmak izi tanıma, yüz ve iris taramadır (T-PD, 2005: 2; Ergen ve Çalışkan, 2011: 455). Kullanım alanına göre ihtiyaçlar, şartlar ve performans gibi parametreler değerlendirilerek herhangi bir biyometrik sistemin kullanılmasına karar verilmektedir. Örneğin, imza tanıma, orta düzey bir doğruluk sağlamaktadır. İmza tanıma, birden çoğa işlemlerde kullanılmaya uygun değildir (OECD, 2004: 33). Biyometrik sistemlerin başarısı yanlış kabul ve yanlış ret verilerine göre değerlendirilmektedir. Biyometrik sistemlerin başarısı yüzde yüz değildir (JRC, 2005: 10).

Biyometrik sistemlerin sorunlarından birisi, yüzde yüz başarılı çalışmamalarıdır. Üç boyutlu (3D) yüz tanıma sistemlerinin önümüzdeki dönemde

artması beklenmektedir (Busch, 2006: 24). Çünkü üç boyutlu yüz tanıma sistemlerinin doğruluğu daha fazladır, yüz özellikleri daha ayrıntılıdır ve yetkili kişilerin bilgilere ulaşması konusunda daha güvenlidir (Busch, 2006: 24).

Doğruluğun tam olmaması, üst düzey güvenlik gerektiren uygulamalarda önemli bir sorundur. Bu problem, biyometrik sistemlerde bir biyometrik türün olmasından kaynaklanmaktadır. Araştırmacılar bu problemi aşmak için tek biyometrik türü içeren biyometrik sistemler yerine, birden fazla biyometrik özellik içeren çoklu biyometrik sistemlerin (*multimodal biometric systems*) kullanılmasını önermektedirler (Yadav, Gothwal, Jitendra ve Singh, 2011: 57). Çoklu biyometrik sistemlerde birden fazla biyometrik özellik kullanılarak doğruluk ile ilgili problem aşılmaktadır. Önümüzdeki dönemde biyometrik sistemlerin yaygınlaşmasıyla birlikte artan güvenlik ihtiyacı çoklu biyometrik sistemlerin daha fazla kullanımını sağlayabilecektir.

Biyometrik sistemlerin önümüzdeki yıllarda yaygın olarak kullanılması beklenen bir başka alan ise, bankacılık ve finans işlemleridir. Ödeme ihtiyacını karşılamak üzere biyometrik sistemler kullanan farklı kredi kart uygulamaları finans sektöründe denenmektedir.

Örneğin, Hitachi şirketi bir banka ile birlikte el ve parmak geometrisi tanıma yöntemiyle alışverişte para ödeme sistemini tasarlamıştır (Kaya, 2009: 160). Bu sistem ile alışverişten sonra nakit olarak veya kart ile para ödemek yerine müşterilerin Resim 13'de gösterildiği gibi elini kasaya uzatması yeterli olacaktır. Sistem kişinin el ve parmaklarındaki kişiye özel damarları okuyarak kişiyi doğrulamaktadır. Bu yöntem kullanıcı için kullanımı kolay ve tercih edilebilir bir yöntem olmakla birlikte bu tür uygulamaların yaygınlaşması kullanıcı kabulü, sistemin uygulanabilirliği, sistemin maliyeti ve doğruluk oranı gibi faktörler değerlendirilerek karar verilebilecektir.



Resim 13: El ve Parmak Geometrisi Tanıma İle Ödeme Sistemi

Benzer şekilde Jacob Palmberg firması parmak izi tanıma sistemi ile geleceğin kredi kartı diye iddia edilen sistemi tasarlamıştır (Kaya, 2009: 160). Mobil olarak taşınabilen ve kablosuz bağlantı özelliğine sahip bu cihaz, hamilinin kart bilgisini üzerinde taşımakta ve kablosuz olarak ödeme yapabilmektedir. Resim 14’te gösterilen bu cihaz, aynı zamanda ödeme ve bakiye gibi bilgileri gösteren bir ekrana da sahiptir. Biyometrik özelliğe sahip bu cihaz kişinin birden fazla kart bilgisini de depolayabilecek durumdadır.



Resim 14: Parmak İzi Tanıma İle Mobil Ödeme Sistemi

Biyometri pazarındaki büyüme her geçen gün artmaktadır. Biyometrik ürünlerin toplam pazar büyüklükleri ve pazar tahminleri, Uluslararası Biyometrik Grup (*International Biometric Group*) isimli şirket tarafından sürekli yayınlanmaktadır. Uluslararası Biyometrik Grup'un verileri ve tahminleri, hem devlet kurumlarının raporlarında hem de akademik makalelerde kullanılmaktadır. Uluslararası Biyometrik Grup, biyometri pazarını 1999 yılında yaklaşık 250 milyon ABD Doları¹², 2001 yılında yaklaşık 500 milyon ABD Doları¹³, 2003 yılında yaklaşık 1000 milyon ABD Doları¹⁴, 2009 yılında yaklaşık 3400 milyon ABD Doları¹⁵ olarak belirtmektedir. Aynı şirket, biyometri sektörünün 2017 yılı Pazar büyüklüğünü yaklaşık 9,36 milyar ABD Doları olarak tahmin etmektedir.¹⁶

Çeşitli alanlarda artan güvenlik ihtiyacını karşılamada bir alternatif olan biyometri ve biyometrik sistemler kullanılmaktadır ve yakın gelecekte de artarak kullanılmaya devam edecektir. Bu durumun kişiler nezdinde doğal bir sonucu vardır: o da, insanlar önümüzdeki yıllarda her ortamda biyometrik ölçümlere ve kayıtlamalara hazır olmalıdırlar (T-PD, 2005: 7). Tabii bu durum kişisel verilerin çeşitli ortamlarda paylaşılması ve mahremiyete müdahale olarak da algılanabilir. Günümüzde daha çok kamu sektörü tarafından (pasaport veya kimlik kartları gibi) kullanılan biyometrik sistemler, hız ve güvenlik gibi gerekçelerle özel sektör tarafından da daha yaygın bir şekilde kullanılmaya başlanacaktır.

Kamu ve özel sektörün güvenlik ile ilgili artan talepleri biyometrik sistemlere ilerde olabilecek ilginin düzeyini belirleyecektir (Busch, 2006: 23). Fakat görünen odur ki, tanıma ve doğrulama gibi amaçlarla önümüzdeki yıllarda biyometrik sistemler daha yoğun kullanılacaktır.

1.8. BÖLÜM ÖZETİ

Genel olarak kişilerin tanımlanması veya kimlik doğrulanması üç yöntemle yapılmaktadır (Kumar, Sirinvasan ve Narendran, 2012: 18). Birinci yöntem, kişinin sahip olduğu bir şey ile (kimlik kartı gibi), bir diğer yöntem, kişinin bildiği bir şey ile

¹² Roberts, 2005: 5.

¹³ a.g.e.

¹⁴ a.g.e.

¹⁵ Broeders, 2011: 7.

¹⁶ a.g.e.

(şifre veya PIN) veya kişiye ait ve sadece o kişide bulunan bir özellik ile (biyometrik özellikleri) kişiler tanımlanmakta veya kişinin iddia ettiği şahıs olduğu doğrulanmaktadır. Biyometrik sistemler anahtar ve parolalardan daha güvenli sayılmaktadırlar. Biyometrik özellikler kişinin ayrılmaz bir parçasıdır ve kopyalanması çok zordur.

Biyometri, bireylerin tanımlanmasında veya doğrulanmasında kullanılan geleneksel bir yöntemdir. Örneğin parmak izi yıllardır kullanılmaktadır. Ancak, iki gelişme biyometri kullanımını artırmıştır. Birincisi, kamu ve özel sektörde bireyleri tespit etmek amacıyla artan bir eğilim vardır. İkincisi, dünya çapındaki terör tehdidi sonucu teröristlerin kimliklerini belirleme çabaları yoğunlaşmıştır. Kamu ve özel sektörde artan güvenlik ihtiyacı sonucu birçok alanda biyometrik sistemler kullanılmaktadır (T-PD, 2005: 2). Dizüstü bilgisayarlarda, bankamatiklerde, giriş çıkış sistemlerinde ve güvenlik ihtiyacı olan çeşitli alanlarda biyometrik sistemler kullanılmaktadır.

Biyometri, güvenlik ve doğrulama gibi amaçlarla kişileri biyolojik özellikleri aracılığıyla otomatik olarak tanımlamaktır. Biyometri, bir insanın otomatik olarak tekil ve özgün biyolojik özellikleri aracılığıyla tanınması ve doğrulanması demektir. Biyometri, insanın fizyolojik veya davranışsal özelliklerini tanımlamada sayısallaştırmayı ifade etmektedir (Thomas, 2005: 377).

Parmak izi, el geometrisi, iris, yüz yapısı, ses, kulak yapısı ve vücut kokusu gibi özellikler fizyolojik özelliklere; el yazısı ve yürüyüş gibi özellikler de davranışsal özelliklere örnektir (Thomas, 2005: 377). Biyometrik sistem, biyometrik kayıt ve karşılaştırma aşamalarında kullanılan donanım, yazılım ve ağ cihazlarının hepsine birden denmektedir.

Biyometri terminolojisinde tanıma, mevcut biyometrik verinin sistemde önceden kaydedilmiş veriler ile karşılaştırılmasıdır (ICAO, 2004: 8). Diğer bir deyimle, bu işlem birden çoğa kıyaslamadır. Tanıma bir anlamda teşhis etmedir.

Biyometri terminolojisinde doğrulama ise, bir insanın mevcut biyometrik özelliğinin kişinin sistemde önceden kaydedilmiş biyolojik özelliği ile karşılaştırılmasıdır (ICAO, 2004: 8). Diğer bir deyimle bu işlem bire bir kıyaslamadır. Doğrulama, tanımlamaya göre daha kolay bir işlemdir.

Biyometrik tanımlama için, yüz (*facial recognition*), parmak izi (*fingerprint recognition*), iris ve retina (*iris and retina recognition*), el ve parmak geometrisi tanıma (*hand geometry recognition*) gibi kullanımı yaygın olan fiziksel karakteristik özellikler kullanabileceği gibi, ses (*voice recognition*) ve imza tanıma (*signature recognition*) gibi davranışsal özellikler de kullanabilmektedir (Das, 2006:3–4). Kulak geometrisi, vücut kokusu, klavye tuş dokunuşu veya yürüyüş tanıma gibi biyometrik tanıma sistemleri yaygın olarak kullanılmayan sistemlerdir.

Hiçbir biyometrik sistem yüzde yüz başarılı değildir (Redpath, 2007: 33; JRC, 2005: 10). Biyometrik türlerin başarı sonuçları farklıdır. Başarı kıyaslaması yapılırken yanlış kabul (*false positive*) ve yanlış ret (*false negative*) gibi çeşitli sonuç değerleri kullanılmaktadır.

Hangi biyometrik türün hangi uygulamada kullanılacağına biyometrik sistemlerin doğruluk, yaygınlık, masraf ve kişiler tarafından kabul edilebilirlik ölçütlerine bakılarak karar verilmektedir. Bununla birlikte biyometri teknolojisinde sürekli çalışmalar yapılmakta ve yeni uygulamalar denenmektedir. Özellikle doğruluk problemi çoklu biyometrik sistemlerin kullanılmasıyla aşılabilecektir. Yapılan bütün çalışmalar sonucu kesin olarak varılan karar odur ki: çeşitli alanlarda hız, güvenlik ve doğruluk amaçlarıyla kullanılmakta olan biyometrik sistemlerin kullanımının önümüzdeki yıllarda artacağı birçok kişi tarafından öngörülmektedir.

İKİNCİ BÖLÜM

GÖÇ POLİTİKALARI

Dünya tarihinde insanların sürekli göç ettiği bilinmektedir. Son yıllarda, küresel bir fenomen olan sınır ötesi göç olgusu ile karşı karşıya bulunmaktayız. Yasadışı göç sayısı tam olarak bilinmemesine rağmen, sadece yasal uluslararası göç sayısı bile göçün ne kadar önemli bir konu olduğunu göstermeye yetmektedir. Günümüzde dünya nüfusunun yaklaşık %3'ü¹⁷ yasal uluslararası göç yapmaktadır (IOM, 2011). Bu farklı göç deneyiminin en dikkate değer görünümü özellikle İkinci Dünya Savaşı sonrası dönemde Batı Avrupa'ya yönelik gerçekleşen göç hareketleridir.

Avrupa Komisyonunun 2007-512 sayılı tebliği ile Avrupa Konseyine sunduğu “Göç ve Bütünleşme Konusunda Üçüncü Yıllık Rapor” göre, 2007 yılında Avrupa Birliği'nde yaşayan her 26 kişiden biri¹⁸ göçmendir. Raporla Avrupa Birliği'ndeki yasal göçmen sayısının 2007 yılında 18,5 milyon olduğu belirtilmiştir. Raporun önemli bir diğer tespiti de, Avrupa Birliği'nde 2007 yılı itibariyle göçmenlerin en çok Türkiye (2,3 milyon), Fas (1,7 milyon), Arnavutluk (0,8 milyon) ve Cezayir'den (0,6 milyon) gelmekte olduğudur (COM, 2007/512).

Diğer yandan, Avrupa Komisyonu'nun 2010-214 sayılı tebliği ile Avrupa Konseyine sunduğu “Göç ve İltica Konusunda Birinci Yıllık Rapor” göre 2008 yılında 27 Avrupa Birliği üyesi ülkede yasadışı göçmen statüsünde yakalanan üçüncü ülke vatandaşları toplam sayısı 609 bindir (COM, 2010/214: 11). Belirtilen sayı sadece yakalanan yasadışı göçmen sayısını göstermektedir.

Göç, insan hareketleri olarak tanımlanmaktadır (Ünsal, 2007: 29). Türk Dil Kurumu Türkçe Sözlük'te göç, “Ekonomik, toplumsal, siyasi sebeplerle bireylerin veya toplulukların bir ülkeden başka bir ülkeye, bir yerleşim yerinden başka bir yerleşim yerine gitme işi, taşınma, hicret, muhaceret” olarak tanımlanmaktadır.¹⁹

Kartal, sade bir anlatım ile göçü, insanların bireysel veya grup olarak “itici etkenlerden” uzaklaşıp, “çekici etkenlere” yöneldiği nüfus hareketidir diye tanımlamıştır (Kartal, 2008: 8).

¹⁷ 214 milyon/ 6,8 milyar – 28Ekim2010 tarihli ABD Seçim Bürosu Tahmini Değeri.

¹⁸ 18,5 milyon / 493 milyon = %3,8.

¹⁹ Türkçe Sözlük, Türk Dil Kurumu Yayınları, Ankara, 2005: 769.

En genel anlamıyla göç, şahıs veya toplulukların fiili ikametgâhlarını isteyerek ya da zorla, kalıcı veya belirli bir süreyi kapsayıcı şekilde gerçekleşen fiziki mekân değişikliğidir. Gönüllü göç, insanların kendi istekleri ve beklentileri yönünde bir kentten diğerine ya da bölgeye olan hareketliliğini ifade etmektedir. Zorunlu göç ise, bireylerin istekleri dışında çeşitli kuvvetlerin etkisi veya zorlamasıyla gerçekleşmektedir. Göç gerekçeleri olarak dini, iktisadi, siyasi, sosyal ve ekonomik sebepler sayılmaktadır.

Göç, yasal göç, yasadışı göç ve uluslararası göç gibi alt kırımlarıyla politika yapıcıların dikkatini çekmektedir. Yasal göç, gelişen sanayiye paralel olarak ortaya çıkan özellikle nitelikli işgücü ihtiyacı bağlamında başta Avrupa Birliği ülkeleri olmak üzere birçok ülkenin çözmeye çalıştığı bir konudur. Ekonominin ihtiyaç duyduğu miktarda işçi veya nitelikli işçi bulunamadığında aranan vasıflara sahip kişilerin yasal yollar kullanılarak diğer ülkelerden karşılanması yasal göçün sunduğu önemli bir katkıdır. Yasadışı göç, 11 Eylül 2001 terör olayı sonrasında daha yoğun bir şekilde gündeme gelen ve ulusal güvenliği tehdit etme riski olan bir başka önemli konudur. Yasadışı göç, teröristlerin veya ülke güvenliğini tehdit edebilecek kişilerin başvurduğu bir yöntemdir.

Bununla birlikte, uluslararası göçün bugün nasıl yönetilebileceği konusunda net bir karara varılabilmiş değildir. Gelecek nesiller ve göçmenler için göçün olumlu katkılarını en üst düzeye çıkarmak ve potansiyel olumsuz etkilerini en aza indirmek için neler yapılabileceği ülkelerin önemli bir gündem maddesidir.

Birçok ülke, dünyanın tüm bölgelerinde uluslararası göçün giderek artan öneminin ve küresel nüfus hareketliliğinin yakın gelecekte daha fazla artışta olacağının farkındadır. Uluslararası göç artık önemli bir politika konusudur. Bunun sonucu olarak devletler, göç konusunu iyi yönetmek için politikalar üretmekte ve belirli şekillerde işbirliği çalışmaları yapmaktadırlar.

Bu bölümde, Avrupa Birliği'nin ve Amerika Birleşik Devletleri'nin göç politikaları genel olarak incelenmektedir. Göç politikalarına, biyometrik sistemlerin kullanımına referans olacak şekilde özet olarak değinilmektedir. Sonrasında Avrupa Birliği ve Amerika Birleşik Devletleri göç politikaları değerlendirilmektedir. Değerlendirme sonrası Türkiye göç politikası tartışılarak bölüm bitirilmektedir.

2.1. AVRUPA BİRLİĞİ GÖÇ POLİTİKASI

Avrupa Birliği üyesi ülkeler, uluslararası göç dalgalarından etkilenmektedir. Avrupa Birliği, üye ülkelerin kendi ulusal politikaları ile birlikte, bütünleşmenin siyasi bir sonucu olarak ve Avrupa’da yaşanan göç olgusunun baskısı sonucu ortak bir göç politikası oluşturmak durumunda kalmıştır (Somuncu, 2006: 28). Yaşanan bu gelişmeler sonucu üye ülkeler, Avrupa Birliği düzeyinde ortak bir göç politikası geliştirme konusunda hemfikir olmuşlardır.

Göç, Avrupa Birliği’nde önemli bir politika konusudur. Avrupa ülkeleri, göçmenleri kendi ekonomilerine destek sağlayanlar olarak görmektedirler (Doğan, 2007: 128). Avrupa Birliği’nde göçün, 1999 yılından sonra genelde ekonomik sebeplerden dolayı yapıldığı kabul edilmektedir (Ertem, 2007: 47). Özellikle Avrupa’da nüfus artışında yaşanan düşüş ve iş gücü ihtiyacındaki artış, Avrupa Birliği üyesi ülkelerin nitelikli göçmenleri istihdam etme konusunu gündemlerine taşımıştır (Ertem, 2007: 41).

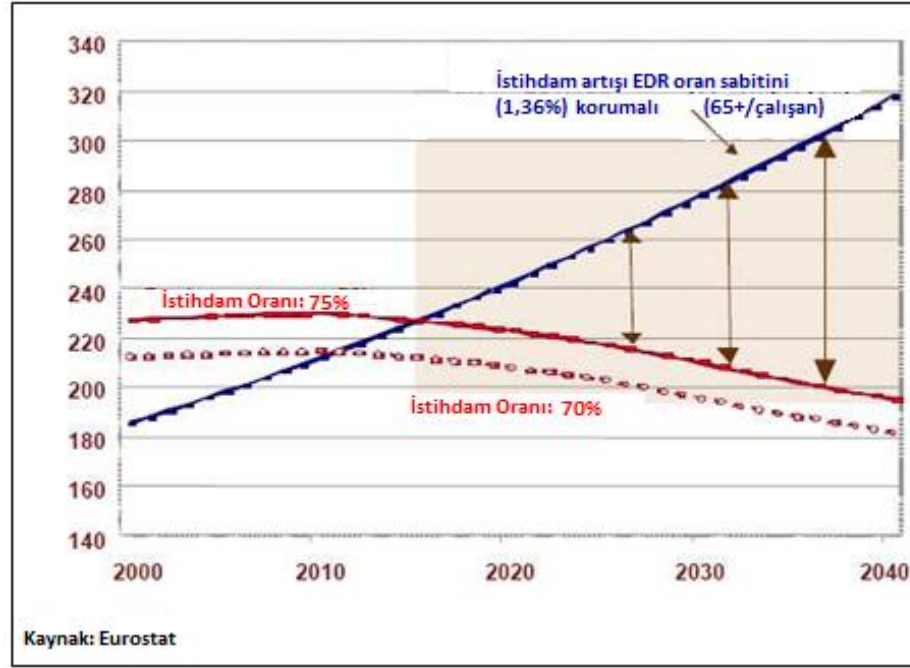
Eurostat²⁰ tahminlerine göre, 25 Avrupa Birliği Ülkesinde nüfusun %75’i çalışırsa 2015 yılından sonra nüfus artışı iş gücü ihtiyacını karşılayamaz olacaktır. Örneğin, 25 Avrupa Birliği Ülkesinde nüfusun %75’i çalışırsa 2020’de çalışan kişi sayısı ile toplam iş gücü ihtiyacı arasındaki fark 40 milyona yakın (200–240 milyon) olacaktır.

Avrupa Birliği eski Komisyon Başkan Yardımcısı Frattini 20 Haziran 2005 tarihinde yaptığı bir konuşmada iş gücü ihtiyacını karşılama konusunda Avrupa Birliği’nin Avustralya, Kanada ve Amerika Birleşik Devletleri’nden öğrenecekleri var diye ifade etmiştir.²¹

²⁰ Eurostat, <http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/>, (Erişim Tarihi: 04 Aralık 2011).

²¹ Franco Frattini, “The Green Paper on an EU approach to Managing Economic Migration”, Institute of European Affairs, Dublin, 20 Haziran 2005, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/05/364&format=HTML&aged=1&language=EN&guiLanguage=en>, (Erişim Tarihi : 04 Aralık 2011).

25 AB Ülkesinde Nüfus Artışı ve İş Gücü İhtiyacı Grafiği



Şekil 5: 2000–2040 Yılları Arasında 25 AB Ülkesinde Nüfus Artışı ve İş Gücü İhtiyacı Grafiği²²

Avrupa Kömür Çelik Teşkilatı'nı kuran Paris Antlaşması²³ ile Avrupa Ekonomik Topluluğu'nu kuran Roma Antlaşması²⁴ ortak bir göç politikası öngörmemektedir (Ertem, 2007: 144). Diğer taraftan, Roma Antlaşması'nda Avrupa Birliği üye ülkelerinin vatandaşlarının üye ülkelerde serbest bir şekilde seyahat edebilme hakkına sahip olduğuna ilişkin bir hüküm bulunmaktadır. Avrupa Birliği üye ülkelerin vatandaşlarına, 1957 tarihli Roma Antlaşması'yla verilen serbest seyahat edebilme hakkı, üye ülkelerin iç sınırların kaldırılmasına bir kapı aralamıştır.

²² Eurostat, <http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/>, (Erişim Tarihi: 04 Aralık 2011).

²³ Paris Antlaşması, 18 Nisan 1951'de imzalanan, 23 Temmuz 1952'de yürürlüğe giren ve 23 Temmuz 2002'de yürürlükten kalkan, http://eur-lex.europa.eu/en/treaties/dat/11951K/tif/TRAITES_1951_CECA_1_EN_0001.tif, (Erişim Tarihi: 04 Aralık 2011).

²⁴ Roma Antlaşması, 25 Mart 1957'de imzalanan, 1 Ocak 1958'de yürürlüğe giren, http://eur-lex.europa.eu/en/treaties/dat/11957E/tif/TRAITES_1957_CEE_1_EN_0001.tif, (Erişim Tarihi: 04 Aralık 2011).

2.1.1. AB Ortak Göç Politikası

İmza tarihi 1990 yılı olan Schengen Sözleşmesi, iç sınırların kaldırılmasını öngörmektedir (Ertem, 2007: 60). İmza tarihi Haziran 1985 ve yürürlük tarihi 26 Mart 1995 olan Schengen Antlaşması ile Schengen Bölgesine dâhil olan üye ülkelerde, Avrupa Birliği üye ülkelerinin vatandaşlarına ve herhangi bir üye ülkeye giren suçlulara dahi üye ülkelerde serbest bir şekilde seyahat edebilme imkânı verilmiştir (Ertem, 2007: 48).

Schengen Antlaşması, iç sınırların iptal edilmesi ile dış sınırlardaki vize ve sınır kontrol işlemlerinin ortak bir formata göre yapılmasını öngörmektedir. Schengen Antlaşması ile iltica ve göç Avrupa Birliği politika gündemine daha ciddi olarak gelmiştir. Bu antlaşma Avrupa Birliği göç politikasının dönüm noktası olmuştur. Schengen Antlaşması'nı İrlanda ve İngiltere imzalamamıştır. Norveç, İzlanda ve İsviçre Avrupa Birliği'ne üye olmamakla birlikte, Schengen Antlaşmasına dâhil olmuştur.

Yasadışı göç ile mücadele edebilmek için Avrupa Birliği ülkeleri 1990 yılında Dublin sözleşmesini imzalamışlardır. Bu kapsamda daha sonradan Londra Kararı imzalanmıştır. Londra Kararı'nın önemli noktası, yasadışı göçmenlerin güvenli üçüncü ülkeye gönderilmesidir. Fakat güvenli üçüncü ülkeler konusunda anlaşmazlık çıkmıştır. Aslında bütün bunlar ortak bir göç politikası olmayışından kaynaklanmaktadır.

Maastricht Antlaşması²⁵ ile iltica ve göç Avrupa Birliği'nde ortak çıkar olarak kabul edilmiştir (Ertem, 2007: 16). Maastricht Antlaşması ile 3. Sütun olan Adalet ve İçişlerinde İşbirliği'nin artırılması maksadıyla Avrupa Polis Ofisi (*Europol*) kurulmuştur.

Yürürlük tarihi 1999 yılı olan Amsterdam Antlaşması²⁶ Avrupa Birliği'nin iltica ve gümrük ortak politikasının belirlenmesinde önemli bir noktada bulunmaktadır. Avrupa Birliği üyesi ülkelerin ulusal göç politikalarının ortak bir göç politikasında uyumlulaştırılması ilk defa Amsterdam Antlaşması ile gündeme

²⁵ 7 Şubat 1992 tarihinde imzalanan ve 1 Kasım 1993'te yürürlüğe giren Maastricht Antlaşması, <http://eur-lex.europa.eu/en/treaties/dat/11992M/htm/11992M.html>, (Erişim Tarihi: 04 Aralık 2011).

²⁶ 2 Ekim 1997 tarihinde imzalanan ve 1 Mayıs 1999 tarihinde yürürlüğe giren Amsterdam Antlaşması, <http://eur-lex.europa.eu/en/treaties/dat/11997D/htm/11997D.html>, (Erişim Tarihi: 04 Aralık 2011).

gelmiştir. Antlaşma ile iltica ve göç konuları ulusal düzeyden birlik düzeyine yani birinci sütuna taşınmıştır (Ertem, 2007: 59). Amsterdam Antlaşması ile Avrupa Birliği göç, vize ve serbest dolaşım gibi konularda yasalar çıkarma imkânına kavuşmuştur. Avrupa Komisyonu, Avrupa Parlamentosu'na iltica ve göç konusunda yasal düzenleme önerileri yapabilmektedir (Aslan, 2010: 41).

Amsterdam Antlaşması'ndan hemen sonra Finlandiya'nın Tampere Şehrinde 1999 yılının Aralık ayında yapılan Avrupa Konseyi Zirvesi'nde iltica ve göç politikası programının ana detayları kabul edilmiştir (Ertem, 2007: 23). Zirvede, göç konusunda ortak bir Avrupa Birliği yaklaşımı belirlenmiş ve göç politikasının kuralları ve hedefleri belirlenmiştir. Zirvede konuşulan başka bir konu da, Avrupa Birliği düzeyinde ortak bir iltica politikası belirlenmesidir.

Özetle, Avrupa Birliği göç politikasının dört yönü vardır (Bozkurt, Özcan ve Köktaş, 2008: 339):

- Göç dalgalarının düzenlenmesi
- AB içinde yaşayanların entegrasyonu
- Ortak gelişme
- Yasadışı göçmenlerin geri kabulü

Avrupa Birliği Komisyonu, ortak bir göç politikası geliştirme konusunda çeşitli düzenleme teklifleri yapmıştır. Göç politikası geliştirmede temel ilke Avrupa Birliği'nin ekonomik ve demografik yapısı göz önünde bulundurularak göç akımlarını müşterek bir yaklaşımla daha iyi yönetmektir. Avrupa Birliği politikası, göç, iltica ve tek bir dış sınır kontrol stratejisi için ortak bir sistem geliştirmektir. Burada amaç, mültecilerin uzun süreli ikamet statüsü doğrultusunda, geri dönüş ve tekrar kabul politikalarını geliştirerek ortak bir iltica politikası oluşturmaktır.

Diğer yandan, 1990'larda Batı Avrupa'da, 2001'de Amerika Birleşik Devletleri'nde, 2004'de Madrid'de ve 2005'te Londra'da yaşanan terör olayları Avrupa Birliği göç politikasını daha sınırlayıcı hale getirmiştir (Aslan, 2010: 41).

2.1.2. AB Göç Politikasında Son Gelişmeler

Avrupa Birliği göç politikasının önemli kilometre taşları olarak aşağıdaki gelişmeler sayılabilir:

- Kasım 2004: AB Zirvesi, Adalet ve İçişleri alanında Lahey (*Hague*) Programını onaylamıştır.
- Aralık 2005: Komisyon, Lahey Programının yol haritasını içeren Yasal Göç Konusunda Politika Planını yayınlamıştır. Politika Planı 2009 yılına kadar uygulanması gereken bazı tedbirleri içermektedir.
- AB içinde çalışmak isteyen göçmenler için tek bir geri kabul prosedürünü içeren bir yönerge yayınlanmıştır.
- Eylül 2005: Komisyon, Yasadışı kalan üçüncü ülke vatandaşları için ortak kurallar ve işlemleri öngören bir yönerge teklif (Geri Dönüş Yönergesi) etmiştir.
- Kasım 2005: Göçe Yönelik Küresel Yaklaşım Stratejisi belirlenmiştir.
- Şubat 2008: Avrupa Komisyonu tarafından Yeni Sınır Paketi önerisi sunulmuştur.
- 5 Haziran 2008: AB Bakanlar Konseyi, Geri Dönüş Yönergesini kabul etmiştir.
- 18 Haziran 2008: Avrupa Parlamentosu Geri Dönüş Yönergesini onaylamıştır.
- 4 Mayıs 2010: Avrupa Birliği Konseyi Stockholm Programı'nı kabul etmiştir.
- 12 Aralık 2011: Avrupa Komisyonu Avrupa Birliği Sınır Gözetleme Sistemi *Eurosur*'un kurulmasına ilişkin bir öneri sunmuştur.

Avrupa Konseyi, 21. yüzyılın başında Avrupa Birliği'nin öncelikli alanlarından biri olan göçün, beraberinde getireceği fırsatlar ve zorlukların ele alınması gerektiğine inanmaktadır. Avrupa göç politikası 1999 yılında Tampere Zirvesi sonuçları, 2004 yılında kabul edilen ve 2005–2010 yılları arasını kapsayan Lahey Programı ile 2005 yılında kabul edilen Göçe Yönelik Küresel Yaklaşım

üzerine inşa edilmiştir. Avrupa Birliği’nde adalet, özgürlük ve güvenlik alanını güçlendirmek üzere belirlenen son program 2010–2014 yılları arasını kapsayan Stockholm Programı’dır. Stockholm Programı, sınır aşan suçla etkin mücadele edilerek yasal girişlerin kolaylaştırılması ile dış sınırlarının güçlendirilerek yasadışı göçle mücadele edilmesini amaçlamaktadır. Ayrıca, Avrupa göç politikası karşılıklı güvene, ortak sorumluluklara, insan haklarına, göçmenlerin temel özgürlüklerine ve 1951 tarihli Cenevre Sözleşmesi’ne dayanmaktadır.

Avrupa Birliği’nde ortak bir göç politikası belirleme çalışmaları uzunca bir süre yürütülmüştür. Bu çalışmalardan bir tanesi Yeni Sınır Paketidir (*New Border Package*). Avrupa Komisyonu tarafından 13 Şubat 2008 tarihinde yeni sınır paketi sunulmuştur.²⁷ Yeni sınır paketi ile dış sınırların güvenliğinin artırılması ve sınırlardaki sistemlerin güçlendirilmesiyle yasadışı göçmenlerin sayısının azaltılması planlanmaktadır (Guild, Carrera ve Geyer: 1). Yeni sınır paketi ile sınırlardaki izleme sistemlerinin güçlendirilmesi ve Avrupa Birliği Bütünleşmiş Sınır Yönetimi Birimi FRONTEX²⁸ bünyesinde operasyonel işbirliği hedeflenmektedir.²⁹

Avrupa Birliği’nde ortak bir göç politikası belirleme çalışmalarından bir başkası, Avrupa Birliği Sınır Kontrol Sistemi *Eurosur*’un kurulmasıdır. Avrupa Komisyonu 13 Şubat 2008 günü *Eurosur* Sınır Kontrol Sistemi’nin kurulmasına ilişkin bir çalışma önerisi sunmuştur.³⁰ Sunulan öneriye göre, Avrupa Birliği’ne giren yasadışı göçmenlerin sayısını ve Avrupa Birliği’ne girmeye çalışırken denizlerde ölen yasadışı göçmenlerin sayısını azaltarak iç güvenliğin artırılmasıdır (Frontex, 2011a: 4). *Eurosur*’un kurulması için, gerekli araçlar temin edilmesi önerilmiştir.

Gerekli planlama çalışmaları yapıldıktan sonra Avrupa Komisyonu 12 Aralık 2011 günü *Eurosur*’un kurulmasına ilişkin bir öneri sunmuştur.³¹ Avrupa

²⁷ EU, “Managing borders in a globalised world”, http://ec.europa.eu/news/justice/080213_1_en.htm, (Erişim Tarihi: 10 Aralık 2011).

²⁸ Avrupa Sınır Örgütü FRONTEX, AB üye devletlerin dış sınırlarının bütünleşmiş yönetimini ve sınırlardaki operasyonel işbirliğini yürütmektedir. Frontex, Lahey Programı kapsamında yürütülen uygulamalardan birisi olarak kurulmuştur.

²⁹ EU, “Border package: Facilitating travel and securing Europe’s borders”, http://ec.europa.eu/home-affairs/summary/docs/border_package_en.pdf, (Erişim Tarihi: 10 Aralık 2011).

³⁰ EU Press Release, (2008), “Examining the creation of a European Border Surveillance System (EUROSUR)”, <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/86&format=HTML&aged=0&language=EN>, (Erişim Tarihi: 01 Mart 2012).

³¹ EU Press Release, (2011), “EUROSUR: ‘connecting the dots’ in border surveillance (Eurosur Sınır Kontrol Sistemi Kuruluyor)”, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1528>, (Erişim Tarihi: 01 Mart 2012).

Komisyonu'nun *Eurosur*'un kurulmasına ilişkin 12 Aralık 2011 günü sunduğu tebliğin COM 2011/873³² 21. maddesi olan yürürlük maddesi *Eurosur*'un 1 Ekim 2013 tarihinde faaliyete başlamasını düzenlemektedir. *Eurosur* ile Avrupa Birliği üyesi devletler sınırlara ilişkin gözetleme verilerini Frontex ile paylaşmaktadırlar.

Avrupa Birliği Konseyi; adalet, özgürlük ve güvenlik alanını güçlendirmek ve 2010–2014 yılı plan ve programlarını ortaya koyan dönem önceliklerini belirlemek üzere Stockholm Programı'nı³³ kabul etmiştir. Stockholm Programı 04 Mayıs 2010 tarihli ve C 115 sayılı resmi gazetede yayımlanmıştır. Stockholm Programı Tampere ve Lahey programlarının başarıları üzerine inşa edilmiştir. Stockholm Programı, sınır aşan suçla etkin mücadele edilerek Avrupa Birliği üye devletlerin topraklarına yasal girişlerin kolaylaştırılmasını amaçlamaktadır (Köktaş ve Yılmaz, 2010: 16). Stockholm Programı'nın önceliklerinden birisi Avrupa Birliği'nin dış sınırlarının güçlendirilmesi ve yasadışı göçle mücadele edilmesidir. Avrupa Birliği Bütünleşmiş Sınır Yönetimi Birimi FRONTEX'in güçlendirilmesi de program kapsamındadır.

Göç yönetiminde güvenliğin artırılmasına ilişkin Avrupa Birliği'nin yeni politikası Avrupa Parlamentosu'nda 24 Kasım 2011 tarihinde yapılan bir toplantıda³⁴ uzmanlar tarafından tartışılmıştır. Avrupa Parlamentosu'nda yapılan toplantıda Stockholm programının ikinci yılında Avrupa Birliği'nin Kale Avrupa olma yolundaki ilerlemeleri konuşulmuştur.³⁵ Akıllı sınır kapılarının kurulması, yolcu bilgilerinin paylaşılması ve Avrupa Sınır Gözetleme Sistemi *Eurosur*'un kurulması Avrupa Birliği'nin gündemindedir. *Eurosur* sistemi ile *Frontex* sistemindeki açıklıklar ve eksikliklerin tamamlanması³⁶ öngörülmektedir.

Akıllı sınır kapıları ile Avrupa Birliği yasadışı göçle daha etkin mücadele etmeyi planlamaktadır. Akıllı sınır kapıları sistemi bünyesinde uçak ve uydu ile gözleme sistemleri ile insansız kara ve deniz araçları bulunmaktadır. Bu kapsamda

³² EU Press Release, (2011), "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Establishing the European Border Surveillance System (EUROSUR)", http://ec.europa.eu/home-affairs/doc_centre/borders/docs/eurosur%20final.pdf, (Erişim Tarihi: 01 Mart 2012).

³³ The Stockholm Programme, http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/jl0034_en.htm, (Erişim Tarihi: 01 Mart 2012).

³⁴ <http://www.edri.org/edrigram/number9.23>, (Erişim Tarihi: 01 Mart 2012).

³⁵ <http://ec.europa.eu/home-affairs/news/intro/docs/20111025/20111025-680en.pdf>, (Erişim Tarihi: 03 Mart 2012).

³⁶ <http://www.edri.org/edrigram/number9.23>, (Erişim Tarihi: 03 Mart 2012).

üye ülkeler arasında kapsamlı bir veri değişim altyapısının kurulması öngörülmektedir. Avrupa Parlamentosu büyük ölçekli bilişim sistemlerinin operasyonel yönetimi için 25 Ekim 2011 tarih ve 1077/2011 sayılı düzenlemesi ile operasyonel bir birimin³⁷ kurulmasını kabul etmiştir. Büyük ölçekli bilişim sistemlerinin operasyonel yönetimi için kurulacak bu birim 1 Aralık 2012 tarihinden itibaren fiilen çalışmaya başlayacaktır³⁸. Birimin temel görevi *EURODAC*, *VIS* ve *SIS II* sistemlerinin 24 saat esasına göre kesintisiz çalışmasını Avrupa Birliği düzeyinde temin etmektir³⁹. Birim, *SIS II* isimli Schengen bilgi sistemini ve *SIRENE* sistemini ise *SIS II* sisteminin faaliyete başlama tarihi olan 1 Mart 2013 tarihinden itibaren yürütecektir.⁴⁰

Diğer taraftan bazı üye ülkeler iç sınırların kaldırılması durumuna ilişkin endişeler taşımaktadırlar. Endişe taşıyan ülkelerin teşvikiyle ve yasadışı göçle daha iyi mücadele edebilmek için “Kale Avrupa” kurma çalışmaları başlatılmıştır (Ertem, 2007: 19). Aslında, Amsterdam Antlaşması’ndan itibaren bir özgürlük, güvenlik ve adalet alanı oluşturmaya çalışan Avrupa Birliği Kale Avrupa çalışmalarına taraftardır (Köktaş ve Yılmaz, 2010: 3). Kale Avrupa, iç sınırların kaldırıldığı Avrupa Birliği üye ülkelerinin göçmenlere karşı korunması gerektiği düşüncesidir (Kajevic, 2006: 33).

2.2. AMERİKA BİRLEŞİK DEVLETLERİ GÖÇ POLİTİKASI

Son üç yüzyıldan beri hem yasal hem de yasal olmayan göçün en rağbette olduğu ülkelerden birisi hiç şüphesiz Amerika Birleşik Devletleri’dir. Bütün ülkelerde, 1820-1930 yılları arasındaki göç hareketlerinin %61’ini Amerika Birleşik Devletleri’ne yapılan göçler oluşturmaktadır (Aslan, 2010: 44). Amerika Birleşik

³⁷ EU, “Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice”, <http://eur-lex.europa.eu /JOhtml.do? uri= OJ:L: 2011: 286: SOM:EN:HTML>, (Erişim Tarihi: 10 Ocak 2012).

³⁸ EUBusiness, “New EU Agency for managing large-scale IT systems in the area of freedom, security and justice”, <http://www.eubusiness.com/topics/research/it-agency-justice>, (Erişim Tarihi: 03 Mart 2012).

³⁹ EU 1077/2011, Madde 1.

⁴⁰ EUBusiness, “New EU Agency for managing large-scale IT systems in the area of freedom, security and justice”, <http://www.eubusiness.com/topics/research/it-agency-justice>, (Erişim Tarihi: 03 Mart 2012).

Devletleri'ne her yıl ortalama 1 milyon 100 bin kiři yasal göçmen (*legal permanent resident*) olarak kabul edilmektedir (DHS, 2010: 5).

Amerika Birleşik Devletleri göç politikası, 2001 yılına kadar yasadışı yollarla Amerika Birleşik Devletleri'ne gelen Meksikalı göçmenlerin ülkede çalışabilmeleri için yasal göçmen statüsüne kavuşturulması merkezindedir (Martin, 2004: 83; Aslan, 2010: 440). Amerika Birleşik Devletleri'ne göç etmiş ve ülkede yaşayan Meksika asıllı kiři sayısının 2000 yılında 9 milyon olduğu bilinmektedir (Aslan, 2010: 46).

Diğer taraftan, 2010 yılında Amerika Birleşik Devletleri'nde toplam 12 milyon yasal olmayan göçmen bulunduğu tahmin edilmektedir (Fano, 2010). Amerika Birleşik Devletleri'nde yaşadığı düşünülen yasadışı göçmen sayısı 2000'li yıllarda 5 milyon civarında iken 2007 yılına gelindiğinde bu sayı 12 milyonlara kadar çıkmıştır (Hanson, 2007: 3). Amerika Birleşik Devletleri'nde yaşayan yasadışı göçmenler en çok Meksika sınırından ülkeye girenler ve kısa süreli vize ile ülkeye gelip Amerika Birleşik Devletleri'nde kalmaya devam edenlerden oluşmaktadır (Hanson, 2007: 9).

Amerika Birleşik Devletleri göçle meydana gelen ve gelişen bir ülke olarak göç konusunu politika gündeminde her zaman tartışmıştır. Altın arama, refah temini veya özgürlük adına 18. yüzyılda yapılan göçler, göç sürecinin başlangıcını oluşturmaktadır. Amerika Birleşik Devletleri'ndeki yasal göçmenler, önceleri ekonomik gelişmenin motor gücü olarak değerlendirilmektedir (Hanson, 2007: 19).

Ronald Reagan'ın Başkanlık döneminde 1986 yılında yasalaşan Göç ve Reform Kontrol Yasası (*Immigration Reform and Control Act-IRCA*) sonucu 2,8 milyon yasadışı göçmen liberal ekonomik piyasa ihtiyaçları düşünülerek yasal göçmen statüsüne kavuşturulmuştur (Aslan, 2010: 44). Yaşanan bu olay, Amerikalıların göç politikasını oluşturmada, ekonomik parametreleri dikkate aldığını göstermektedir. Göç, bazı işçilerin maaşını düşürse de toplamda göç Amerika Birleşik Devletleri ekonomisine ekstra katkı olarak görülmektedir (Hanson, 2007:19).

Amerika Birleşik Devletleri'nde göç ile ilgili düzenlemeler de göç kadar eskidir. İlk düzenlemeler 1880'li yıllara kadar gitmektedir. Örneğin, 6 Mayıs 1882 tarihli Çin İhraç Yasası (*Chinese Exclusion Act of 1882*), 5 Şubat 1917 tarihli Göç Yasası (*Immigration Act of 1917*) ve 26 Mayıs 1924 tarihli Ulusal Köken Yasası

(*National Origins Act of 1924*), göçmenlere toplam sayı limiti yani kota koyan ve Avrupalı göçmenleri diğer bölgelerden gelen göçmenlere tercih eden düzenlemelerdir. Daha sonraları, 1952 yılında ve 1965 yılında Göç ve Vatandaşlık Yasası (*Immigration and Nationality Act*) şeklinde düzenlemeler yapılmıştır. 1965 düzenlemeleri ulusal kota sınırlamasını iptal etmiştir. İnsani amaçlarla mülteci kabulü 1 Nisan 1980 tarihli Mülteci Yasası (*The Refugee Act of 1980*) ile düzenlenmiştir.

Artan göçmen sayısı Amerikan Kongresinin, 1986 yılında Göçmenlik Reformu ve Kontrol Kanun'u (*The Immigration Reform and Control Act - IRCA*) kabul edip göçmen sayısını kontrol etme düzenlemesini yapması sonucunu doğurmuştur. Yasal göçle ilgili göçmen kabul sebeplerinin tesisi gibi eksiklikler 29 Kasım 1990 tarihli Göçmenlik Kanunu (*The Immigration Act of 1990*) ile düzenlemiştir. Yasadışı göçle mücadele amacıyla 30 Eylül 1996 tarihinde Yasa Dışı Göç Reformu ve Göçmen Sorumluluğu Kanunu (*Illegal Immigration Reform and Immigrant Responsibility Act of 1996 - IRIRA*) düzenlemesi kabul edilmiştir. 1990'lı yıllarda ekonomideki gelişmeler sonucu ihtiyaç olarak ortaya çıkan vasıflı göçmenlerin temini adına 17 Ekim 2000 tarihli 21. Yüzyılda Amerikan Rekabeti Kanunu (*The American Competitiveness in the Twenty-First Century Act*) yasalaşmıştır.

Amerika Birleşik Devletleri göç politikası 11 Eylül 2001 tarihine kadar ekonomik gelişim odaklı iken 11 Eylül 2001 terör olayından sonra ulusal güvenlik odaklı değerlendirmelere sahne olmaya başlamıştır. Politikadaki bu değişiklik düzenlemelere de yansımıştır.

On bir Eylül 2001 tarihli terör eylemlerine katılan şahısların göçmen olması ve ülkede yasal olarak kalış sürelerinin dolmuş olması (McGowan, 2003: 1) Amerika Birleşik Devletleri göç politikasının değişmesinde belirleyici bir faktör olmuştur. Amerika Birleşik Devletleri'nde yaşanan terör saldırılarından sonra Meksikalı göçmenlerin yasal göçmen statüsüne kavuşturulması tartışılmaz olmuştur (Aslan, 2010: 46). Belirtilen terör olayına katılan şahıslar, doğru bir göç kontrol sistemi ile takip edilip, süreleri dolunca sınır dışı edilmeleri sağlansaydı belki böyle bir olay yaşanmamış bile olabilirdi (Khanat, 2008: 68).

Amerika Birleşik Devletleri göç politikasındaki 2001 yılı sonrası yapılan değişiklik göçmen sayısını azaltmak suretiyle ülkeye muhtemel terörist girişlerini engellemek şeklinde özetlenebilmektedir (Aslan, 2010: 47). On bir Eylül 2001 terör eylemini yapanların göçmen olması Amerika Birleşik Devletleri ulusal güvenlik politikasının bu konuya yoğunlaşması sonucunu doğurmuştur.

Amerika Birleşik Devletleri göç politikası, 11 Eylül olaylarının hemen akabinde ulusal güvenliğin önemli bir gündem maddesi haline gelmiştir. Benzer terör saldırılarını bir daha yaşamamak için birçok güvenlik politikası gündeme alınmıştır (Stock, 2006: 124; Aslan, 2010: 48).

Değerlendirmeye alınan güvenlik politikalarından önemli bir tanesi göç ve ulusal güvenlik arasında doğrudan bir ilişki kurularak göç kontrol mekanizmasında güvenlik önlemlerinin artırılmasıdır. Örneğin; sınır kapılarında, seyahat belgelerinde ve vize işlemlerinde güvenlik artırıcı önlemler alınmaktadır.

On bir Eylül terör olaylarını incelemek üzere kurulan ulusal komisyonun Amerikan Kongre'sine 2004 yılında sunduğu raporda (*9/11National CommissionReportonTerroristAttacks2004*⁴¹) Amerika Birleşik Devletleri göç yönetimindeki ve sınır kontrollerindeki zayıflıklar yer almaktadır (Khanat, 2008: 48; Aslan, 2010: 44). Raporda, Amerikan Göç Yönetimi'ndeki eksikliklerin 11 Eylül saldırısına katılan teröristler tarafından istismar edildiği belirtilmektedir. Öyle ki, terör olayında uçak kaçırılanların hepsinin yabancı olduğu (Kajevic, 2006: 35) ve Amerika'ya yasal vizeleriyle girdikleri, yani Amerikan Sınır Kontrol Görevlilerinin incelemesinden geçtikleri anlaşılmaktadır (Stock, 2006: 119). Bahsedilen eksiklikler, Amerikan Göç Yönetimi'ne ilişkin zafiyetlere işaret etmektedir. Doğal olarak, göç kontrol yönetimindeki eksiklikleri telafi etmek üzere düzenleme yapma konusunda Amerikan kamuoyu yönetime baskı uygulamıştır (Aslan, 2010: 48).

Bush Yönetimi, 11 Eylül olayları sonucu kamuoyunda tartışılan konular ve göç politikasındaki değişikliklerle ilgili olarak ivedi düzenlemeler yapmıştır. On bir Eylül 2001 tarihli terör eylemleri ile birlikte Amerika Birleşik Devletleri'nde göç, sınır kontrolleri ve güvenlik artırma amacıyla birçok düzenlemede ve kurumsal

⁴¹ The National Commission on Terrorist Attacks upon the United States, (2004), (<http://www.9-11commission.gov/>, Erişim Tarihi: 25 Aralık 2010).

yapılanmada deęişiklik yapılmıştır. Yapılan düzenlemelerin en önemlisi Vatanseverlik Yasası'dır (*The USA Patriot Act*). Vatanseverlik Yasası, Ekim 2001 tarihinde Başkan Bush tarafından imzalanmıştır. Yasada birçok konuyla birlikte sınır güvenliğinin artırılması düzenlenmekte ve kolluk kuvvetlerinin terörist organizasyonları takip etmelerine ilişkin geliştirilmiş ek imkânlar sunulmaktadır (Rudolph, 2006: 79; Aslan, 2010: 48).

Bir başka önemli düzenleme, 14 Mayıs 2002 Tarihli Sınır Güvenliğinin Artırılması ve Vize Reform Yasası'dır (*The Enhanced Border Security and Visa Entry Reform Act of 2002*) (Aslan, 2010: 48). Yasada vize başvurularının daha detaylı incelenmesi, Amerika Birleşik Devletleri üniversitelerinin, yabancı öğrenciler konusunda daha dikkatli olmaları ve yabancı kişilerin ülkeye girişlerini daha kapsamlı şekilde inceleyebilmek için yeni ulusal güvenlik sisteminin devreye alınması öngörülmektedir (Aslan, 2010: 48; McCabe ve Meissner, 2010: 5).

Kurumsal yapılanmalar kapsamında yapılan önemli bir deęişiklik 2003 yılında faaliyete başlayan İç Güvenlik Örgütü'nün (*Department of Homeland Security-DHS*) kurulmasıdır (Özeren ve Cinoęlu, 2006: 185). On bir Eylül 2001 tarihli terör saldırısı hem Amerika Birleşik Devletleri hem de birçok ülke için alışık olunmayan bir eylem örneğidir. On bir Eylül saldırısı, Amerika Birleşik Devletleri'nin özellikle sınır kontrollerindeki ve göç yönetimindeki güvenlik algılamasının ve uygulamasının daha kapsamlı hale gelmesine sebep olmuştur. Aşağıda, Amerika Birleşik Devletleri'nde 11 Eylül 2001 tarihinden sonra göç ve ulusal güvenlik kapsamında yapılan düzenlemeler daha detaylı incelenmektedir.

2.2.1. Vatanseverlik Yasası (*USA Patriot Act, 2001*)

On bir Eylül 2001 saldırısından sonra Amerika Birleşik Devletleri'nde yapılan ilk ve en önemli düzenleme Vatanseverlik Yasası'dır (*The Patriot Act*) (Aslan, 2010: 48). Tamamı 342 sayfadan oluşan kısa adıyla Vatanseverlik Yasası⁴² diye bilinen yasanın amacı, istihbarat paylaşımının düzenli ve kolay bir şekilde yapılmasını sağlamaktır

⁴² ABD'nin 11 Eylül saldırıları sonrasında yürürlüğe koyduğu kısaltılmış adı "vatansever" manasına gelen açılımı "Terörizmin Durdurulması ve Engellenmesi İçin Gerekli Araçların Tahsisini Sağlayarak Amerika'yı Güçlendirmek ve Birleştirmek" yasası olan U.S.A P.A.T.R.I.O.T Act'in tam olarak adı "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" şeklindedir.

(Khanat, 2008: 60). Vatanseverlik Yasası, 11 Eylül terör olayının güvenlik kuvvetlerinin bilgi paylaşımındaki aksaklıkların sebep olduğu bilgi eksikliğinden kaynaklandığı düşünülerek hazırlanmış ve 2 Ekim 2001 tarihinde yürürlüğe girmiştir.

Vatanseverlik Yasası'nın dördüncü kısmında, Amerika Birleşik Devletleri sınır kontrol yönetiminde yapılacak değişiklikler düzenlenmektedir (Khanat, 2008: 63). Vatanseverlik Yasası ile düzenlenen bir konu, Amerika Birleşik Devletleri'ne seyahat etmek isteyen insanların, diğer ülkelerdeki Amerika Birleşik Devletleri konsolosluklarında parmak izlerini sisteme kaydettirmeleridir (Khanat, 2008: 63).

Amerika Birleşik Devletleri'nde 2001 yılında yasalaşan Vatanseverlik Yasası, bütün yabancı turistlerin makine tarafından otomatik okunabilen biyometrik seyahat belgesi taşımasını ve ülkeye giriş çıkışların kaydedilebileceği bir giriş-çıkış (*entry-exit*) sisteminin yürürlüğe konmasını zorunlu kılmıştır (Thomas, 2005: 378).

2.2.2. Sınır Güvenliğinin Artırılması ve Vize Reform Yasası (*The Enhanced Border Security and Visa Entry Reform Act of 2002*)

Sınır Güvenliğinin Artırılması ve Vize Reform Yasası (*The Enhanced Border Security and Visa Entry Reform Act of 2002*)⁴³ Amerika Birleşik Devletleri'ne giren yabancıların, ülkeye girişleri esnasında sınır görevlilerine daha detaylı inceleme imkânı sunan bir düzenlemedir (Meissner ve Kerwin, 2009: 20). Yasanın amacı, 11 Eylül olaylarından sonra gündeme gelen sınır kontrol işlemlerindeki eksikliği tamamlamaktır.

Sınırlardaki kontrol işlemlerini artırmak maksadıyla, yasa sonucu Amerika Birleşik Devletleri Ziyaretçi ve Göçmen Statüsünü Gösterge Teknolojisi Programı (*The United States Visitor and Immigrant Status Indicator Technology Program-US VISIT*) çalışmaları başlamıştır. Kısa adı US VISIT olan bu program ile Amerika Birleşik Devletleri hava ve deniz limanlarına 01 Ocak 2004 tarihinden itibaren vizeyle giren yabancıların parmak izleri alınmakta, seyahat belgeleri elektronik cihazlarla taranmakta ve kimlikleri terörist izleme listesindeki isimlerle karşılaştırılmaktadır¹³. US VISIT programı ile ülkeye girip çıkanların takip edilmesi

⁴³ Enhanced Border Security and Visa Entry Reform Act of 2002, http://travel.state.gov/visa/laws/telegrams/telegrams_1403.html, (Erişim Tarihi: 10 Aralık 2011).

amaçlanmaktadır. Böylece yabancıların vize süresini aşması ya da vize amaçlarının dışında işler yapmaları engellenmiş olmaktadır.

US VISIT programı, ulusal güvenlik kapsamında sınır güvenliğini artırmak üzere Amerika Birleşik Devletleri hükümeti tarafından gerçekleştirilen icraatların en başarılısı olarak ifade edilmektedir (Meissner ve Kerwin, 2009: 20).

2.2.3. İç Güvenlik Örgütü Yasası (*Homeland Security Act, 2002*)

Kurumlar arasındaki bilgi paylaşımını koordine etmek üzere kurulan İç Güvenlik Örgütü, 11 Eylül 2001 saldırısından sonra Amerika Birleşik Devletleri'nde yapılan önemli kurumsal düzenlemelerden birisidir (Özeren ve Cinoğlu, 2006: 185). İç Güvenlik Örgütü Yasası 2002 yılında yürürlüğe girmiş olmakla birlikte kurumun faaliyete başlaması 2003 yılıdır. İç Güvenlik Örgütü, Amerika Birleşik Devletleri'ndeki 22 kurumun bir araya gelmesiyle oluşmuş ve 200 bine yakın personeliyle Amerika Birleşik Devletleri'nin en büyük federal kurumlarından birisi olmuştur (Özeren ve Cinoğlu, 2006: 185).

İç Güvenlik Örgütü'nün görevlerinden bir tanesi seyahat ve taşımacılık alanlarındaki sınır güvenliğinin sağlanmasıdır (Aslan, 2008: 72). İç Güvenlik Örgütü'ne bağlı Taşımacılık Güvenliği Örgütü (*Transportation Security Administration-TSA*) sınır güvenliği kapsamında “Güvenli Uçuş Programı”⁴⁴ (*Secure Flight Program*) isimli bir proje yürütmektedir (Cinoğlu ve Özeren: 186). Güvenli Uçuş Programı sebebiyle Amerika Birleşik Devletleri'ne seyahat eden yabancıların sınır kapılarında yüz resimleri ve parmak izleri alınmaktadır. Güvenli Uçuş Programı bünyesinde “uçuş yok” listesi tutulmakta ve bu listede bulunan kişiler güvenlik nedeniyle uçağa bindirilmemektedir (Özeren ve Cinoğlu, 2006: 185).

Özetle Amerika Birleşik Devletleri göç politikası 11 Eylül 2001 tarihine kadar ekonomik yani işgücü ihtiyacını karşılama amaçlı iken yaşanan terör olaylarından sonra güvenlik amaçlı olmuştur. Dolayısıyla yapılan düzenlemeler ve kurumsal değişiklikler önceki düzenlemelere göre daha sert olarak

⁴⁴ Secure Flight Program, [http://www.tsa.gov/what we do/layers/secureflight/](http://www.tsa.gov/what_we_do/layers/secureflight/), (Erişim Tarihi: 06 Aralık 2011).

değerlendirilmektedir. Bu amaçla yapılan düzenlemeler ve kurumsal yapılanmalar kamuoyunun tepkisini çekmiştir.

2.3. AB VE ABD GÖÇ POLİTİKALARININ DEĞERLENDİRİLMESİ

1990'lı yıllarda iki kutuplu dünyada Sovyetler Birliği'nin dağılması ile tanımlanan güvenlik tehdidi ortadan kalkmış, ancak güvenliğe karşı tehdit oluşturabilecek göç gibi yeni kavramlar ortaya çıkmıştır.

Uluslararası göç yeni bir olgu olarak, hem Avrupa Birliği'nin hem de Amerika Birleşik Devletleri'nin güvenlik politikası oluşturma açısından gündemine girmiştir. Amerika Birleşik Devletleri'nde 11 Eylül 2001 tarihinde yaşanan terör olayları önce Amerika Birleşik Devletleri sonra da Avrupa Birliği'nin göç politikalarının sertleşmesine sebep olmuştur.

On bir Eylül 2001 tarihinde yaşanan terör olayları Amerika Birleşik Devletleri ve Avrupa Birliği'nin sınır güvenliğinin artırılması için çeşitli önlemler almasına yol açmıştır. Güvenliği artırmak üzere alınan bu önlemler, özgürlük ve güvenlik arasındaki ilişkinin güvenlik alanına doğru kaymasını sağlamıştır. Özgürlükten yapılan bu feragat, özellikle kişisel verilerin korunması ve mahremiyetin ihlali alanlarında ayrı bir tartışma konusu oluşturmuştur.

Avrupa Birliği uzun bir süre boyunca gündeminde olan ortak iltica ve göç politikası oluşturma yönünde bir iradeyi Amsterdam Antlaşması'yla beraber ortaya koymuş olmasına rağmen iltica ve göç politikalarında üye ülkeler düzeyinde bir standartlaşma yakalanamamıştır (Ünsal, 2007: 132). Ayrıca, iltica ve göç politikası kapsamında oluşturulan programların başarıya ulaşması da tam anlamıyla sağlanamamıştır (Ünsal, 2007: 132).

Amerika Birleşik Devletleri'nde önce 1990'lu yıllarda daha sonra 11 Eylül 2001'de gerçekleşen terör saldırılarından sonra, göç, ulusal güvenliğe bir tehdit olarak algılanmaya başlamıştır. Değişen tehdit algılaması, göç kontrol yönetiminin sıkılaştırılması ve göçmen sayısının sınırlandırılması sonuçlarını doğurmuştur. Çünkü Amerikan yönetiminin bu konudaki endişesi, terörist yabancıların ülkeye girip eylemler yapabilir olmalarıdır. Bu şekildeki tehdit algılaması ile güvenliği artırarak göçmen sayısının sınırlandırılması yöntemiyle baş edilmeye çalışılmaktadır.

Diğer yandan, Amerika Birleşik Devletleri'nde yeni kanunlar çıkartılmış, yeni kurumlar kurulmuş, sınır güvenliği için yeni yöntemler uygulanmış olmasına rağmen, 11 Eylül sonrası yapılan reformların tam anlamıyla başarıya ulaşmadığı dile getirilmektedir (Khanat, 2008: 59). Bu değerlendirmeye kaynak olarak ülkede yasadışı olarak yaşayan göçmenlerin sayısında 11 Eylül sonrasında ciddi bir düşüş olmaması gösterilmektedir (Khanat, 2008: 59).

2.4. TÜRKİYE GÖÇ POLİTİKASI

Türkiye, coğrafi konumu ve ekonomik durumu itibariyle hem göç alan, hem göç veren, hem de transit bir ülke konumundadır (Buz, 2008: 120; Çiçekli, 2004). Avrupa Birliği'ne aday ülke olmasından dolayı, Türkiye iltica ve göç politikası konularında Avrupa Birliği mevzuat uyumunu gözetmektedir. Avrupa Birliği iltica ve göç mevzuatına uyum sebebiyle vize politikası, çalışma izni ve geri kabul şartları gibi konular Türkiye'nin politika gündeminde her zaman bulunmaktadır (Çiçekli, 2004).

Türkiye göç politikasının tarihçesine bakıldığında yıllardır hala politika belirleme çalışmalarının devam ettiği görülmektedir. Önemle belirtilmesi gereken bir başka husus ise, Türkiye'de mevzuat bağlamında göç politikası veya hukuku kavramlarından daha çok yabancılar hukuku kavramının konuşuluyor olmasıdır.

Türkiye, uluslararası belgelere taraf olmak bakımından, mültecilerin anayasası kabul edilen Mültecilerin Hukuki Statüsüne İlişkin 1951 tarihli Cenevre Sözleşmesi'ni, TBMM'de 29 Ağustos 1961 tarihinde 359 sayılı Kanunla onaylamıştır.⁴⁵ Ancak Türkiye, Cenevre Sözleşmesi'nin 1. maddesinin (B) fıkrasının 1. bendi gereğince, Cenevre Sözleşmesi'ne tarih ve coğrafi çekince koyma konusunda tercih hakkını kullanmıştır. Cenevre Sözleşmesi'nin hükümlerini, sadece 01 Ocak 1951'den önce Avrupa'da meydana gelen olaylar nedeniyle ülkesine yapılacak sığınmalarda uygulayacağını 359 sayılı Onay Kanunu'nda hükme bağlanan Deklarasyonun (B) bölümünde beyan etmiştir.

Ayrıca, 1951 Sözleşmesi'ne Ek 1967 Protokolünü ise, 5 Ağustos 1968 tarihli Resmi Gazetede yayımlanan 6/10266 Sayılı Bakanlar Kurulu Kararı ile onaylanarak

⁴⁵ 359 Sayılı Onay Kanunu. 5 Eylül 1961 Gün ve 10898 Sayılı Resmi Gazete'de yayımlanmıştır.

kabul edilmiştir. 1967 Protokolünü 1968 yılında imzalayan Türkiye zaman sınırlamasının kaldırılmasını kabul etmekle beraber coğrafi çekince hakkını korumuştur. Avrupa Birliği Müktesebatına uyum kapsamında, Türkiye, mülteciler için kabul ettiği coğrafi çekinceyi kaldırmak durumundadır (Buz, 2008: 120).

Türkiye 1951 Cenevre Sözleşmesi'ne ve 1967 Protokolüne imza atarak uluslararası mülteci tanımını kabul etmiş ve uluslararası yükümlülükler üstlenmiştir. Bununla beraber Türkiye'nin Avrupa'dan gelen mültecilere Cenevre Sözleşmesi ve 1967 Protokolü dâhilinde değil İskân Kanunu doğrultusunda "Türk kökenli, soylu" olmaları temelinde sığınma sağladığı görülmektedir. Bu dönemin temel karakteristiği budur.

Türkiye sığınma tarihi açısından önemli bir düzenleme, 30 Kasım 1994 tarih ve 22127 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren "Türkiye'ye İltica Eden veya Başka Bir Ülkeye İltica Etmek Üzere Türkiye'den İkamet İzni Talep Eden Münferit Yabancılar ile Topluca Sığınma Amacıyla Sınırlarımıza Gelen Yabancılar ve Olabilecek Nüfus Hareketlerine Uygulanacak Usul ve Esaslar Hakkında Yönetmelik" olarak kabul edilmektedir. Türkiye'ye kitlesel bir şekilde Irak'tan 1988 ve 1991 yıllarında gelen Kürtlerin sığınması sürecinde, 1994 Yönetmeliği olarak bilinen bu düzenleme ihtiyaç olarak ortaya çıkmıştır. Bu yasal düzenleme Avrupa dışından Türkiye'ye sığınan kişilerle ilgili takip edilecek esas ve usulleri içermektedir (Buz, 2008: 121). Türkiye'nin sığınma hareketleri karşısında yasal yükümlülük üstlenmesi ve sığınma başvurularını değerlendirmeye ilgili usul ve esasları belirlemesi önemlidir. Böylece olası sığınma hareketleri karşısında hükümetlerin farklı tutum alması yerine, benzer usullere göre hareket edilmesinin gerekliliği bu yasal düzenlemeyle kabul edilmiştir.

Avrupa Birliği'ne tam üyelik müzakereleri sürecinde aday ülkelerin yerine getirmesi gereken şartlar bağlamında üzerinde durulan noktalardan biri de, Avrupa Birliği müktesebatıyla tezat oluşturmayacak nitelikte bir iltica mevzuatının yürürlükte olması ya da kısa vadede yürürlüğe konmasıdır. Avrupa Birliği, üzerinde hassasiyetle durduğu, ilticaya belirli bir düzen tesis edilmesi, yasadışı göç ve toplu göçün önlenmesi amacıyla, devletlerin mevzuatlarında gerekli değişikliklerin yapılarak, Avrupa Birliği müktesebatına uygun bir yapıya oturtulmasını öngörmekte ve bu konuda hazırlanan kanun tasarılarının da bir an önce yürürlüğe konmasını talep

etmektedir. Bu çerçevede, Avrupa Birliği'ne tam üyelik için başvuran devletlerin kabul etmeleri gereken bazı sözleşmelerin bulunduğu veya sınırlı olarak uygulamaya konulan sözleşmelerde gerekli değişikliklerin yapılması gerektiği vurgulanmaktadır. Yine, yasadışı göçün önlenmesi ve denetlenmesi amacıyla, Avrupa Birliği'nin göç alanındaki müktesebatı ve uygulamaları ile kabul edeceği ortak iltica ve göç prosedürünün benimsenerek uygulanmaya konulması hedeflenmektedir.

1999 yılında Helsinki Zirvesinde Türkiye'nin Avrupa Birliğine aday ülke olarak gösterilmesi ve Katılım Ortaklığı Belgelerinin açıklanmasıyla beraber Türkiye'nin iltica ve göç politikası yeni bir seyir kazanmıştır. Türkiye iltica ve göç politikasının Avrupa Birliği Müktesebatıyla uyumlu hale getirilmesi amacıyla, 2003 yılında Ulusal Programı (24 Temmuz 2003 tarihli ve 25178 sayılı Resmi Gazete), Nisan 2003 tarihinde Türkiye'de Dış Sınırların Korunmasına İlişkin Strateji Belgesi, Ekim 2003 tarihinde Türkiye'de Göç Yönetimi Eylem Planına Katkı Sağlayacak Strateji Belgesi (Göç Strateji Belgesi) ve Mart 2005 tarihinde İltica ve Göç Ulusal Eylem Planı kabul edilmiştir.

Avrupa Birliği müktesebatının üstlenilmesine ilişkin Türkiye Cumhuriyeti tarafından 24 Temmuz 2003 tarihli ve 25178 sayılı Resmi Gazetede ilan edilen Ulusal Program'da Türkiye, bu konuda 2005 yılına kadar özel bir İltica Yasası çıkaracağını, bu yasada en azından hangi konu ve düzenlemelerin olacağını evvelce taahhüt etmiştir. Yapılan değişiklikle İltica Yasası'nın 2012 yılına kadar çıkartılacağı söylenmiştir (Gümüş ve Kara, 2009: 2840). Bu ulusal eylem planı ile çıkarılması öngörülen İltica Yasası konusunda Nisan 2012 tarihi itibarıyla henüz bir gelişme olmamıştır. Emniyet Genel Müdürlüğü'nün internet sitesinde 25 Mart 2005 tarihinde Başbakan'ın imzası ile yürürlüğe giren İltica ve Göç Ulusal Eylem Planı metni bulunmaktadır.⁴⁶ Çıkarılması planlanan İltica Yasası ile konu hakkında uzman ve yetkili kurum olarak çalışması düşünülen ihtisas biriminin kurulması ve geliştirilmesi ile burada çalışacak personelin istihdam ve eğitimi planlanmıştır. Bu kapsamda, İçişleri Bakanlığı'na bağlı sivil ve profesyonel bir bütünleşmiş sınır yönetimi uzman biriminin kurulması öngörülmektedir (Acer, Kaya, ve Gümüş, 2011: 167).

⁴⁶ İltica Göç İşlemleri, http://www.egm.gov.tr/icerik_detay.aspx?id=123, (Erişim Tarihi: 10 Mart 2012).

Öncelikle doğu bölgelerinden başlamak üzere, Türkiye’de 2006 – 2010 yılları arasında 7 ayrı ilde, her biri ortalama 750 kişi kapasiteli olacak Sığınmacı Kabul, Barınma Merkezleri ve Mülteci Misafirhanelerinin kurulması planlanmıştır. İltica ve göç alanında çalışmakta olan ve çalışacak personelin eğitiminin sürekli kılınması için orta vadede Avrupa Birliği Twinning Projesi’ne bağlı olarak bir Eğitim Akademisi açılması düşünülmüştür. Ülkeden geri dönüşleri yapılacak kişilerin işlemleri sonuçlandırılana değin geçici olarak barındırılacakları yerler olarak orta vadede “Geri Gönderme Merkezleri” tesis edilmiştir. Yine orta vadede, mültecilerin entegrasyonu, eğitim programları, sağlık sorunları, sosyal yardımlar, çalışma hakları, sosyal ve kültürel haklara erişim konusunda planda öngörülen hususlar bulunmaktadır. Külfet paylaşımı konusunda; hem mülteci, sığınmacı, geçici koruma sağlanan yabancı ve tamamen yasadışı durumunda bulunan yabancıların Avrupa Birliği ülkelerince paylaşılması, hem de ekonomik faturanın paylaşılması öngörülmektedir. Emniyet Genel Müdürlüğü verilerine göre, 1995–2007 yılları arasında başvuru yapan sığınmacı sayısı yaklaşık 50 bindir (Gümüş ve Kara, 2009: 2844).

Avrupa Birliği Müktesebatına uyum çerçevesinde Türkiye, 22 Haziran 2006’da 57 sayılı İçişleri Bakanlığı Emniyet Genel Müdürlüğü genelgesini kabul etmiştir.⁴⁷ Bu genelgede, sığınmacılara sağlanacak yardımlara (sağlık, sosyal ve ekonomik) ve sığınmacılık başvurularına ilişkin usul ve esaslara değinilmektedir.

Türkiye, yasadışı göç ve insan ticaretiyle ilgili çeşitli uluslararası sözleşme ve protokolleri imzalamış ve onaylamıştır. Türkiye Sınır Aşan Örgütlü Suçlara karşı Birleşmiş Milletler Sözleşmesi’ni imzalamıştır (Çiçekli, 2005: 52). Ayrıca, Sınır Aşan Örgütlü Suçlara karşı BM Sözleşmesinin ek protokolleri olan Göçmen Kaçakçılığı ile Mücadele Protokolü ve İnsan Ticareti ile Mücadele Protokolü’nü de imzalamıştır (Çiçekli, 2005: 52).

Son yıllarda, iltica ve göç politikası konusunda Türkiye’de atılan önemli bir adım, 25 Mayıs 2010 tarihinde Resmi Gazetede yayımlanan Bütünleşmiş Sınır Yönetimi konulu, 2010/15 sayılı Başbakanlık Genelgesidir. Genelge ile İçişleri Bakanlığı’nın Avrupa Birliği müzakereleri kapsamında yürüttüğü Bütünleşmiş Sınır

⁴⁷ Uygulama Talimatı, http://www.egm.gov.tr/indirilendosyalar/uygulama_talimati_2010_genelge.pdf, (Erişim Tarihi: 10 Mart 2012).

Yönetimi Projesinin üst düzeyde koordinasyon ve işbirliğini sağlamak üzere Bütünleşmiş Sınır Yönetimi Koordinasyon Kurulu'nun kurulması uygun görülmüştür.⁴⁸ Genelgede öngörülen önemli bir konu da, sadece sınırlardan sorumlu, asker olmayan ve profesyonel bir sınır güvenlik teşkilatının kurulmasıdır.

“Ülkemizin daha açık ve daha güvenli bir sınır kontrol ve gözetim yapısına sahip olabilmesi için, bu konuda görevli kuruluşlarımızın ve mevzuatımızın Avrupa Birliği müktesebatıyla uyumlu hale getirilmesi, tüm sınır kapıları ile kara ve deniz sınırlarında görev yapmak üzere İçişleri Bakanlığına bağlı profesyonel bir sınır güvenlik teşkilatının kurulması amaçlanmaktadır.”⁴⁹

Dönemin İçişleri Bakanı Beşir Atalay “2014–2015 yıllarında hayata geçirilecek Bütünleşmiş Sınır Yönetimi Projesi ile sadece sınırlardan sorumlu ve İçişleri Bakanlığı'na bağlı profesyonel bir kolluk gücünün oluşturulacağı ve gerekli uzmanların yetiştirilmesi için Polis Akademisinde Sınır Yönetimi Bölümü'nün kurulduğunu açıklamıştır.”⁵⁰

Avrupa Birliği'nin uzunca zamandır belirlemeye çalıştığı ortak iltica ve göç politikasının somut adımları Tampere, Lahey ve Stockholm programlarıdır. 1999–2004 yılları arası dönemi kapsayan Tampere programı, 2005–2010 yılları arası dönemi kapsayan Lahey programı ve 2010–2015 yılları arası dönemi kapsayan Stockholm programlarında iltica ve göç alanında en somut başlık dış sınırların korunmasıdır. Diğer yandan, yasadışı göçün önlenmesinde birincil derecede önemli bir konu dış sınırların korunmasıdır. Bütün bunlar değerlendirildiğinde ise Avrupa Birliği müktesebatıyla uyumlu bir şekilde Türkiye'de bir iltica yasasının ivedilikle yürürlüğe konması gerekmektedir. Çıkartılması planlanan iltica yasası ile gerekli kurumsal düzenlemelerin kurulması ve görevli uzman birimin belirlenmesi sağlanmalıdır. Bununla birlikte, Türkiye, 1951 tarihli Cenevre Sözleşmesi kapsamında mülteciler için kabul ettiği coğrafi çekinceyi Avrupa Birliği müktesebatıyla uyum çerçevesinde kaldırmak durumundadır(Buz, 2008: 120).

⁴⁸ 2010/15 Sayılı Bütünleşmiş Sınır Yönetimi konulu Başbakanlık Genelgesi, http://www.basbakanlik.gov.tr/genelge_pdf/2010/2010-0010-006-6393.pdf#page=1, (Erişim Tarihi: 11 Aralık 2011).

⁴⁹ a.g.e.

⁵⁰ a.g.e.

2.5. BÖLÜM ÖZETİ

Yasal göç ve yasadışı göç, ülkelerin politika gündemindedir. Ülkeler göçü ve göçmenleri ekonomiye destek sağlayan ve ihtiyaç duydukları istihdamı karşılamalarına yardımcı olan bir alternatif olarak görmektedirler. Göç ve göçmenler hakkındaki bu değerlendirme, 11 Eylül 2001 tarihinde Amerika Birleşik Devletleri'nde yaşanan terör olayları sonrasında değişmiştir. Yaşanan terör olayından sonra başta Amerika Birleşik Devletleri olmak üzere, Avrupa Birliği ve birçok ülke göç konusunu ulusal güvenlik bağlamında değerlendirmeye başlamıştır.

Avrupa Birliği'nde iltica ve göç politikasının birlik düzeyinde ortak çıkar olarak kabul edilmesi 1993 Maastricht Antlaşması ile belirlenmiştir. Ortak bir göç politikası belirleme çalışmaları 1999 yılında yürürlüğe giren Amsterdam Antlaşması'ndan beri devam etmektedir. Avrupa Birliği'nde ortak göç politikası belirleme çalışmaları son olarak Avrupa Komisyonu tarafından 13 Şubat 2008 tarihinde sunulan yeni sınır paketi ile düzenlenmektedir.

Amerika Birleşik Devletleri son yüzyıllarda en çok göç alan ülke konumunda olmuştur. Amerika Birleşik Devletleri göç politikası, 2001 yılına kadar daha çok Meksikalı göçmenlerle ilgili düzenlemeler çerçevesindedir. On bir Eylül 2001 tarihine kadar ekonomik odaklı olan Amerika Birleşik Devletleri göç politikası 11 Eylül 2001 tarihinden sonra güvenlik odaklı düzenlemelere sahne olmaktadır. Güvenlik odaklı yaklaşımın en somut göstergesi 2001 yılında yasalaşan kısa adıyla Vatanseverlik Yasası ve 2003 yılında kurulan İç Güvenlik Örgütü'dür.

Amerika Birleşik Devletleri göç politikasında, 11 Eylül 2001 terör olayından sonra reform mahiyetinde birçok değişiklik yapılmıştır. Amerika Birleşik Devletleri göç politikasındaki en önemli değişiklik sınır güvenliğini artırarak yasadışı göçmen sayısını azaltmak ve muhtemel teröristlerin ülkeye girişini engellemek üzere biyometrik sistemlerin göç kontrol yönetiminde kullanılmasıdır. Amerika Birleşik Devletleri göç politikasında yapılan değişiklikler ile göç politikası Amerika Birleşik Devletleri için ulusal güvenlik politikası haline getirilmiştir.

Türkiye, coğrafi konumu ve içinde bulunduğu siyasi bölge itibariyle hem göç alan hem de göç veren bir ülkedir. Türkiye'de uzunca zamandır göç politikası çalışmaları devam etmektedir. Bu konuda, Türkiye'de müstakil bir yasal düzenleme

henüz yapılmamıştır. Türkiye’de göç politikası belirleme kapsamında yapılan en son ve önemli bir gelişme 25 Ekim 2010 tarihinde Resmi Gazetede yayımlanan 2010/15 sayılı “Bütünleşmiş Sınır Yönetimi” konulu Başbakanlık Genelgesi’dir. Başbakanlık Genelge’si ile Bütünleşmiş Sınır Yönetimi Projesi’nin üst düzeyde koordinasyonunu sağlayan “Bütünleşmiş Sınır Yönetimi Koordinasyon Kurulu” kurulmuştur.

ÜÇÜNCÜ BÖLÜM

BİYOMETRİNİN GÖÇ KONTROL MEKANİZMASINDA KULLANILMASI

Sınır kontrollerinde güvenlik önlemlerinin artırılmasında ilk akla gelen çözüm biyometrik sistemlerin kullanımı olmuştur. Terörizm, yasadışı göç ve kimlik hırsızlığı gibi suçların artması sebebiyle insan hata unsurunu da minimuma indiren biyometri gibi güvenlik artırıcı sistemlerin sınır kontrollerinde kullanılması son yıllarda artmaya başlamıştır. Yasadışı göçün önlenmesinin öncelikle bir sınır kontrol meselesi olduğu düşünülerek, özellikle 11 Eylül olayının yarattığı güvenlik baskısının etkisiyle de, ülkeler sınır kontrollerinde güvenlik önlemlerini artırmaktadır.

Farklı amaçlarla çeşitli alanlarda kullanılan biyometri, sınır kontrollerinde de bir ihtiyacı doldurmuştur (Thomas, 2005: 378). Seyahat belgelerinde biyometrik özelliklerin varlığı sınır kontrolünün daha etkin yapılmasını sağlamaktadır. Diğer yandan, biyometrik seyahat belgeleri olsa bile rutin kontroller veya arananlar listesine göre denetim gibi çeşitli kontroller ayrıca yapılabilmektedir. Avrupa Birliği uygulamasında, şüpheli durumlarda biyometrik sistem denetimine ek olarak rutin kontrol de yapılabilmektedir (COM 2004/116: 4).

Biyometrinin göç kontrol mekanizmasında kullanılması çok yeni bir durum değildir. Göç kontrol kapsamında biyometrik sistemler ilk defa 1992 yılında Amsterdam Schiphol Havalimanı'nda kullanılmıştır (Frontex, 2007: 24). Schiphol Havalimanı'nda kurulan bu sistem iyi niyetli seyahat eden yolcuların kolay geçmeleri için parmak izi ile kişileri tanıyan bir yapıdır (Frontex, 2007: 25).

İyi niyetli seyahat eden yolcular için sınır geçiş işlemlerinin kolaylaştırılması, biyometrik özelliklerin de dâhil olduğu sınır görevlilerinin müdahalesine gerek bırakmayan otomatik geçiş sistemleri ile mümkün olabilmektedir.

Otomatik sınır kontrolü, sınır geçişinde bir görevli olmadan, kişinin geçerli bir biyometrik pasaportu ve pasaportundaki bilgiler ile otomatik geçiş sisteminden faydalanarak geçmesidir (Redpath, 2007: 29). Otomatik sınır kontrol kapıları, gönüllü olarak sisteme kaydolana hizmet vermekte ve biyometrik bilgiler ile

sınırdan hızlı geçmek için bazı havalimanlarında ayrı şerit olabilmektedir (Redpath, 2007: 29).

İngiltere’de Sınır ve Göç Kurumu (*Borders and Immigration Agency*) tarafından sınır güvenliğini artırmak ve iyi niyetli sık seyahat eden yolcuların sınır geçiş işlemlerini kolaylaştırmak üzere e-sınır (*e-borders*) programı başlatılmıştır. E-sınır uygulamasına göre, 29 Şubat 2012 tarihinden itibaren İngiltere’de altı aydan fazla kalacak kişiler biyometrik vize almak durumundadırlar.⁵¹ E-sınır uygulaması kapsamında yapılanlardan birisi, IRIS sisteminin havalimanlarında kurulmasıdır. IRIS sistemi ile bu sisteme kayıt olmuş gönüllü kullanıcılar sınır kontrollerinde görevlilerin önünde sıra beklemeden iris tanıma sisteminin önünde gözlerini tanıtarak sınır kapısındaki otomatik kapılardan hızlıca ve güvenle geçmektedirler (PublicTechnology, 2007). IRIS sistemine kullanıcılar ortalama 5 dakikada kayıt olabilmektedirler (Frontex, 2007: 61). IRIS sistemine kaydolabilen yolcu türü üçtür. Bunlar; İngiltere’de kalıcı vizeyle ikamet eden yabancılar, çalışma vizesiyle İngiltere’de ikamet eden yabancılar ve aileleri ile uzun süreli olarak İngiltere’de ikamet eden öğrenciler ile İngiltere’de ikamet şartlarını taşıyan sık seyahat eden yolcular olarak sıralanabilmektedir (PublicTechnology, 2007).

Parmak izi tanıma, iris tanıma, ses tanıma gibi biyometrik sistemler ile kişiler daha hızlı ve doğru olarak tanınabilmektedirler. Biyometrinin, klasik yöntemler olarak bilinen kimlik kartı, seyahat belgesi ve resim karşılaştırması gibi yöntemlere göre doğruluk oranı daha yüksektir (Redpath, 2005: 8). Göç bağlamında pasaport ve seyahat belgelerinde biyometrik özelliklerin varlığı sahte seyahat belgelerinin tespitini kolaylaştırmaktadır (Redpath, 2007: 29).

On bir Eylül 2001 günü Amerika Birleşik Devletleri’nde meydana gelen terör olayı ile 11 Mart 2004 günü İspanya’da ve 7 Temmuz 2005 günü İngiltere’de meydana gelen terör olayları sınır kontrollerinin artırılması için vize işlemlerinde biyometrinin kullanımının yaygınlaşmasına etki etmiştir. Amerika Birleşik Devletleri’nde İç Güvenlik Örgütü’nün (*Department of Homeland Security*) pasaport ve seyahat belgelerine biyometrik özelliklerin dâhil edilmesini öngören US-VISIT programı 2004’de uygulamaya konmuştur. Akabinde Avrupa Birliği Konseyi, 13

⁵¹ UK Border Agency, <http://www.ukba.homeoffice.gov.uk/visas-immigration/settlement/>, (Erişim Tarihi: 20 Mart 2012).

Aralık 2004 tarihinde kabul ettiđi bir tüzük (EC 2252/2004) ile Avrupa Birliđi üye ülkelerinin pasaportlarına biyometrik özelliklerin eklenmesini kabul etmiştir. Tüzük, yüz ve parmak izi özelliklerini kaydetmek üzere pasaport ve seyahat belgelerine RFID bütünleşmiş devrelerinin eklenmesini zorunlu kılmıştır (Hornung, 2007: 246).

Bununla birlikte, biyometri kullanımının insan haklarına olumsuz bazı etkileri bulunabilmektedir. Bunlardan birkaçı, mahremiyetin ihlali ve kişisel bilgilerin korunmasındaki zafiyetler olarak sayılabilmektedir. Pasaport ve seyahat belgelerinde biyometrik özelliklerin bulunması özgürlük savunucuları tarafından yoğun bir şekilde eleştirilmektedir.⁵² Diğer yandan devletler sınır güvenliğinin artırılması için ek önlemler alınması gerektiğine inanmaktadırlar. Biyometrik pasaport tartışmaları ile devletlerin güvenlik ihtiyacı ile kişilerin mahremiyet hakkının doğru bir şekilde dengelenmesi gerekliliđi bir kez daha gündeme gelmektedir.

3.1. YASADIŞI GÖÇLE MÜCADELE

Göç politikası kapsamında önemli bir başlık yasadışı göçle mücadeledir. Örneğın, Amerika Birleşik Devletleri'ne yılda yaklaşık üç milyon kişinin yasadışı yollarla giriş yaptığı tahmin edilmektedir (Koyuncu, 2006: 60).

Yasadışı göç; “bir kişinin, yasal olarak bulunduğu ülkeyi terk ederek başka bir ülkeye yasadışı yollarla girmesi, yasal yollardan girdikten sonra süresi içinde ülkeyi terk etmemek suretiyle, o ülkede, yasal izin sahibi olmaksızın uzun süreli olarak yaşaması ve/veya çalışmasıdır” (Özcabı, 2007: 10).

Yasadışı göçle mücadele, günümüzde hem ekonomik gerekçelerle hem de güvenlik gerekçesiyle yapılmaktadır. Yasadışı göçle mücadele için yasal ve teknik önlemler ile birlikte uluslararası yardımlaşma da gereklidir (Koyuncu, 2006: 63). Ülkelerarası işbirliđi olmadan yasadışı göçle etkin bir şekilde mücadele edilmesi çok zordur.

Yasadışı göçle mücadele için BM Sınırşan Örgütlü Suçlarla Mücadele Sözleşmesi ve Sözleşme'nin eki Göçmen Kaçakçılığı ile İnsan Ticaret'ine ilişkin Ek

⁵² An Open Letter to the European Parliament on Biometric Registration of all EU Citizens and Residents To the Members of the European Parliament, <http://www.edri.org/campaigns/biometrics>, (Erişim tarihi: 11 Ekim 2011).

Protokoller gibi yasal düzenlemeler bulunmaktadır. BM Göçmen Kaçakçılığına Karşı Ek Protokol'ün 11. maddesi, göçmen kaçakçılığının önlenmesi için gerekli olabilecek sınır kontrollerinin güçlendirilmesini öngörmektedir (Koyuncu, 2006: 60). Türkiye, BM Sınırşan Örgütlü Suçlarla Mücadele Sözleşmesi ve Göçmen Kaçakçılığı ile İnsan Ticaretine ilişkin ek protokolleri 13 Aralık 2000 tarihinde imzalamıştır (Terzioğlu, 2002: 12). Bu Sözleşme ve ekleri TBMM'de onaylanmış ve 19 Mart 2003 tarihli resmi gazetede yayınlanmıştır.⁵³ Ülkemizde BM Sınırşan Örgütlü Suçlarla Mücadele Sözleşmesi'nin eki olan Göçmen Kaçakçılığı Protokolü'ne uyum çerçevesinde bazı yasal önlemler alınmıştır.

Avrupa Birliği üye ülkelerine yasadışı girişin cezai çerçevesinin güçlendirilmesi için 28 Kasım 2002 tarihinde, 2002/90/JHA ve 2002/946/JHA isimli iki çerçeve karar kabul edilmiştir. Bu çerçeve kararlarda özgürlük, güvenlik ve adalet alanını sağlamak için yasadışı göçle mücadele edilmesi gerektiği belirtilmiştir.

Avrupa Birliği, üçüncü ülkelere gelen yasadışı göçle mücadele etmek üzere bir tebliğ kabul etmiştir.⁵⁴ Tebliğ ile hem yasadışı göçün önlenmesi hem de sınır kontrollerinin artırılarak güvenliğinin sağlanması öngörülmektedir.

Ayrıca, Geri Kabul Anlaşmaları, ülkeleri yasadışı göçe karşı önlem almaya teşvik eden, yasadışı göçmenlerin insan onuruna yakışır şekilde ülkelere gönderilmelerini sağlayan etkin bir araçtır. Sahte pasaport ve vize, yasadışı göçmenlerin yoğun olarak kullandığı yöntemlerdendir (Koyuncu, 2006: 53). Sahteciliğin önlenmesi için yapılan çalışmalar da, yasadışı göçle mücadele için etkin bir araçtır.

Teknik önlemler olarak öncelikli olarak sınırların güvenliğinin artırılması,⁵⁵ yabancı göçmenlerin dikkatlice izlenmesi ve yasadışı göçmenlerin iş imkânlarının azaltılması gibi konular sayılabilmektedir. Ayrıca, göç veren ülkelerdeki yoksullukla mücadele göç talebinin azaltılması sonucunu doğurabilmektedir (Koyuncu, 2006: 78). Göç alan ülkeler ekonomik gerekçelerle göç eden kişilere göç veren ülkedeki iş imkânlarının artırılması ile yardımcı olmaktadır. Tabii bu yöntem daha çok

⁵³ Sınırşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair 4800 ve 4804 sayılı Kanunlar, 19 Mart 2003 tarih ve 25052 sayılı Resmi Gazete.

⁵⁴ Communication from the Commission of 19 July 2006 on policy priorities in the fight against illegal immigration of third-country nationals. COM(2006) 402.

⁵⁵ Koyuncu, 2006: 58.

ekonomik gerekçelerle göç eden kişiler için faydalı olabilecek bir durumdur. Sosyal gerekçelerle göç eden kişiler için süreç yeniden değerlendirilmelidir.

3.2. BİYOMETRİK PASAPORT

Biyometrik sistemlerin göç yönetiminde kullanılmasının bir uygulaması biyometrik pasaportlarda görülmektedir. Biyometrik pasaport, elektronik veya e-pasaport denilen pasaportlar ile karıştırılabilmektedir. Hem biyometrik pasaportlar hem de elektronik pasaportlar makine tarafından otomatik olarak okunabilen özelliktedir. Bu bölümde, makine tarafından otomatik olarak okunabilen pasaport, elektronik pasaport ve biyometrik pasaport türleri ve farkları tartışılmaktadır. Belirtilen bu üç pasaport türü, Türkiye kamuoyunda net olarak bilinmemektedir. Türkiye’de 1 Haziran 2010 tarihinde yeni başlayan uygulama kamuoyunda biyometrik pasaport olarak bilinmesine rağmen aslında elektronik pasaporttur. Türkiye’de yeni uygulamaya başlayan pasaport türünün neden biyometrik pasaport değil de elektronik pasaport olduğu Türkiye uygulaması bölümünde izah edilmektedir.

3.2.1. Uluslararası Sivil Havacılık Örgütü (*International Civil Aviation Organization - ICAO*)

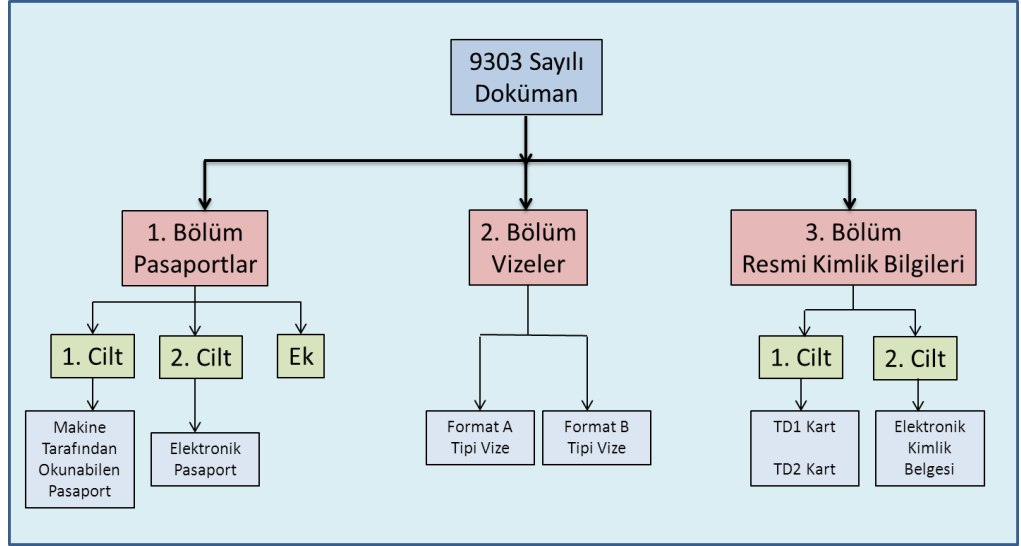
Birleşmiş Milletlere bağlı bir uzmanlık kuruluşu olan Uluslararası Sivil Havacılık Örgütü (*International Civil Aviation Organization - ICAO*), 7 Aralık 1944 tarihinde Şikago Sözleşmesi’nin imzalanmasıyla kurulmuştur.

Uluslararası Sivil Havacılık Örgütü, Uluslararası Sivil Havacılık Sözleşmesi’ne göre, seyahat belgelerinin standardizasyonu ve güvenliklerinin artırılması konusunda çalışmalar yapmaktadır (Roberts, 2005: 31).

Uluslararası Sivil Havacılık Örgütü’nün 9303 sayılı kararı,⁵⁶ pasaport ve seyahat belgelerinin taşınması gereken ortak formatı belirlemektedir. Pasaport ve seyahat belgelerinin biyometrik özellikleri içermesi ve buna bağlı özelliklerin

⁵⁶ ICAO Kararı 9303 Bölüm 1, <http://www2.icao.int/en/MRTD/Downloads/Doc%209303/Doc%209303%20English/Doc%209303%20Part%201%20Vol%201.pdf>, (Erişim Tarihi: 15 Eylül 2010).

Uluslararası Sivil Havacılık Örgütü'nün 2005 yılında yayınladığı kurallara uygun olması gerekmektedir. Uluslararası Sivil Havacılık Örgütü'nün 9303 sayılı kararında, pasaport, vize ve çeşitli kimlik kartlarının hepsinin standartları ayrıntılı olarak açıklanmaktadır.⁵⁷



Şekil 6: ICAO 9303 Sayılı Dokümanın Bölümleri⁵⁸

Uluslararası Sivil Havacılık Örgütü'nün 9303 sayılı kararında tanımlanan seyahat belgelerinin çeşitleri şekil 6'da toplu olarak gösterilmektedir. Özetle, 9303 sayılı doküman, vize, pasaport ve kimlik belgelerinin elektronik sürümlerinde bulunması gereken standart özellikleri belirlemektedir.

3.2.2. Makine Tarafından Okunabilen Seyahat Belgeleri (*Machine-Readable Travel Documents-MRTD*)

Makine tarafından okunabilen seyahat belgeleri (*Machine-Readable Travel Documents-MRTD*), seyahat belgesi veya pasaporttaki kimlik bilgilerinin kodlanmış bir şekilde optik karakter formatında seyahat belgesinin üzerinde saklandığı belgelerdir (Demirci, 2005: 7). Makine tarafından otomatik olarak okunabilen seyahat belgesinin kimlik sayfasında 44 karakterden oluşan bir alan bulunmaktadır

⁵⁷ a.g.e.

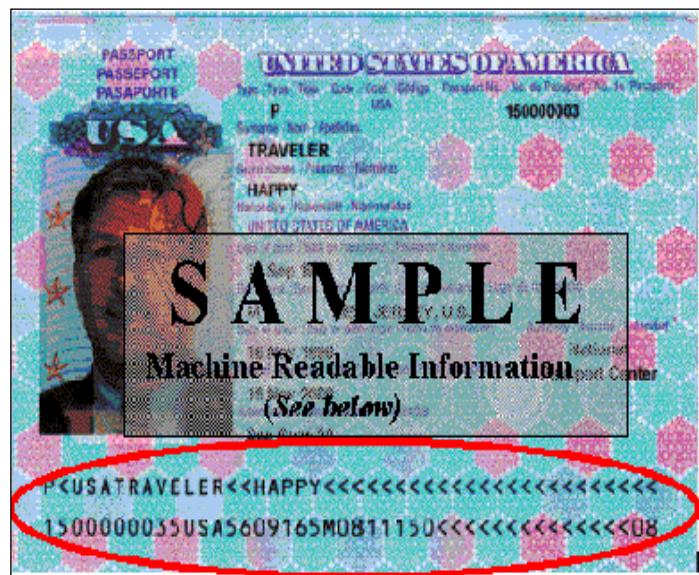
⁵⁸ ICAO, 2007: 9.

(Vakalis, 2011: 485). Makine tarafından otomatik olarak okunabilen 44 karakterlik alan genelde seyahat belgesinin en alt bölümde bulunmaktadır. MRZ diye kısaltılan makine tarafından okunabilen bölge (*machine readable zone*) belge sahibine ilişkin bilgileri içermektedir.

Uluslararası Sivil Havacılık Örgütü ICAO, her ülkenin pasaportlarının makine tarafından okunabilen (*Machine-Readable Travel Documents-MRTD*) pasaport standartlarını taşıması için Nisan 2010 tarihini nihai tarih olarak belirlemiştir (Roberts, 2005: 31). Pasaport ve seyahat belgelerindeki biyometrik özelliklerin, bütün ülkelerde ortak bir standart formata gelmesi önemlidir. Eylül 2010 tarihi itibarıyla 188 ülke, makine tarafından okunabilen pasaport (MRTD) düzenlemesi yapmıştır (Kajevic, 2006: 22; Khanat, 2008: 22).

Amerika Birleşik Devletleri'nde Ekim 2001'de yasalaşan Vatanseverlik Yasası (*The USA Patriot Act*), bütün yabancı turistlerin makine tarafından otomatik okunabilen biyometrik pasaport taşımaması zorunlu kılmıştır (Thomas, 2005: 378).

Makine tarafından okunabilen seyahat belgelerinin standart özellikleri, Uluslararası Sivil Havacılık Örgütü ICAO'nun 9303 sayılı dokümanının 1980 yılında yayımlanan ilk sürümünde tanımlanmıştır (Demirci, 2005: 7).



Resim 15: Makine tarafından otomatik olarak okunabilen pasaport (ABD pasaportu)

Resim 15'in alt tarafında makine tarafından otomatik olarak okunabilen 44 karakterlik bölüm bulunmaktadır. Elektronik pasaportlardaki kimlik bilgileri sınır kontrol işlemlerini yürüten mercilerce, kolay ve hızlı bir şekilde tespit edilip kontrol edilebilmektedir.

1980 yılından itibaren birçok ülkede makine tarafından okunabilen seyahat belgesi veya pasaport kullanılmaya başlanmıştır. Amerika Birleşik Devletleri tarafından 2004 yılında yapılan bir düzenlemeyle, Vize Feragat Programına (VWP) dâhil olan ülkelerin vatandaşları Amerika Birleşik Devletleri'ne girişlerinde makine tarafından otomatik olarak okunabilen pasaport taşımak zorundadırlar.⁵⁹

Seyahat belgelerinin doğruluğu ve düzenlenme bilgilerinin doğrulanması biyometri ile üç türlü yapılabilir. ⁶⁰ Seyahat belgelerini düzenleyen devlet görevlilerinin yaptıkları işlerin logunun tutulması, seyahat belgelerinin içerisinde kişiye ait biyometrik özelliklerin muhafaza edilmesi ve son olarak seyahat belgelerine biyometrik özelliklerin standart bir format ile kaydedilmesi ile sağlanabilmektedir (Redpath, 2007: 29).

3.2.3. Elektronik Pasaport

Elektronik pasaport, Uluslararası Sivil Havacılık Örgütü ICAO'nun 9303 sayılı belgesi standartlarına göre makine tarafından otomatik olarak okunabilen pasaporttur. Pasaporttaki bütünleşmiş devrede hangi ülke pasaportu olduğunu belirten elektronik sertifika bulunmaktadır. Elektronik pasaporttaki bütünleşmiş devreye yüz resmi kaydedilebilmektedir. Elektronik pasaporta kaydedilen resim biyometrik özellikler içermemektedir. Örneğin, Malezya pasaportları 1998 yılında elektronik pasaport özelliklerine sahiptir (Juels, Molnar, ve Wagner, 2005: 1). Malezya pasaportlarında o dönemde pasaport sahibinin parmak izi resminin kaydedildiği bir bütünleşmiş devre bulunmaktadır.

⁵⁹ Vize Feragat Programına dâhil olan kişilerin ABD'ye biyometrik pasaport ile giriş tarihi uzatılarak 26 Ekim 2006 tarihine ertelenmiştir.

⁶⁰ Ergen ve Çalışkan, 2011: 459.

3.2.4. Biyometrik Pasaport

Biyometrinin göç kontrol mekanizmasında kullanılması sonucu ortaya çıkan önemli bir kavram biyometrik pasaporttur. Biyometrik pasaport, seyahat eden kişinin tanınması ve doğrulanmasına yarayan biyometrik özellikleri içeren pasaporta denmektedir.

Avrupa Birliği biyometrik pasaport uygulamasında; pasaporttaki biyometrik bilgiler Radyo Frekans Tanımlama (*Radio-frequency identification-RFID*) bütünleşmiş devrelerine kaydedilmektedir. Amerika Birleşik Devletleri biyometrik pasaport uygulamasında pasaporttaki biyometrik bilgiler contactless devrelerine kayıt yapılmaktadır. Avrupa Birliği ve Amerika Birleşik Devletleri uygulamaları arasındaki tek fark bu değildir. Uluslararası Sivil Havacılık Örgütü' nün ICAO biyometrik pasaportlarda bulunan kayıt ünitesinin 32 KB olması önerisi bulunmasına rağmen Amerika Birleşik Devletleri biyometrik pasaportlarındaki kayıt ünitelerinin hafızası 64 KB ve Avrupa Birliği biyometrik pasaportlarındaki kayıt ünitelerinin hafızası 32 KB olarak kullanılmaktadır.



Resim 16: Finlandiya Biyometrik Pasaportu

Biyometrik pasaport, Uluslararası Sivil Havacılık Örgütü ICAO'nun 9303 sayılı belgesi standartlarına göre makine tarafından otomatik olarak okunabilen, bütünleşmiş devrede hangi ülke pasaportu olduğunu belirten elektronik sertifika ve bütünleşmiş devrede parmak izi veya yüz resmi gibi biyometrik verilerin saklandığı bir elektronik pasaporttur.

3.3. VİZE İŞLEMLERİNDE VE SINIR KONTROLLERİNDE BİYOMETRİ UYGULAMALARI

Vize işlemlerinde ve sınır kontrollerinde biyometri uygulamaları birçok ülkede yaygın bir şekilde kullanılmaktadır. Göç kontrol yönetiminde biyometrik sistemler, pasaportlarda, sınırlardaki otomatik geçiş kapılarında ve vize kontrol işlemlerinde kullanılmaktadır.

Yukarıda da ifade edildiği gibi, 188 ülke, Eylül 2010 tarihi itibarıyla ICAO'nun 9303 sayılı dokümanında belirlediği standartlara göre makine tarafından okunabilen pasaport (*MRTD*) uygulamasına sahiptir (Kajevic, 2006: 22; Khanat, 2008: 22). Ayrıca, İsviçre, Finlandiya ve İngiltere gibi birçok ülke iyi niyetli seyahat eden yolcular için sınır geçiş işlemlerini kolaylaştırmak üzere biyometrik sistemler kullanılmaktadırlar (PublicTechnology, 2007).

Benzer şekilde, İngiltere'de, Temmuz 2003 yılında altı aylık bir biyometrik vize denemesi yapılmıştır. Vize kontrol denemesi, sadece Sri Lanka kökenli ziyaretçiler için uygulanmış ve altı aylık deneme sonucu sistem yedi belgesiz göçmen ortaya çıkartmıştır (Thomas, 2005: 382). Bu sonuçtan sonra İngiltere biyometrik vize sistemini Cibuti, Eritre, Etiyopya, Tanzanya ve Uganda vatandaşlarını kapsayacak şekilde genişletmiştir.

İlerleyen bölümlerde, biyometrik pasaport ve uygulaması detaylı inceleneceğinden burada Avrupa'nın dört büyük havalimanında uygulanan biyometrik sistem temelli otomatik geçiş kapıları hakkında kısaca bilgi verilmektedir.

Göç yönetiminde kullanılan bir başka biyometrik sistem otomatik sınır geçiş kapısı sistemidir. Otomatik sınır geçiş kapıları, iyi niyetli veya sık seyahat eden yolcuların sınır kontrol işlemlerini hızlandırmaktadır. Otomatik geçiş kapısı mevcut bulunan sınır kapılarında ise yolcular herhangi bir biyometrik tarama türünü kullanarak sınır kapısını hızlıca geçmektedirler.

Avrupa ülkelerinde birçok havalimanında otomatik geçiş kapısı kullanılmaktadır. Amsterdam Schiphol Havalimanı'nda PRIVIUM iris tarama sistemi, Frankfurt Havalimanı'nda ABG iris tarama sistemi, Paris Charles de Gaulle Havalimanı'nda PEGASE parmak izi tanıma sistemi ve Londra Heathrow

Havalimanı'nda IRIS ve miSense iris tarama sistemi otomatik geiş kapısı olarak kullanılmaktadır (Frontex, 2007: 6).



Resim 17: Schiphol Havalimanı PRIVIUM Iris Tarama Otomatik Geiş Kapısı⁶¹

Göç kontrol kapsamında biyometrik sistemler ilk defa 1992 yılında Amsterdam Schiphol Havalimanı'nda kullanılmıştır (Frontex, 2007: 24). Amsterdam Schiphol Havalimanı'nda Privium isimli iris otomatik geiş sistemi 23 Ekim 2001 tarihinde test uygulamasına başlamıştır (Frontex, 2007: 29).



Resim 18: Frankfurt Havalimanı ABG İris Tarama Otomatik Geiş Kapısı⁶²

⁶¹ Frontex, 2007: 34.

⁶² Frontex, 2007: 42.

Frankfurt Havalimanı'nda 2004 yılı Şubat ayından itibaren ABG İris Tarama Otomatik Geçiş Kapısı sistemi mevcuttur (Frontex, 2007: 37). ABG projesinin amacı hızlı geçiş, güvenli sistem ve insan kaynaklarından azami tasarruf etmektir.



Resim 19: Charles de Gaulle Havalimanı PEGASE Parmak İzi Tanıma Otomatik Geçiş Kapısı

Londra Heathrow Havalimanı, IRIS Iris Tarama Otomatik Geçiş Kapısı sistemi 2005 yılından bu yana hizmet vermektedir (Frontex, 2007: 59). Heathrow Havalimanı, Temmuz 2005 tarihinde Londra bombalamalarının akabinde 2 hafta kapalı kalmıştır.



Resim 20: Londra Heathrow Havalimanı IRIS İris Kayıt Bölümü

Şimdi, Avrupa Birliği uygulaması ve Amerika Birleşik Devletleri'nin göç kontrol yönetiminde biyometrik sistem kullanımı tartışılmaktadır.

3.3.1. Avrupa Birliği Uygulaması

Avrupa Birliği göç politikasında güvenlik artırımı anlamında yapılan değişikliklerden birisi, üye ülkelere giriş yapan Avrupa Birliği üyesi olmayan ülke vatandaşlarının biyometrik pasaport kullanma zorunluluğunun getirilmiş olmasıdır (Özcan ve Yılmaz, 2007: 99). Diğer yandan, Avrupa Birliği'nin pasaport ve seyahat belgelerinde biyometrik özelliklerin eklenmesi düzenlemesi yüz resmi özelliği açısından 28 Aralık 2007 ve parmak izi özelliği açısından 28 Haziran 2009 tarihinde yürürlüğe girmiştir.⁶³ Yüz resmi taşıyan seyahat belgesine birinci nesil biyometrik pasaport belgesi parmak izi taşıyan seyahat belgelerine ikinci nesil biyometrik pasaport belgesi denmektedir (Frontex, 2011b: 4). Göç kontrol yönetim sisteminde güvenliğin artırılması ve sahteciliğin önlenmesi gibi

⁶³ Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009R0444:EN:NOT>, (Erişim Tarihi: 14 Aralık 2011).

sebeplerle Avrupa Birliği'nde birlik düzeyinde 2000'li yıllardan itibaren çeşitli düzenlemeler yapılmıştır.

3.3.1.1. AB Biyometrik Pasaport Düzenlemeleri

Avrupa Birliği Konseyi, sahteciliğin önlenmesi için pasaport ve seyahat belgelerinin güvenlik standartlarını belirleyen kararını⁶⁴ 17 Ekim 2000 tarihinde kabul etmiştir. Karar, 28 Ekim 2000 tarihli ve OJ C 310 sayılı Resmi Gazetede yayımlanarak karar tarihinde yürürlüğe girmiştir. Avrupa Birliği üye ülkeleri, 11 Eylül 2001 terör olayından sonra seyahat belgelerinin güvenliğini artırmak için hızlıca önlem alınması gerektiğini ve pasaport ile seyahat belgelerinin güvenlik standartlarını belirleyen 17 Ekim 2000 tarihli kararın geliştirilmesi gerektiğini düşünmektedirler. Daha sonradan, pasaportlarda yüksek güvenliqli resim olmasını zorunlu kılan EC 1683/1995 tüzüğünü deęiřtiren ve güncelleyen bir tüzük (EC 334/2002) 18 řubat 2002 tarihinde kabul edilmiştir.

Selanik'te 19–20 Haziran 2003 tarihlerinde yapılan Avrupa Birliği Zirvesi'nde, üçüncü ülke vatandaşlarının ve Avrupa Birliği üyesi ülke vatandaşlarının pasaport ve seyahat belgelerinin güvenliğini artırmak için biyometrik özelliklerin eklenmesi kararı alınmıştır.

Dięer yandan, Avrupa Birliği üye ülkelerinin vatandaşlarının Amerika Birleşik Devleti'ne vizesiz girebilmesini düzenleyen Vize Feragat Programından (*Visa Waiver Program-VWP*) faydalanabilmeleri için pasaport ve seyahat belgelerine biyometrik özelliklerin eklenmiş olması gerekmektedir.

Bütün bu gelişmeler sonucu, üye ülkeler pasaportlara biyometrik özelliklerin eklenmesinin de bir ihtiyaç olduğunu belirtmişler ve bu konuda tekliflerde bulunmuşlardır. Konsey, 13 Aralık 2004 tarihinde kabul ettięi bir tüzük (EC 2252/2004)⁶⁵ ile Avrupa Birliği üye ülkeleri vatandaşlarının pasaportlarına biyometrik özelliklerin eklenmesini öngörmüştür (Council, EC 2252/2004). Tüzük,

⁶⁴ The Security Characteristics Of Passports And Other Travel Documents, 17 Ekim 2000, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000X1028:EN:NOT>, (Eriřim Tarihi: 04 Aralık 2011).

⁶⁵ Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 13.12.2004, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:EN:NOT>, (Eriřim Tarihi: 04 Aralık 2011).

29 Aralık 2004 tarihli ve OJ L 385 sayılı Resmi Gazetede yayımlanarak 18 Ocak 2005 tarihinde yürürlüğe girmiştir. Avrupa Konseyi'nin EC 2252/2004 sayılı tüzüğünün 1. maddesinin 3. fıkrasına göre tüzük sadece üye ülkeler tarafından düzenlenen pasaport ve seyahat belgeleri için geçerlidir. Üye ülkelerin düzenledikleri kimlik kartı gibi diğer belgeler tüzük kapsamında değildir.

EC 2252/2004 tüzüğü ile pasaportlara eklenecek biyometrik özellikler yüz resmi veya parmak izi olarak belirlenmiştir. Bu düzenleme ile güvenliği artırma ve pasaportlardaki sahtecilikle daha etkin mücadele etme planlanmıştır. Pasaportlar veya seyahat dokümanlarının üzerinde biyometrik özelliklerin kaydedileceği ve karşılaştırmada kullanılacak yeterli kapasitede yüksek güvenli bir kayıt ünitesi bulunmalıdır. Kayıt ünitesi, Uluslararası Sivil Havacılık Örgütü (*International Civil Aviation Organization-ICAO*) tavsiyesine göre en az 32KB veya 64KB boyutunda, minimum PKI sayısal imza içeren veya yüz resmi ve parmak izini de içinde bulunduran bir bütünleşmiş devre (*chip*) olmalıdır. Kayıt ünitesi, kaydedilen biyometrik verilerin bütünlüğünü, gizliliğini ve orijinallliğini sağlamaktadır. Fiziksel engelli kişiler ve 12 yaşın altındaki çocuklar bu kararın getirdiği yükümlülükten muaf tutulmaktadır. Avrupa Konseyi'nin EC 2252/2004 tarihli tüzüğünün önemli bir başka maddesi biyometrik verilerin toplanma sebebidir (Hornung, 2007: 255). Yani, veriler makul sebepler için toplanmalıdır.

Komisyon, uluslararası standartlara uygun bir şekilde pasaport ve seyahat belgelerinin güvenliğini artırıcı ek özelliklerini 28 Şubat 2005 tarihinde C(2005)409 sayılı kararı ile belirlemiştir. Belirlenen ek özellikler, kayıt ünitesi ve güvenliği, yüz resmi ve parmak izi için kalite standardı ile sahtecilikle mücadele kapsamında alınan ek özelliklerdir.

Avrupa Birliği Komisyonu, pasaport veya seyahat belgesindeki ek güvenlik özellikleri ve biyometrik özellikler konularında kapsamlı bir karar (C (2006) 2909) yayınlamıştır ("*Commission Decision laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States*") (Frontex, 2011b: 17). Komisyonun bu kararında, pasaport veya seyahat belgesindeki güvenlik özellikleri ve biyometrik özellikleri ile ilgili detaylı teknik açıklamalarda bulunmaktadır. Örnek olarak;

- Birincil biyometrik, yüz resmi dir.
 - Yüz resmi önden çekilmiş olmalıdır.
 - Resim, JPEG (resim başına 12-20 KB) veya JPEG2000 (resim başına 6-10 KB) formatında olmalıdır.
- İkincil biyometrik, parmak izidir.
 - Standartlar: ICAO NTGW, *Biometrics Deployment of Machine Readable Travel Documents*, vb.
 - Sol ve sağ işaret parmağının parmak izi kullanılmalıdır.
 - Parmak izi başına 12-15 KB yer tutmalıdır.
- Kayıt ünitesi, RF-CHIP yapısında olmalıdır.
 - Kayıt ünitesinde, PKI (*Public Key Infrastructure*) sayısal imza ve biyometrik bilgiler bulunmalıdır.
- Elektronik pasaport devre yapısı
- Veri güvenliği ve bütünlük konuları
- Uyumluluk değerlendirmesi

Tüzüğe göre, her üye ülke, pasaport ve seyahat dokümanını düzenleyecek bir birim belirlemelidir ve bu birimi Komisyona bildirmelidir. Bu birimde sadece yetkili ve görevli kişiler biyometrik özelliklerin kaydedilmesi işlemlerini yapmalıdırlar.

EC 2252/2004 tüzüğü;

- Toplam 6 (altı) maddedir.
- Pasaport ve seyahat belgelerinin ortak bir formatta olmasını belirleyen 9303 sayılı ICAO kararına uyum aranmaktadır. Biyometrik özellikler için Uluslararası Sivil Havacılık Örgütü kurallarına uygunluk aranmaktadır.
- Kişisel verilerin korunması düzenlenmesini öngörmektedir.
- Üye ülkeler açısından Schengen Antlaşması ile uyumludur.

Avrupa Konseyi'nin EC 2252/2004 sayılı tüzüğünün 6. maddesine göre tüzüğün yürürlüğü, teknik özellikler belirlendikten 18 ay sonra pasaportlarda yüz resminin uygulanmasına ve 36 ay sonra parmak izinin uygulanmasına başlamaktadır. Pasaportlarda güvenlik artırıcı birinci grup ek teknik özellikler⁶⁶ Komisyon tarafından C (2005) 409 sayılı tebliğ ile 28 Şubat 2005 tarihinde kabul edilmiştir. Pasaportlarda, güvenlik artırıcı ikinci grup ek teknik özellikler⁶⁷ Komisyon tarafından C(2006) 2909 sayılı tebliğ ile 28 Haziran 2006 tarihinde kabul edilmiştir. Avrupa Konseyi'nin EC 2252/2004 sayılı tüzüğüne göre Komisyon tarafından ikinci grup teknik özelliklerin belirlendiği 28 Haziran 2006 tarihinden sonra, pasaportlarda biyometrik yüz resminin uygulanmasına (18 ay sonra) 28 Aralık 2007 tarihinde ve parmak izinin uygulanmasına (36 ay sonra) 28 Haziran 2009 tarihinde başlanması öngörülmüştür. Avrupa Birliği'nde 28 Haziran 2009'da başlayan biyometrik pasaportlar ile hem pasaport hem de pasaport sahibi doğrulaması yapılabilmektedir.⁶⁸

Uygulamada her ülke belirtilen tarihi beklememiştir. Örneğin, Almanya, yüz resminin bulunduğu RFID bütünleşmiş devresi eklenmiş şekildeki biyometrik pasaportları 2005 yılı sonlarına doğru uygulamaya koymuştur (Hornung, 2007: 247; Thomas, 2005: 378) Almanya biyometrik pasaportu Avrupa Birliği'nde uygulayan ilk ülkedir (JRC, 2008: 25).

13 Aralık 2004 tarihinde kabul edilen tüzüğün (EC 2252/2004) uygulaması esnasında bazı zorluklarla karşılaşmıştır. Pilot uygulamada ve testlerde bazı sorunlar çıkmıştır. Konsey, bu sıkıntıları aşmak üzere 18 Ekim 2007 tarihinde 13 Aralık 2004 tarihinde kabul edilen tüzüğün bazı maddelerini değiştiren iki (2) maddelik bir tüzük daha kabul etmiştir (EC 444/2009⁶⁹). Değişiklik yapan tüzük, Avrupa Konseyi'nde 28 Mayıs 2009 tarihinde kabul edilmiş ve 6 Haziran 2009 tarihinde OJ L142 sayılı Resmi Gazetede yayımlanmıştır.

⁶⁶ Technical specifications concerning facial images were adopted by Commission Decision C(2005)409 Commission on 28 February 2005.

⁶⁷ Integration of biometric features in passports and travel documents, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/114154_en.htm, (Erişim Tarihi: 04 Kasım 2011).

⁶⁸ New, secure biometric passports in the EU, strengthen security and data protection and facilitates travelling, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/872&type=HTML&aged=0&language=EN&guiLanguage=en>, (Erişim Tarihi: 20 Aralık 2011).

⁶⁹ Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009R0444:EN:NOT>, (Erişim Tarihi: 14 Aralık 2011).

Bu tüzük ile yapılan deęişikler; her bir kiřiye ayrı bir pasaport veya seyahat belgesinin düzenlenmesi ve 6 yařından küçük çocuklar ve fiziksel olarak parmak izi veremeyecek kiřilerden parmak izinin alınmayacağı řeklindeir. EC 2252/2004 sayılı tüzük ile pasaport ve seyahat belgelerindeki biyometrik özelliklerin sadece kayıt ünitelerinde tutulmasının öngöröldüğü, ölkelerin biyometrik özellikleri kendi ulusal veri tabanlarında tutmalarına bu tüzüğün dayanak oluřturmayacağı belirtilmektedir.

Pasaport ve seyahat belgelerindeki güvenlik ve biyometrik özelliklerin standartlarını belirleyen 13 Aralık 2004 tarihli ve EC 2252/2004 sayılı tüzüğü deęiřtiren 28 Mayıs 2008 tarihli ve EC 444/2009 sayılı tüzük; yüz resmi bakımından yürürlük tarihinden itibaren 18 ay sonra, parmak izi özellięi de yürürlük tarihinden itibaren 36 ay sonra uygulanmaya bařlamıřtır. EC 444/2009 sayılı tüzüğün yürürlük tarihi 28 Haziran 2009 tarihidir.

Avrupa Birlięi'nin 13 Aralık 2004 tarihli EC 2252/2004 sayılı tüzük ile yürürlüęe koyduęu pasaport ve seyahat belgelerine biyometrik özelliklerin eklenmesi düzenlemesini 28 Mayıs 2008 tarihli ve EC 444/2009 sayılı tüzüğü ile deęiřtirilmiřtir. Deęiřiklik yapan düzenleme ile birlikte yürürlük tarihleri uzatılmıřtır. EC 444/2009 sayılı tüzük ile yüz resmi özellięi ağıısından 28 Aralık 2011 ve parmak izi özellięi ağıısından 28 Mayıs 2013 tarihine kadar uzatılmıřtır.

Avrupa Birlięi'nde pasaport ve seyahat belgelerine biyometrik özelliklerin eklenmesi konusu, 2004 yılından beri gündemdedir. Birlik düzeyinde çeřitli düzenlemeler, Aralık 2004 tarihinden itibaren yapılmaktadır. Bununla birlikte, Vize Feragat Programı kapsamında bulunan ve Amerika Birleřik Devletleri'ne vizesiz seyahat etme hakkına sahip Avrupa Birlięi üye ölkelerine, Ekim 2006 tarihinden itibaren biyometrik pasaport sahibi olma zorunluluęu getirilmiřtir. Son olarak, Uluslararası Sivil Havacılık Örgütü'nün 9303 sayılı tavsiye kararı sonucu, örgüt üyesi olan ölkeler Nisan 2010 tarihinden itibaren makine tarafından otomatik olarak okunan seyahat belgesi düzenlemektedirler. Bütün bu gelişmeler paralelinde, Avrupa Birlięi üyesi ölkeler kendi vatandaşları için farklı tarihlerde biyometrik pasaport düzenlemeleri yapmıřlardır. Ařağıda tablo olarak, Avrupa Birlięi üyesi bazı ölkelerin, biyometrik pasaport uygulama tarihleri listelenmektedir. Tablo 3'de örnek verilen Avrupa Birlięi üyesi ölkelerin birinci nesil biyometrik pasaport uygulama

tarihleri 2005–2007 yılları arasında ve birinci nesil biyometrik pasaport uygulama tarihleri ise 2007–2010 yılları arasındadır.

AB Üyesi Bazı Ülkelerin Biyometrik Pasaport Uygulama Tarihleri

Ülke	Birinci Nesil Biyometrik Pasaport (Yüz Resmi)⁷⁰	İkinci Nesil Biyometrik Pasaport (Parmak İzi)⁷¹
Almanya	2005	2007
Avusturya	2006	2009
Belçika	2005	2007
Danimarka	2006	2009
Estonya	2007	2009
Finlandiya	2006	2009
Fransa	2006	2009
Hollanda	2005	2009
İngiltere	2006	2008
İspanya	2007	2009
İsveç	2006	2009
İtalya	2006	2010
Lüksemburg	2006	2009
Macaristan	2006	2009
Polonya	2006	2009
Romanya	2007	2010
Slovenya	2006	2009
Yunanistan	2007	2009

Tablo 3:AB Üyesi Bazı Ülkelerin Biyometrik Pasaport Uygulama Tarihleri⁷²

⁷⁰ Survey, 2004, ss.10-11.

⁷¹ Gellert ve Gutwirth, 2011: 37.

⁷² Survey, 2004, ss.10-11; Gellert ve Gutwirth, 2011: 37; JRC, 2008, ss.33-66.

3.3.1.2. AB Göç Yönetiminde Kurumsal Düzenlemeler

Biyometrik sistemlerin göç kontrol yönetiminde kullanılmasına bir başka örnek, Frontex isimli Bütünleşmiş Sınır Yönetimi Birimi'nin çalışmalarıdır. Avrupa Birliği'nin 2004 tarihli EC 2007/2004 sayılı bir tüzüğü ile Frontex (AB Bütünleşmiş Sınır Yönetimi Birimi- *European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union- Frontières extérieures for 'external borders'*) kurulmuştur.⁷³ Frontex, 3 Ekim 2005 tarihinde faaliyete başlamıştır. Frontex'in Genel Merkezi, Polonya'nın Varşova kentindedir. Frontex, sınır yönetimini daha iyi duruma getirmek için yeni yapılar (giriş-çıkış sistemi, *entry-exit system*, kayıtlı yolcular, *registered travellers*, biyometrik sistem kullanımı, *use of biometrics*, otomatik sınır geçişi, *automated border crossing*, vb.) geliştirmektedir.

Pasaport ve seyahat belgelerindeki biyometrik özellikler Avrupa Birliği'nde Vize Bilgi Sistemi'nde (*Visa Information System-VIS*) kaydedilmektedir. Komisyon, 22 Eylül 2006 tarihinde Vize Bilgi Sistemi ile ilgili biyometrik özelliklerin teknik standartlarına ilişkin bir karar kabul etmiştir.⁷⁴ Bu karar, Konseyin Vize Bilgi Sistemi'ni kuran 8 Haziran 2004 tarihli kararına ek olarak, vize bilgi sistemine biyometrik özelliklerin eklenmesini düzenlemiştir.⁷⁵ Avrupa Birliği üye devletlerin vatandaşlarına ait pasaport ve seyahat belgelerinde bulunan biyometrik özellikler Vize Bilgi Sistemi'ne 29 Haziran 2009 tarihinden itibaren kaydedilmeye başlanmıştır.⁷⁶ Biyometrik özellikler olarak resim ve parmak izi ifade edilmektedir.

Diğer taraftan, üçüncü ülke vatandaşlarının, Schengen vize bölgelerine biyometrik özelliklerin olduğu pasaportlarla seyahat etmelerine 2011 yılında başlanmıştır.⁷⁷ Kuzey Afrika ülkeleri Cezayir, Mısır, Libya, Moritanya, Fas ve Tunus vatandaşlarına, Avrupa Birliği'ne giriş yaparken biyometrik kontrol uygulaması Kasım 2011 tarihinde başlamıştır (Frontex, 2011c: 25). Resim 21'de, Avrupa Birliği sınır kapılarında üçüncü ülke vatandaşları için yapılan sınır kontrol işlemine örnek bulunmaktadır. Yapılan kontrollerde elde edilen biyometrik veriler, Vize Bilgi

⁷³ Council, EC 2007/2004.

⁷⁴ COM (2006) 3699.

⁷⁵ Council, EC 512/2004.

⁷⁶ COM(2008) 69.

⁷⁷ a.g.e.

Sistemi VIS'e kaydedilmektedir. Sınır kontrollerinde, parmak izi karşılaştırmasının 15–20 sn. içerisinde ve %5 hata payı ile yapılması beklenmektedir.



Resim 21: AB Sınır Kapısında Vize Kontrolü Uygulaması

Seyahat belgelerinde bulunan biyometrik veriler belge üzerinde bulunan bütünleşmiş devrelere ve Avrupa Birliği veri tabanı olan SIS II (*Schengen Information System*) bilgi sistemleri veri tabanına kaydedilmektedir (JRC, 2003: 123).

Sınır kontrollerinde, güvenlik için biyometrik sistemlerin kullanımıyla ilgili düzenlemeler yapılırken bu tür sistemlerin tahmini kurulum maliyetleri konusunda da çalışmalar yapılmaktadır. Komisyonun, 13 Şubat 2008 tarihli ve “Avrupa Birliği Sınır Yönetiminde Geleceğe Yönelik Adımlar ile İlgili Hazırlık” isimli bildirisinde, merkezi giriş-çıkış sisteminin ve kayıtlı yolcu programının (*registered traveler program*) 2–3 yıl içinde 20 milyon avroya kurulabileceği ve yıllık ortalama 6 milyon avro bakım masrafının olacağı tahmin edilmektedir.⁷⁸ Bir otomatik geçiş kapısı da yaklaşık 35 bin avroya kurulmaktadır.

Avrupa Birliği, göç kontrol mekanizmasında biyometri kullanımına önderlik etme bakımından Amerika Birleşik Devletleri'nden sonra hemen ön sıralarda bulunmaktadır. Amerika Birleşik Devletleri'nin Vize Feragat Programı'nın⁷⁹ (*The Visa Waiver Program-VWP*) getirdiği pasaport ve seyahat belgelerine biyometrik özelliklerin eklenmesi gibi yükümlülükler Avrupa Birliği tarafından da uygulamaya konmuştur.

⁷⁸ COM(2008) 69, s.52.

⁷⁹ ABD'ye turizm veya iş amacıyla 90 gün veya daha az süre kalmak üzere giden kişilere uygulanan bir vize programıdır (http://travel.state.gov/visa/temp/without/without_1990.html, (Erişim Tarihi: 05 Aralık 2011)).

3.3.1.3. Avrupa Birliği'nin ABD ile Yolcu Bilgilerini Paylaşması

Avrupa Birliği'nin göç yönetimi konusunda Amerika Birleşik Devletleri ile işbirliği yaptığı bir başka konu terörizmle daha etkin mücadele edebilmek amacıyla yolcu bilgilerinin (*Passanger Name Record - PNR*) paylaşılmasıdır.⁸⁰ Yolcu bilgileri, havayolu seyahati ile ilgili uçuş tarihi, bilet numarası, havayolu şirketi, ödeme, koltuk numarası ve uçuşta tercih edilen yemek bilgisi gibi çeşitli bilgileri içermektedir.⁸¹

Avrupa Birliği Konseyi, 17 Mayıs 2004 tarihli ve 2004/96/EC⁸² sayılı kararı ile Avrupa Birliği havayolu şirketlerinin, Amerika Birleşik Devletleri yetkilileri ile yolcu bilgilerinin paylaşılmasını öngören anlaşmayı kabul etmiştir. Bu karar, Avrupa kamuoyunda kişisel verilerin korunması anlamında bazı tartışmalara sebep olmuştur.⁸³ Bununla birlikte, Avrupa Parlamentosu, bu kararın iptal edilmesi için 9 Temmuz 2004 tarihinde Avrupa Adalet Divanı'na başvurmuştur (Özcan ve Yılmaz, 2007: 109). Kamuoyundaki tartışmalar sonucu 95/46/AT sayılı Kişisel Verilerin Korunması yönergesine göre kurulan Çalışma Grubu, varılan anlaşmada yolcu bilgilerinden 34 farklı başlığın⁸⁴ Amerika Birleşik Devletleri'ne transfer edilmesinin yerine terörizmle mücadele kapsamında daha ilgili olan 19 başlığın Amerika Birleşik Devletleri'ne transfer edilmesinin daha uygun olduğunu değerlendirmiştir.⁸⁵

Avrupa Adalet Divanı, ölçülülük ilkesi ile bağdaşmayan taleplerin yolcu bilgileri kapsamında talep edildiğini kabul ederek 30 Mayıs 2006 tarihinde verdiği kararı ile Komisyonun yaptığı anlaşmayı iptal etmiştir (Özcan ve Yılmaz, 2007: 112). Avrupa Adalet Divanı'nın kararına göre, 90 gün içerisinde Avrupa Birliği ve Amerika Birleşik Devletleri'nin yolcu bilgilerinin transferi konusunda yaptıkları anlaşmayı iptal etmeleri gerekmektedir. İki taraf, Adalet Divanı kararından sonra

⁸⁰ http://epic.org/privacy/intl/passenger_data.html, (Erişim Tarihi: 25 Aralık 2011) .

⁸¹ <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/60>, (Erişim Tarihi: 25 Aralık 2011).

⁸² <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0496:EN:HTML>, (Erişim Tarihi: 10 Aralık 2011).

⁸³ Europarl debate on PNR and data retention, <http://www.edri.org/edriagram/number3.5/retention>, (Erişim Tarihi: 18 Aralık 2011) .

⁸⁴ http://www.dhs.gov/xnews/releases/press_release_0421.shtm, (Erişim Tarihi: 15 Aralık 2011).

⁸⁵ Opinion of the European Data Protection Supervisor, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-12-09_US_PNR_EN.pdf, (Erişim Tarihi: 18 Aralık 2011).

yaptıkları anlaşmayı iptal edip, 31 Temmuz 2007 tarihine kadar yürürlükte kalan geçici dönem anlaşmasını 16 Kasım 2006 tarihinde imzalamışlardır.⁸⁶

Yolcu bilgilerinin üçüncü ülkelerle paylaşılması konusunda, Avrupa Birliği düzeyinde teklif edilen son düzenleme, 23 Kasım 2011 tarihinde⁸⁷ Avrupa Konseyine sunulan “Yolcu Bilgilerinin Amerika Birleşik Devletleri İç Güvenlik Örgütü’ne Transfer Edilmesi konusunda Avrupa Birliği ve Amerika Birleşik Devletleri Arasında Yapılan Anlaşma’nın Sonucu” isimli tebliğdir (COM (2011) 807 *final*). Bu tebliğ, 19 Nisan 2012 tarihinde, Avrupa Parlamentosu’nda onaylanarak kabul edilmiştir⁸⁸.

Avrupa Birliği düzeyinde kabul edilen bir başka düzenleme ise, 22 Kasım 2010 tarihinde Komisyon tarafından kabul edilen “Avrupa Birliği İç Güvenlik Stratejisi”⁸⁹ dir. Avrupa Birliği İç Güvenlik Stratejisi, Stockholm Programı kapsamında, birliği tehdit eden en önemli sorunlarla mücadele aşamalarını belirlemektedir. Strateji belgesi, vatandaşların ve kurumların terör şebekelerine karşı korunması için sınır güvenliğinin artırılması bir tanesi olmak üzere toplam beş başlıkta alınacak önlemleri ve yapılacak hazırlıkları düzenlemektedir.

3.3.2. Amerika Birleşik Devletleri Uygulaması

Amerika Birleşik Devletleri’nde göç ve sınır güvenliğinin sağlanması Amerika Birleşik Devletleri İç Güvenlik Örgütü’nün US-VISIT programı (*United States Visitor and Immigrant Status Indicator Technology-US-VISIT*) ile yapılmaktadır.⁹⁰ Program uygulamasında, Amerika Birleşik Devletleri’ne giriş yapan kişilere, yüz

⁸⁶ <http://www.statewatch.org/news/2006/oct/eu-usa-pnr-press-release.pdf>, (Erişim Tarihi: 02 Ocak 2012).

⁸⁷ COUNCIL DECISION on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, 23 Kasım 2011, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:DKEY=627802:EN:NOT>, (Erişim Tarihi: 06 Ocak 2012).

⁸⁸ AP’den yolcu bilgilerinin ABD ile paylaşılmasına onay, <http://www.euractiv.com.tr/abnin-gelecegi/article/avrupa-birligi-yolcu-bilgilerini-abd-ile-paylasacak-025112>, (Erişim Tarihi: 20 Nisan 2012).

⁸⁹ Commission presents a new set of EU measures to better protect European citizens, 22 Kasım 2010, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1535&format=HTML&aged=0&language=EN&guiLanguage=fr>, (Erişim Tarihi: 06 Ocak 2012).

⁹⁰ http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm (Erişim Tarihi: 06 Ocak 2012).

resmi ve parmak izi biyometrik tanımlayıcıları ile sınır kontrol işlemleri yapılmaktadır.

Amerika Birleşik Devletleri'nde göç ve sınır güvenliği için toplanan biyometrik bilgiler US-VISIT programı kapsamında koordine edilmektedir. Programın başlangıç tarihi olan 31 Aralık 2003 tarihinden itibaren, sadece vize sahibi kişiler US-VISIT programına dâhil iken, 26 Ekim 2006 tarihinden sonra ABD Vize Feragat Programı'na dâhil kişiler de US-VISIT programı kapsamına alınmıştır. Bununla birlikte, Amerika Birleşik Devletleri Dışişleri Bakanlığı, kendi vatandaşlarına 2006 yılından itibaren biyometrik pasaport vermeye başlamıştır.⁹¹

3.3.2.1. ABD Ziyaretçi ve Göçmen Statüsünü Gösterge Teknolojisi Programı (The United States Visitor and Immigrant Status Indicator Technology-US-VISIT)

Amerika Birleşik Devletleri'nde İç Güvenlik Örgütü'nün (*Department of Homeland Security-DHS*) Ziyaretçi ve Göçmen Statüsünü Gösterge Teknolojisi Programı olan US-VISIT programı (*The United States Visitor and Immigrant Status Indicator Technology-US-VISIT*) 5 Ocak 2004 tarihinde uygulamaya konmuştur (Subcommittee on Biometrics, 2008: 30). Göç kontrol mekanizmasında kullanılan biyometrik bilgiler konusunda önemli bir başlangıç olan US-VISIT programının 31 Aralık 2003 tarihinde başlaması öngörülmüştür. Fakat yılbaşı tatil yoğunluğu geçtikten hemen sonra 5 Ocak 2004 tarihinde uygulama başlanmıştır (Subcommittee on Biometrics, 2008: 30).

⁹¹ a.g.e.



Resim 22: US-VISIT Programı Açılış Resmi⁹²

Bu program 1996 yılı Yasadışı Göç Reformu ve Göçmen Sorumluluğu Kanunu (*Illegal Immigration Reform and Immigrant Responsibility Act*), 2000 yılı Göçmenlik ve Vatandaşlık Servisi Veri Yönetimi İyileştirme Kanunu (*The Immigration and Naturalization Service Data Management Improvement Act*), 2001 yılı Vatanseverlik Kanunu (*The USA PATRIOT Act*) ve 2002 yılı Sınır Güvenliğinin Artırılması ve Vize Reform Kanunu'na (*The Enhanced Border Security and Visa Entry Reform Act*) dayanarak uygulanmaktadır.

US-VISIT programının amacı Amerika Birleşik Devletleri'nin güvenliğini artırırken yasal göçmen ve tüccarların işlemlerinin kolaylaştırılmasıdır (Redpath, 2005: 9). Amerika Birleşik Devletleri Dışişleri Bakanlığı 26 Ekim 2004 tarihinden itibaren diğer ülkelerdeki bütün büyükelçiliklerinde (207 adet) göçmen olmayan vize başvurularında, başvuranların parmak izlerini ve sayısal fotoğraflarını Otomatik Biyometrik Tanımlama sistemleri ile almaya başlamıştır (Redpath, 2007: 30).⁹³ US-VISIT programı kapsamında sadece 14 yaşın altındaki çocuklar ve 79 yaşın üstündeki yaşlılar kapsam dışında tutulmuştur (Liu, 2011: 39). Avrupa Birliği ile Amerika Birleşik Devletleri uygulamalarında, kıyaslama yapıldığında görülmektedir ki; Amerika Birleşik Devletleri uygulamasında hem 14 yaş altı hem de 79 yaş üstü kapsam dışında tutulurken, Avrupa Birliği uygulamasında sadece 12 yaş altı çocukların parmak izi alınmamaktadır. Diğer taraftan, Avrupa Birliği uygulamasında

⁹² Subcommittee on Biometrics, 2008: 30.

⁹³ Section 303 of the Enhanced Border Security and Visa Entry Reform Act of 2002, (Erişim Tarihi: 06 Ocak 2012).

fiziksel özürlü kişiler biyometrik sistem uygulaması dışında tutulabilirken, Amerika Birleşik Devletleri uygulamasında, fiziksel özürlü olan kişiler kapsam dışına alınmamaktadır.

Amerika Birleşik Devletleri Dışişleri Bakanlığı büyükelçilik ve konsolosluklarında, Amerika Birleşik Devletleri'ne seyahat etmek isteyen ziyaretçilerden parmak izi ve yüz resmi gibi biyometrik bilgiler alınmaktadır. Alınan biyometrik bilgiler, ziyaretçi kişiler Amerika Birleşik Devletleri'ne giriş yaparken, sınır kapılarında sınır görevlileri tarafından kontrol edilmektedir (Subcommittee on Biometrics, 2008: 17).

Amerika Birleşik Devletleri Ulusal Bilim ve Teknoloji Konseyi'nin (*National Science and Technology Council-NSTC*) biyometri konusundaki alt çalışma komisyonu, 2001 ile 2008 yılları arasındaki göç yönetiminde kullanılan biyometri uygulamaları konusunda kapsamlı bir rapor hazırlamıştır. Rapor, "*Privacy and Biometrics: Building a Conceptual Foundation*" ismiyle yayınlanmıştır (Subcommittee on Biometrics, 2008: 1). Ağustos 2008 tarihinde yayımlanan bu raporda, Amerika Birleşik Devletleri'ne giriş yapan ziyaretçi kişilerin US-VISIT programı kapsamında biyometrik bilgilerinin nasıl alındığı aşağıdaki resim ile gösterilmektedir.



Resim 23: ABD Sınır Kapısında Vize Kontrolü Uygulaması
(US-VISIT Programı Kapsamında Biyometrik Bilgilerin Kontrol Edilmesi)⁹⁴

⁹⁴ Subcommittee on Biometrics, 2008: 17.

3.3.2.2. ABD Vize Feragat Programı (Visa Waiver Program-VWP)

Amerika Birleşik Devletleri Vize Feragat Programı (*The Visa Waiver Program-VWP*), Amerika Birleşik Devletleri'ne turizm veya iş amacıyla 90 gün veya daha az süre kalmak üzere gelen kişilere uygulanan bir vize programıdır (B tipi ziyaretçi vizesi).⁹⁵ Bu program, turizm endüstrisine destek olmak ve iş veya ticaret amaçlı yapılan seyahatleri kolaylaştırmak üzere 1986 yılında başlamıştır. Her ülke Vize Feragat Programı'na dâhil değildir. Amerika Birleşik Devletleri Vize Feragat Programı'na (VWP), 2010 yılı itibarıyla 36 ülke üyedir (Monger, 2011: 2). Avrupa Birliği üye ülkelerinden, Bulgaristan, Kıbrıs, Polonya ve Romanya haricindeki bütün ülkeler Vize Feragat Programı'na üyedirler.⁹⁶ Bu programa dâhil olan ülkelerin vatandaşları vize almak zorunda değildirler.

Sınır Güvenliğinin Artırılması ve Vize Reform Yasası (*Enhanced Border and Visa Reform Act*) 303(c) maddesine göre Vize Feragat Programına dâhil olan ülkelerin vatandaşlarının seyahat belgeleri makine tarafından okunabilen formatta olması, biyometrik özellikler eklenmiş olması ve ICAO standartlarına uygun olması gerekmektedir (Hornung, 2007: 252).

Vize Feragat Programına dâhil olan ülke vatandaşlarının seyahat belgelerinde biyometrik özelliklerin bulundurulması en son 26 Ekim 2006 tarihine ertelenmiştir. İlk olarak 26 Ekim 2004 tarihi sonradan bir yıl ertelenerek 26 Ekim 2005 tarihi ve en son bir yıl daha ertelenerek 26 Ekim 2006 tarihi son tarih olarak belirlenmiştir (Hornung, 2007: 252).

3.3.2.3. Elektronik Seyahat Yetkilendirmesi (The Electronic System for Travel Authorization-ESTA)

Amerika Birleşik Devletleri Vize Feragat Programı'ndan (*The Visa Waiver Program-VWP*) yararlanmak isteyen kişiler, 12 Ocak 2009 tarihinden itibaren Elektronik Seyahat Yetkilendirmesi'ne (*Electronic System for Travel Authorization-ESTA*) başvurup bir e-pasaport almak zorundadırlar (Monger, 2011: 2). Elektronik Seyahat Yetkilendirmesi (*ESTA*), dönemin Amerika Birleşik Devletleri Başkanı George W.

⁹⁵ http://travel.state.gov/visa/temp/without/without_1990.html#vwp (Erişim Tarihi: 06 Ocak 2012).

⁹⁶ a.g.e.

Bush tarafından 3 Ağustos 2007 tarihinde imzalanan 9/11 Komisyonunun Tavsiyelerinin Uygulanması Kanunu (*Implementing Recommendations of the 9/11 Commission Act of 2007*) ile kurulmuştur. ESTA, Amerika Birleşik Devletleri İç Güvenlik Örgütü tarafından yürütülmektedir.

Avrupa Birliği ile Amerika Birleşik Devletleri arasında yapılan toplantılar sonucu, Avrupa Birliği üyesi ülkelerin hepsinin (VWP'a üye olanlar da dâhil olmak üzere) vatandaşlarının, 10 parmak izinin alındığı biyometrik bilgileri vermek, *ESTA*'dan bir e-pasaport almak ve diğer havayolu güvenlik şartlarına (bagaj, vb.) uymak zorunda olmaları kararlaştırılmıştır. VWP'ına üye bütün yolcular, yaş ve pasaport türlerine bakılmaksızın makine tarafından otomatik olarak okunabilen pasaport taşımak zorundadırlar. İlave olarak, Çek Cumhuriyeti, Estonya, Macaristan, Letonya, Litvanya, Malta, Kore Cumhuriyeti ve Slovak Cumhuriyeti ülkelerinin vatandaşları bütünleşmiş devre içeren bir e-pasaporta sahip olmak zorundadırlar.

3.3.3. AB ve ABD Uygulamalarının Değerlendirilmesi

Avrupa Konseyi'nin EC 2252/2004 sayılı tüzüğe göre Komisyon tarafından ikinci grup teknik özelliklerin belirlendiği 28 Haziran 2006 tarihinden sonra pasaportlarda biyometrik yüz resminin uygulanmasına (18 ay sonra) 28 Aralık 2007 tarihinde ve parmak izinin uygulanmasına (36 ay sonra) 28 Haziran 2009 tarihinde başlanması öngörülmüştür.

Avrupa Birliği'nin 13 Aralık 2004 tarihinde EC 2252/2004 sayılı tüzüğü ile yürürlüğe koyduğu pasaport ve seyahat belgelerine biyometrik özelliklerin eklenmesi düzenlemesini değiştiren, 28 Mayıs 2008 tarihli ve EC 444/2009 sayılı tüzüğü ile pasaportlara biyometrik yüz resmi özelliğinin eklenmesi 28 Aralık 2011 tarihine ve pasaportlara parmak izi özelliğinin eklenmesi 28 Mayıs 2013 tarihine kadar uzatılmıştır.

Diğer yandan, Amerika Birleşik Devletleri Vize Feragat Programına dâhil olan Avrupalı kişilerin Amerika Birleşik Devletleri'ne biyometrik pasaport ile giriş tarihi uzatılarak 26 Ekim 2006 tarihine ertelenmiştir. Uygulama için ilk olarak 26 Ekim 2004 tarihi belirlenmiş olsa da iki defa uzatılarak 26 Ekim 2006 tarihi Amerika Birleşik Devletleri Vize Feragat Programının başlangıç tarihi olmuştur.

Bütün bu düzenlemeler ve sınır güvenliğine ilişkin endişeler sonucu Avrupa Birliği üyesi ülkeler 2006 yılından itibaren biyometrik pasaport uygulamasını başlatmıştır. Bazı ülkeler 2006 yılı öncesinde biyometrik pasaport uygulamasını kendi vatandaşları için başlatmıştır. İlave olarak, üçüncü ülke vatandaşları, Schengen vize bölgelerine biyometrik özelliklerin olduğu pasaportlarla seyahat etmelerine 2011 yılında başlamışlardır.⁹⁷

Avrupa Birliği Konseyi tarafından pasaport ve seyahat belgelerinde biyometrik bilgilerin bulundurulmasına ilişkin alınan karar bazı tartışmalara sebep olmuştur. Kısaca, özellikle kişisel verilerin korunması başta olmak üzere, üye ülkelerin parlamentolarının sürece katılım sağlamamaları, ulusal biyometri veri tabanının bulunup bulunmayacağı ve karar öncesinde kamuoyunda yeterli tartışmanın yapılmamış olması biyometri konusunda alınan kararın eleştirilere muhatap olmasına sebep olmuştur (Hornung, 2007: 252). Diğer yandan, bazı uzmanlar, Avrupa Birliği'nin sınır kontrol uygulamalarının genel olarak bir değerlendirmesinin yapılmasını ve etkinlik analizini önermektedirler (Carrera, 2011: 21).

Avrupa Birliği Konseyi tarafından kabul edilen pasaport ve seyahat belgelerinde biyometrik bilgilerin bulundurulmasına ilişkin EC 2252/2004 sayılı tüzükte net olarak belirlenmeyen hususlardan biri, biyometrik verilerin kaydedilip kaydedilemeyeceğidir. Komisyon tarafından 2004 yılında Parlamente'ye sunulan kararda biyometrik verilerin kaydedilmesi konusu varken (COM 2004(116), *Official Journal* C 98 23 Nisan 2004, 39), Avrupa Parlamentosu, biyometrik verilerin kaydedilmesine ilişkin hükmü⁹⁸ kabul etmemiştir (Hornung, 2007: 252).

Avrupa Konseyi'nin EC 2252/2004 tarihli tüzüğünde net olmayan bir başka husus da üye ülkelerin biyometrik özellikleri muhafaza etmek üzere ulusal düzeyde bir veri tabanı kurup kuramayacaklarıdır. Tüzük, bu konuda kararı üye ülkelere bırakmıştır. Üye ülkeler, biyometrik pasaportlarda kıyaslama yapabilmek için biyometrik verilere ihtiyaç duymaktadırlar. Bu ihtiyacı karşılamak üzere ulusal düzeyde bir veri tabanı kurulabilir. Fakat biyometrik özellikleri içeren bir veri tabanı

⁹⁷ COM(2008) 69.

⁹⁸ European Parliament legislative resolution on the proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 – C5-0101/2004 – 2004/0039 (CNS)), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2004-0073+0+DOC+XML+V0//EN>, (Erişim Tarihi; 01 Şubat 2011).

başka amaçlarla da kullanılabileceğinden, kişiler bir anlamda takibe imkân tanıyan bu tür sistemlere şüphe ile yaklaşmaktadırlar.

Amerika Birleşik Devletleri Dışişleri Bakanlığı 26 Ekim 2004 tarihinden itibaren diğer ülkelerdeki bütün büyükelçiliklerinde göçmen olmayan vize başvurularında, başvuranların parmak izlerini ve sayısal fotoğraflarını DHS Otomatik Biyometrik Tanımlama sistemleri ile almaya başlamıştır. Sınır güvenliğinin artırılması adına Amerika Birleşik Devletleri'nde yapılan önemli bir değişiklik US-VISIT programının devreye alınmasıdır. US-VISIT programı kapsamında ülkeye giriş yapan kişilere 2004 yılından beri biyografik bilgiler ve biyometrik tanımlayıcılar kullanılarak sınır kontrol işlemleri yapılmaktadır. 26 Ekim 2006 tarihinden itibaren Vize Feragat Programına dâhil kişiler de US-VISIT programı kapsamına alınmıştır.

3.3.4. Türkiye Uygulaması

Türkiye'nin, Avrupa Birliği ile iltica ve göç konusunda yürüttüğü mevzuat uyum çalışmaları geri kabul anlaşması (Hürriyet, 2010: 1), sınır güvenliği ve biyometrik pasaport⁹⁹ konularıdır. Türkiye Avrupa Birliği geri kabul anlaşması müzakereleri 2012 yılı itibariyle tamamlanmış olmakla birlikte, anlaşma henüz imzalanmamıştır.¹⁰⁰

Vize politikası alanında biyometrik güvenlik özellikleri olan pasaportların dağıtımına 1 Haziran 2010 tarihinde başlanmıştır. İlaveten, yüksek güvenlikli yeni Türk vize bandrolleri 2011 yılında Merkez Bankası tarafından basılmıştır.¹⁰¹

Dış Sınırlar konusunda Bütünleşmiş Sınır Yönetimi Koordinasyon Kurulu kurulmuş, Bütünleşmiş Sınır Yönetimi Yol Haritası ve Kurumlar Arası İşbirliği Protokolü hazırlanmıştır. Bütünleşmiş Sınır Yönetimi'ne ilişkin eğitim faaliyetleri gerçekleştirilmiştir.¹⁰²

⁹⁹ Geri Kabul Anlaşması: Ama Neyin Karşılığında?, Mehmet Özcan, 17.03.2010, <http://www.usak.org.tr/makale.asp?id=1390>, (Erişim Tarihi: 18 Aralık 2011).

¹⁰⁰ 2011 Yılı AB İlerleme Raporu, s.90.

¹⁰¹ a.g.e., s.91.

¹⁰² a.g.e., s.92.

Sınır güvenliğinin sağlanması için, altyapının güçlendirilmesi ve özellikle video gözetleme kameraları ve diğer sistemler gibi ekipmanların daha yaygın kullanımı sağlanmaktadır.¹⁰³

Bu çalışmada, biyometrik pasaport konuları tartışılmaktadır. On bir Eylül 2001 terör olayından sonra Amerika Birleşik Devletleri başta olmak üzere Avrupa Birliği ülkeleri ve daha birçok ülkede yürütülen biyometrik pasaport çalışmalarından Türkiye de etkilenmiştir.

Türkiye, üye olduğu Uluslararası Sivil Havacılık Örgütü'nün¹⁰⁴ tavsiyelerine göre en geç 1 Nisan 2010'da biyometrik pasaporta geçme taahhüdünde bulunmuştur (Tanış, 2012; Uçan, 2010: 2).¹⁰⁵ Uluslararası Sivil Havacılık Anlaşması olan Şikago Sözleşmesi'ne ülkemiz 1945 yılında taraf olmuş ve ICAO'nun kurucu üyeleri arasında yer almıştır.¹⁰⁶ Birleşmiş Milletlere bağlı bir uzmanlık örgütü olan ICAO, 1947 yılından itibaren uçuş emniyeti ve uçuş güvenliğine ilişkin uluslararası sivil havacılık alanında küresel ölçekte kurallar ve politikalar geliştirmektedir.¹⁰⁷

Vize alması gerekmeyen üçüncü ülke vatandaşlarının biyometrik özelliklerin olduğu pasaportlarla Schengen vize bölgelerine kayıtlı yolcu olarak girebilmeleri COM(2008) 69 sayılı tebliğ¹⁰⁸ ile düzenlenmiştir. Bu düzenleme 2011 yılında uygulanmaya başlamıştır.

5682 sayılı Pasaport Kanunu'nun "Pasaport veya Pasaport Yerine Geçerli Vesika Zorunluluğu" başlıklı 2. maddesine göre, Türk vatandaşları ve Türkiye'ye giren veya çıkan yabancı kişiler, giriş-çıkış kapılarındaki polis görevlilerine pasaport veya yerine geçen bir seyahat belgesi ibraz etme zorunluluğu bulunmaktadır.

¹⁰³ a.g.e., s.92.

¹⁰⁴ Uluslararası Sivil Havacılık Örgütü Web Sayfası, <http://www.icao.int/>, (Erişim Tarihi, 10 Ekim 2011) <http://icao.pr.mfa.gov.tr/ShowInfoNotes.aspx?ID=121386>.

¹⁰⁵ Biyometrik pasaportlar geliyor, ama. İbrahim Doğan. Sayı: 794 / Tarih: 22.02.2010. <http://www.aksyon.com.tr/aksyon/haber-26163-200-biyometrik-pasaportlar-geliyor-ama.html>, (Erişim Tarihi: 28 Aralık 2011).

¹⁰⁶ Tarihçe, <http://web.shgm.gov.tr/kurumsal.php?page=tarihce>, (Erişim Tarihi: 28 Aralık 2011).

¹⁰⁷ Uluslararası Sivil Havacılık Örgütü (ICAO)'nın faaliyet alanı ve işlevi, <http://icao.pr.mfa.gov.tr/ShowInfoNotes.aspx?ID=121386>, (Erişim Tarihi: 28 Aralık 2011).

¹⁰⁸ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Preparing the next steps in border management in the European Union, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008DC0069:EN:NOT>, (Erişim Tarihi: 10 Aralık 2011).

Türkiye’de elektronik pasaport uygulamasına ilişkin mevcut durum hakkında bilgi temin etmek üzere Emniyet Genel Müdürlüğü Pasaport Daire Başkanı Sn. Metin Tanış ile 28 Mart 2012 tarihinde bir görüşme yapılmıştır.

Türkiye Cumhuriyeti İçişleri Bakanlığı tarafından Avrupa Birliği müzakere süreci kapsamında tasarlanan yeni elektronik Türk pasaportlarının dağıtımına 1 Haziran 2010 tarihinde başlanmıştır.¹⁰⁹ Türkiye’de 1 Haziran 2010 tarihinde başlayan uygulama Uluslararası Sivil Havacılık Örgütü’nün 9303 sayılı dokümanında belirlenen standartlara uygun şekilde makine tarafından okunabilir elektronik pasaport şeklindedir (Tanış, 2012).

Elektronik pasaportlarda eski pasaportlardan farklı olarak kimlik sayfasının alt tarafında özel cihazlarla otomatik olarak okunabilen 44 karakterden oluşan bir alan bulunmaktadır (Vakalis, 2011: 485). Bu bölgede pasaport sahibinin kimlik bilgileri bulunmaktadır. Elektronik pasaportlardaki kimlik bilgileri sınır kontrol işlemlerini yürüten mercilerce, kolay ve hızlı bir şekilde tespit edilip kontrol edilebilmektedir.

Yeni düzenlenen elektronik Türk pasaportlarında, biyometrik bilgi olan parmak izi özellikleri bulunmamaktadır (Tanış, 2012). Biyometrik bilgiler yeni pasaportlarda olmadığından dolayı bu yeni pasaportlar tam olarak biyometrik pasaport olarak değerlendirilememektedir. Yeni düzenlenen elektronik pasaportlar Uluslararası Sivil Havacılık Örgütü’nün 9303 sayılı belgesi standartlarına göre makine tarafından otomatik olarak okunabilen ve içindeki bütünleşmiş devrede Türk pasaportu olduğunu belirten elektronik sertifika mevcut bulunan bir elektronik pasaporttur (Tanış, 2012).

Tanış (2012) Türkiye’de 1 Haziran 2010 tarihinden itibaren verilen elektronik pasaportların üç avantajından bahsetmektedir. Bunlar: işlemlerin hızlandırılması, sahteciliğe önlem ve vize alma kolaylığıdır (Tanış, 2012). Elektronik pasaportların tüm dünyada kullanılmaya başlanması, Türk vatandaşlarının ziyaret ettikleri ülkelerdeki sınırlarda pasaport kontrol işlemlerini hızlandırmıştır. Bununla birlikte sahteciliğe karşı daha güvenli olmuştur. Elektronik pasaport kullanımının vize

¹⁰⁹ E-pasaport Bilgi ve Randevu Merkezi, <http://www.epasaport.gov.tr/>, (Erişim Tarihi: 10 Aralık 2011).

alma kolaylığı sağlaması ve Avrupa Birliği aday ülkesi olarak mevzuat uyum çalışmaları sebebiyle elektronik pasaport uygulaması başlamıştır (Tanış, 2012).

Yeni elektronik pasaport başvuruları Emniyet Müdürlüklerinin Pasaport Şube Müdürlükleri'nde yapılmakta ve kalan bütün işlemler Ankara/Gölbaşı'nda bulunan Emniyet Genel Müdürlüğü Pasaport Daire Başkanlığı'nda yürütülmektedir. Yeni sistemde düzenlenen elektronik pasaportlar vatandaşlara posta yoluyla ulaştırılmaktadır.

Yeni elektronik pasaport başvurusu yapan her vatandaş bu işlem esnasında on parmağının birden parmak izi kaydını vermektedir. Vatandaşlar bu işlemin elektronik pasaport uygulamasının bir parçası ve zorunlu olduğunu düşünmektedirler. Elektronik pasaport başvurusu esnasında on parmağın birden parmak izinin alınması işlemi elektronik pasaport için değildir (Tanış, 2012). Diğer taraftan Emniyet Genel Müdürlüğü Pasaport Daire Başkanı'nın da ifade ettiği gibi, elektronik pasaport alırken bütün parmakların parmak izi Emniyet Genel Müdürlüğü personeli tarafından alınıp sisteme tanıtılmakta ve bu veriler Emniyet Genel Müdürlüğü sistemlerine aktarılmaktadır. Aktarılan bu bilgiler 2012 yılı Mart ayı itibariyle elektronik pasaport için kullanılmamaktadır.

1 Haziran 2010 tarihli elektronik pasaport uygulamasından sonra Türk sınır kapılarında klasik yöntemlerle sınır kontrol işlemleri yapan alternatif bir yöntem mevcuttur. Mevcut bulunan bu alternatif yöntem, sınır görevlilerince pasaportlardaki bilgilerin elle sistemlere kaydedilmesi ve kontrol edilmesi şeklinde yürütülmektedir.

Pasaport kullanımı ile ilgili düzenlemeleri yapan Uluslararası Sivil Havacılık Örgütü'nün tavsiye kararlarına göre, Türkiye'de biyometrik olmayan eski pasaportların 2012 yılı itibariyle temdit işlemleri yapılmamakta ve eski pasaportlar ise 2015 yılı Kasım ayına kadar geçerlidir.¹¹⁰ 1 Haziran 2010 tarihinden itibaren pasaport başvurusu yapan bütün vatandaşlara yeni elektronik pasaport verilmektedir.

Elektronik pasaportların 2012 yılı Mart ayı itibariyle cüzdan bedeli, 62,50 TL'dir. Ayrıca umumi, hususi ve hizmet gibi pasaport türlerine göre pasaport cüzdan bedeline ilaveten çeşitli miktarlarda pasaport harç bedelleri ödenmektedir. Elektronik

¹¹⁰ Budak, Bülent, 2010, Ve Türkiye Biyometrik Pasaport Dönemini Başlattı, 01 Haziran 2010, <http://www.hessentoplum.com/Haberler/339.html>, (Erişim Tarihi: 10 Aralık 2011).

pasaport konusunda bilgi temin etmek ve randevuları koordine etmek üzere EPasaport (<http://www.epasaport.gov.tr/>) web portalı hizmet vermektedir.

Sn. Tanış'tan alınan bilgilere göre Mart 2012 tarihi itibariyle Türkiye'de pasaport türleri ve geçerli pasaportların sayılarına ilişkin bilgi Tablo 4'de sunulmaktadır.

Türkiye'de Geçerli Pasaport Sayısı

Umumi Eski Pasaport Sayısı	552.070	Umumi E-Pasaport Sayısı	3.464.156
Hususi Eski Pasaport Sayısı	442.774	Hususi E-Pasaport Sayısı	1.387.486
Hizmet Eski Pasaport Sayısı	998.028	Hizmet E-Pasaport Sayısı	3.464.156
Toplam Eski Pasaport Sayısı	998.028	Toplam E-Pasaport Sayısı	4.100.830

Tablo 4: Türkiye'de 06 Mart 2012 Tarihi İtibariyle Mevcut Geçerli Pasaport Sayısı

Özetle, 6 Mart 2012 tarihi itibariyle Türkiye'de geçerli toplam eski pasaport sayısı 998.028 iken aynı tarih itibariyle geçerli toplam elektronik pasaport sayısı 4.100.830'dur. Elektronik olan ve olmayan pasaport sayılarının toplamı olan 5.098.858 sayısı 6 Mart 2012 tarihi itibariyle Türkiye Cumhuriyeti vatandaşlarının sahip olduğu toplam pasaport sayısını göstermektedir.

Türkiye'de 1 Haziran 2010 tarihinde faaliyete başlayan elektronik pasaport uygulaması biyometrik pasaport uygulamasına dönüştürülmelidir. Yani biyometrik bilgiler pasaportlardaki kayıt ünitelerine eklenmelidir. Çünkü Avrupa Birliği vize almadan üye ülkelere seyahat etmek isteyen bazı ülkeler için biyometrik pasaport taşıma zorunluluğunu 2011 yılında başlatmıştır. Bu uygulama Türkiye için de önümüzdeki yıllarda gündeme gelebilecektir. Diğer yandan, Amerika Birleşik Devletleri de ülkelere vizayla seyahat etmek isteyen kişilerden biyometrik pasaport taşıma zorunluluğunu ileriye sürmekte talep edebilir. Türkiye'de elektronik pasaport alan kişiler başvuru esnasında zaten parmak izlerini vermektedir. Verilen parmak izleri pasaportlara yüklenmek suretiyle biyometrik pasaport işlemleri başlatılabilir.

Tabii bu işlemlerin yapılabilmesi için açık bir düzenleme gerekmektedir. Mevcut uygulama, 5682 sayılı Pasaport Kanunu'nun Ek 2. ve 6. maddelerine dayanarak yürütülmektedir.

Yapılacak düzenleme esnasında diğer ülkelerdeki uygulamalar esnasında yaşanan sorunlar göz önünde bulundurulmalıdır. Bu sorunlardan bir tanesi olan kişisel verilerin korunması konusu sadece seyahat belgelerinde kullanılacak biyometrik bilgiler açısından değil birçok uygulama için gerekli bir düzenlemedir. Türkiye'nin iltica ve göç politikası adına da düzenleme yapması beklenmektedir. Biyometrik pasaportlar için yapılacak düzenleme bir bütün olarak iltica ve göç alanındaki bütün ihtiyaçlar değerlendirilerek yapılabilir.

Türkiye'de sadece pasaportlarda değil başka uygulamalarda da biyometrik bilgilerin kullanılması planlanmaktadır. Örneğin, Sosyal Güvenlik Kurumu tarafından 2012 yılının 2. yarısından itibaren hastaların muayenelerinde kimlik doğrulamasının el ve parmak geometrisi tanıma yöntemi ile yapılacağı bildirilmektedir. Bu uygulama milyonlarca insanı etkileyecektir.

Bolu ilinde pilot bölge olarak uygulanan akıllı kimlik kartı projesi önümüzdeki süreçte Türkiye'de uygulanacak bir başka sistemdir. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü her vatandaş için zorunlu olan kimlik kartlarının önümüzdeki yıllarda biyometrik bilgileri de içeren akıllı kimlik kartı olarak vermeyi planlamaktadır. Bu uygulama da milyonlarca insanı etkileyecektir.

Kişilere ait biyometrik bilgilerin bulunduğu veya bulunacağı burada belirtilen veya belirtilmeyen bütün uygulamaların topluca değerlendirilmesi gerekebilir. Mükerrer yatırım, vatandaş mağduriyeti, etkilediği kişi sayısı veya performans açısından bütün uygulamaların gözden geçirilmesi katkı sağlayacaktır. Hatta uygulamalar ile birlikte kurumsal yapılanmalar da gözden geçirilebilir. Örneğin, en çok kişinin etkilendiği uygulama bünyesinde toplanan biyometrik bilgiler diğer bütün uygulamalar için kullanılması gibi bir öneri yapılabilir.

Biyometrik pasaport uygulaması ile elektronik kimlik uygulamasının bir bütün olarak değerlendirilmesi de başka bir uygulama türü olabilir. Amerika Birleşik Devletleri gibi kimlik uygulaması hiç olmayan ülkeler olduğu gibi, Fransa gibi kimlik uygulaması zorunlu olmayan ülkeler olduğu gibi, Türkiye gibi kimlik uygulaması zorunlu olan ülkeler de bulunmaktadır (Grossman, 2005: 6). Vatandaşlar

için kimlik uygulaması seçimlik veya zorunlu olan bazı ülkeler, elektronik kimlik belgesi ile hem kimliğin hem de seyahat belgesinin yerini tutan bir belge uygulaması üzerinde çalışmaktadırlar (Ng-Kruelle, Swatman, Hampe ve Rebne, 2006: 12). Örneğin, Finlandiya'daki uygulamada hazırlanan eIDC hem kimlik, hem seyahat belgesi hem de sosyal güvenlik belgesi yerine geçmektedir. Hatta bu uygulama üç ayrı bakanlık (İçişleri, Ulaştırma ve Haberleşme ile Ekonomi Bakanlıkları) tarafından yürütülmektedir (Rissanen, 2010: 184).

Genel olarak biyometrik bilgiler içeren bütün düzenlemeler, özel olarak biyometrik pasaport uygulaması, diğer ülkelerdeki uygulamalar ve kurumsal yapılanmalar bir komisyon marifetiyle detaylı bir çalışmayla somutlaştırılabilir. Komisyon tarafından yapılacak öneriler de siyasi irade tarafından uygulamaya konabilir.

3.5. BÖLÜM ÖZETİ

Biyometri uzunca zamandır bilinen bir teknoloji olmasına rağmen göç kontrol mekanizmasında kullanımının yaygınlaşması, 11 Eylül 2001 tarihinde Amerika Birleşik Devletleri'nde meydana gelen terör saldırıları nedeniyle olmuştur.

Göç yönetiminde kullanılan biyometrik sistemlerin bir türü, otomatik sınır geçiş kapılarıdır. Otomatik sınır geçiş kapıları, iyi niyetli veya sık seyahat eden yolcuların iş ve işlemlerini kolaylaştırmaktadır. Bu sistem ile yolcular herhangi bir biyometrik tarama türünün kullanımı ile sınır kapısını otomatik olarak hızlıca geçmektedirler. Avrupa ülkelerinde birçok havalimanında otomatik geçiş kapısı kullanılmaktadır. Amsterdam Schiphol Havalimanı'nda; iris tarama sistemi, Frankfurt Havalimanı'nda; iris tarama sistemi, Paris Charles de Gaulle Havalimanı'nda; parmak izi tanıma sistemi ve Londra Heathrow Havalimanı'nda; iris tarama sistemi otomatik geçiş kapısı olarak kullanılmaktadır.

Ülkelerin, göç yönetiminde biyometrik sistemleri kullanmaya başlamalarına paralel olarak Uluslararası Sivil Havacılık Örgütü her ülkenin pasaportlarının makine tarafından otomatik olarak okunabilen pasaport standartlarını taşıması için son tarih

olarak Nisan 2010 tarihini belirlemiştir. Eylül 2010 tarihi itibarıyla 188 ülkede,¹¹¹ makine tarafından otomatik olarak okunabilen pasaport düzenlemesi bulunmaktadır.

Göç yönetiminde kullanılan bir başka biyometrik sistem, biyometrik pasaporttur. Biyometrik pasaport, içinde kişiye ait biyometrik verileri barındıran makine tarafından otomatik olarak okunabilen bir pasaport türüdür. Biyometrik pasaporttaki biyometrik veriler (yüz resmi, parmak izi gibi) pasaport içindeki akıllı kartlarda (*contactless chip*, *rfid* devresi gibi) saklanmaktadır.

Amerika Birleşik Devletleri'nde 11 Eylül 2001 terör saldırısından sonra yapılan düzenlemelerden en önemlisi Vatanseverlik Yasası'dır. Vatanseverlik Yasası diye bilinen yasa, terörle etkin mücadele için istihbarat kuvvetlerinin kabiliyetlerinin artırılmasını ve etkin bir istihbarat paylaşımının yapılmasını sağlamaktadır. Vatanseverlik Yasası'nın dördüncü kısmında Amerika Birleşik Devletleri sınır kontrol yönetiminde yapılacak değişiklikler düzenlenmektedir. Vatanseverlik Yasası'nda öngörülen düzenlemelerden bir tanesi, Amerika Birleşik Devletleri'ne seyahat etmek isteyen yabancıların vize başvurusu yaparken ülkelerindeki Amerika Birleşik Devletleri konsolosluklarında parmak izlerini sisteme kaydettirmeleri ve Amerika Birleşik Devletleri'ne giriş ve çıkışlarında bir giriş çıkış sisteminin yürürlüğe konmasıdır. Öngörülen giriş çıkış sistemi Amerika Birleşik Devletleri İç Güvenlik Örgütü tarafından 2004 yılından beri US-VISIT programı ile yapılmaktadır. Ayrıca, Amerika Birleşik Devletleri Dışişleri Bakanlığı, kendi vatandaşlarına 2006 yılından itibaren biyometrik pasaport vermeye başlamıştır. US-VISIT programı kapsamında Amerika Birleşik Devletleri'ne giriş yapan kişiler için biyometrik tanımlayıcılar kullanılarak sınır kontrol işlemleri yapılmaktadır (Thomas, 2005: 399).

Avrupa Birliği, hem Amerika Birleşik Devletleri'nin hem de ICAO'nun etkisiyle, göç kontrol mekanizmasında biyometrik sistemlerin kullanımını öngören düzenlemeler yapmıştır. Amerika Birleşik Devletleri, Avrupa Birliği'nin göç politikasını etkilemiş ve Avrupa Birliği'nde biyometrik sistemlerin kullanımının hızlanmasını sağlamıştır. Avrupa Birliği Komisyonu, pasaport ve seyahat belgelerine biyometrik özelliklerin eklenmesi için ikinci grup teknik özellikleri 28 Haziran 2006 tarihinde belirlemiştir. Avrupa Birliği'nin pasaport ve seyahat belgelerinde

¹¹¹ Kajevic, 2006: 22.

biyometrik özelliklerin eklenmesi düzenlemesine göre (EC 2252/2004), 28 Haziran 2006 tarihinden 18 ay sonra olan 28 Aralık 2007 tarihinde biyometrik yüz resminin uygulanmasına ve 36 ay sonra olan 28 Haziran 2009 tarihinde ise parmak izinin uygulanmasına başlanmıştır.

Amerika Birleşik Devletleri Vize Feragat Programı'ndan yararlanmak isteyen Avrupa Birliği üye ülke vatandaşları, 26 Ekim 2006 tarihinden sonra Amerika Birleşik Devletleri'ne sadece biyometrik pasaportla giriş yapmak durumunda kalmışlardır.

Avrupa Birliği göç yönetimi konusunda Amerika Birleşik Devletleri ile işbirliği yapmakta ve uçuş tarihi, bilet numarası, havayolu şirketi, ödeme, koltuk numarası gibi yolcu bilgilerini Amerika Birleşik Devletleri ile paylaşmaktadır. Yolcu bilgilerinin Amerika Birleşik Devletleri ile paylaşılmasını öngören 17 Mayıs 2004 tarihli karar, Avrupa Adalet Divanı tarafından iptal edildiğinden dolayı 23 Kasım 2011 tarihinde Avrupa Konseyine sunulan “Yolcu Bilgilerinin Amerika Birleşik Devletleri İç Güvenlik Örgütü'ne Transfer Edilmesi Konusunda Avrupa Birliği ve Amerika Birleşik Devletleri Arasında Yapılan Anlaşma'nın Sonucu” isimli tebliğ¹¹² ile konu yeniden düzenlenmiştir. Avrupa Birliği'nin göçle ilgili yaptığı başka bir düzenleme, üçüncü ülke vatandaşlarının Avrupa Birliği üyesi ülkelere girerken biyometrik pasaport kullanma zorunluluğunun getirilmesidir (Özcan ve Yılmaz, 2007: 99).

Avrupa Konseyi'nin, EC 2252/2004 sayılı tüzüğüne göre Komisyon tarafından ikinci grup teknik özelliklerin belirlendiği 28 Haziran 2006 tarihinden sonra pasaportlarda biyometrik yüz resminin uygulanmasına (18 ay sonra) 28 Aralık 2007 tarihinde ve parmak izinin uygulanmasına (36 ay sonra) 28 Haziran 2009 tarihinde başlanması öngörülmüştür. Avrupa Birliği'nde 28 Haziran 2009 tarihinde başlayan biyometrik pasaportlar ile hem pasaport hem de pasaport sahibi doğrulaması yapılabilmektedir.¹¹³

Avrupa Birliği'nin 13 Aralık 2004 tarihli EC 2252/2004 sayılı tüzüğü ile yürürlüğe koyduğu pasaport ve seyahat belgelerine biyometrik özelliklerin eklenmesi

¹¹² COM (2011) 807 final.

¹¹³ New, secure biometric passports in the EU, strengthen security and data protection and facilitates travelling, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/872&type=HTML&aged=0&language=EN&guiLanguage=en>, (Erişim Tarihi: 20 Aralık 2011).

düzenlemesi EC 2252/2004 tarihli kararı deęiřtiren 28 Mayıs 2008 tarihli ve EC 444/2009 sayılı tüzük ile yüz resmi özellięi açısından 28 Aralık 2011 ve parmak izi özellięi açısından 28 Mayıs 2013 tarihine kadar uzatılmıřtır.

Türkiye’de, 1 Haziran 2010 tarihinden itibaren Uluslararası Sivil Havacılık Örgütü’nün tavsiyelerine uygun řekilde elektronik pasaport düzenlenmektedir. Yeni düzenlenen elektronik Türk pasaportlarında, parmak izi veya biyometrik resim özellikleri gibi biyometrik veriler bulunmamaktadır (Tanıř, 2012). Biyometrik veriler içerisinde olmayan yeni pasaportlar gerçek anlamda “biyometrik pasaport” olarak deęerlendirilememektedir. Yeni elektronik pasaportlar Uluslararası Sivil Havacılık Örgütü’nün standartlarına uygun řekilde makine tarafından otomatik olarak okunabilen elektronik pasaporttur.

DÖRDÜNCÜ BÖLÜM

BIYOMETRİNİN AVANTAJ VE DEZAVANTAJLARI

Uluslararası Sivil Havacılık Örgütü ICAO'nun kararları sonucu ülkeler, pasaport belgelerini makine tarafından otomatik olarak okunabilecek şekilde düzenlemektedirler. Amerika Birleşik Devletleri'nin başta Avrupa Birliği ülkeleri olmak üzere (Hert, 2005: 20) birçok ülkeyi etkilemesi sonucu ülkeler pasaport veya diğer kimlik belgelerine¹¹⁴ biyometrik özellikleri eklemektedirler.

Yasadışı göçü önlemek, sınır kontrollerini güçlendirmek ve seyahat belgelerindeki sahteciliği azaltmak amaçlarıyla 11 Eylül 2001 terör olayından sonra biyometrik sistemlerin yoğun olarak kullanılmaya başlandığı daha önceki bölümlerde ifade edilmiştir.

İyi niyetli seyahat edenlerin veya sık seyahat edenlerin vize işlemlerini hızlandırmak ve kolaylaştırmak amacıyla bazı sınır kapılarında otomatik geçiş sistemleri de kullanılmaktadır.

Çeşitli sebeplerle kullanılan biyometrik sistemlerin sayısı her geçen yıl artmaktadır. Sadece Avrupa'da kullanılan biyometrik sistemler 1996 yılında 8.550 iken bu sayı 2004 yılında 150.000'i geçmiştir (Kajevic, 2006: 24). Biyometrik sistem veya biyometrik ürün kullanımı bütün dünyada her geçen gün yaygınlaşmaktadır.

Biyometrik sistemlerin avantajlı özelliklerinden bir tanesi daha öne çıkmaktadır. Biyometrik sistemler göç kontrol yönetimi haricinde birçok alanda özellikle güvenlik amacıyla kullanılmaktadır. Yukarıda verilen örneklerde olduğu gibi çeşitli alanlarda kullanılan biyometrik sistemler birçok faydalı özelliğe sahip olsalar da tamamen sorunsuz sistemler değildir.

Biyometrik sistemlerin birçok dezavantajı bulunmaktadır. Biyometrik sistemlerin dezavantajları aşağıda sıralanırken özellikle mahremiyetin ihlali ve kişisel verilerin korunması konuları önemi itibarıyla müstakilen tartışılmaktadır.

Bu bölümde önce biyometri teknolojisinin avantaj ve dezavantajlarından bahsedilmektedir. Göç kontrol mekanizmasında biyometrinin kullanımının avantaj ve dezavantajları ayrıca incelenmektedir.

¹¹⁴ Aralık 2004 tarihinde kabul edilen 2252/2004 sayılı tüzük, pasaportlarda biyometrik sistemlerin kullanımını düzenlemektedir.

Sınır kapılarında kurulu bulunan biyometrik sistemlere alternatif olarak klasik geçiş sistemlerinin varlığı bu bölümde değinilen konulardan bir başkasıdır. Biyometrik sistemlerin her zaman yüzde yüz başarılı olmaması (JRC, 2008: 108) sorun olarak değerlendirilmektedir. Göç yönetiminde yaşanan başarısızlık sınır kapısında kişinin hakkına tecavüz olduğundan bu eksikliğin telafisi adına sınır kapılarında alternatif kontrol sistemlerinin kurulması gerekli olmaktadır. Bu da ekstra iş gücü, zaman kaybı ve maliyet demektir. Fakat kişilerin seyahat özgürlüğünün sisteme ait hatalardan dolayı engellenmemesi için alternatif yöntem kurulması bir anlamda zorunluluktur.

Biyometri teknolojisinin mevcut veri koruma kuralları temel ilkelerine etkisi dikkate alınmaktadır. Bu ilkelere göre veriler, açık ve meşru amaçlar için kanunlarla öngörülmüş durumlarda elde edilmelidir. Elde edilen veriler, belirtilen amaçlar ile uyumlu bir şekilde işlenmelidir (Thomas, 2005: 391). Elde edilen veriler güvenli bir şekilde tutulmalı; tutulan veriler doğru, ilgili ve güncel olmalıdır.

Bu bölümde incelenen son konu göç kontrol mekanizması olarak biyometrik sistemlerin etkinliğidir. Etkinlik öncelikle göç kontrol mekanizmasında kullanılan biyometrik sistemlerin avantaj ve dezavantajlarının incelenmesiyle tartışılmaktadır. Ayrıca, 11 Eylül 2001 terör olayından sonra biyometrik sistemlerin yaygınlaşma sebebi olan sınır güvenliğini artırma ve yasadışı göçü önlemedeki başarısı değerlendirilmektedir.

4.1. AVANTAJLAR

Biyometri teknolojisinin ve biyometrik sistemlerin kullanımının ilk akla gelen üstünlükleri hız, doğruluk ve güvenlidir (Redpath, 2007: 31; Kajevic, 2006, ss:17-18). Biyometrik sistemler hızlıdır. Çünkü saniyeler¹¹⁵ gibi bir sürede kıyaslama yapılabilmekte ve sonuç alınabilmektedir. Biyometrik sistemlerin doğruluk oranı yüksektir. Biyometri türlerine göre değişkenlik gösterse bile parmak izi gibi bazı biyometrik sistemlerinin başarısı yüzde yüze yakındır. Biyometrik sistemlerin

¹¹⁵ Parmak izi tanıma ortalama işlem süresi 9 saniye ve iris tarama ortalama işlem süresi 12 saniyedir (JRC, 2005: 60).

Biyometrik sistemlerle otomatik tanımlama saniyeler içinde gerçekleştirilmektedir (PublicTechnology, 2007).

güvenlik oranı yüksektir. Çünkü kişiye ait biyometrik özelliğin sahtesinin üretilmesi ve böylece sistemin aldatılması kolay değildir. Hız, doğruluk ve güvenlik biyometrik sistemlerin avantaj ve üstünlüklerini genel olarak ifade etmektedir.

Biyometrik sistemler daha başka avantajlı özelliklere de sahiptir. Bunlar sırasıyla kullanım kolaylığı, biyometrik sistemlerde kullanılan kişi özelliklerinin değişmeden kalması, sahteciliğin önlenmesi ve sınır kapılarında geçiş işlemlerinin biyometrik sistemler sonucu otomatik olmasından dolayı sınır görevlilerinin inisiyatifinin azalmış olması olarak sayılabilmektedir.

Biyometrinin bir başka avantajı kullanımının kolaylığı ve basitliğidir(Kajevec, 2006: 18). Biyometrik sistemler kullanılırken kişi sistemin yanına yaklaşp, sadece elini, yüzünü veya parmak izini uzatmakta veya ses tanıma sistemi ise konuşmaktadır. Kullanıcının parola gibi bir şeyi hatırlamasına veya anahtar gibi bir şeyi taşımasına gerek yoktur. Klasik kimlik tanıma ve doğrulama yöntemlerinde kişiler kendini tanıtmak için nüfus cüzdanı, ehliyet gibi belgeleri taşımak veya parola, şifre gibi bilgileri hatırlamak zorundadır (Kaymaz, 2010: 1). Biyometrik sistemler, kullanıcı açısından kullanımı kolay ve basittir (Kajevec, 2006: 18).

Biyometrinin en önemli avantajlarından birisi, bir kişiyle ilişkilendirilen vücut özelliğinin uzun süre boyunca hatta bazı durumlarda ömür boyu değişmeden aynı kalmasıdır(T-PD, 2005: 7; Kajevec, 2006: 17). Çünkü biyometrik özellikler vücuda veya davranışlara ait özellikler olduğundan kişiden ayrılamaz, ödünç alınamaz veya bir başkasına devredilemez durumdadır (Kajevec, 2006: 10). Diğer yandan anahtar, parola veya kimlik kartı gibi doğrulama araçları kaybedilebilir, çalınabilir veya bozulabilir durumdadır. Çünkü bu tür doğrulama araçlarında doğrulama işlemi bir bilgi veya bir ürüne sahip olma yoluyla yapılmaktadır. Ancak biyometrik sistemler, kişinin ayrılmaz bir parçası olan fizyolojik ve davranışsal özellikleri ile doğrulama yapmaktadır. Biyometri bu şartlarda diğer araçlardan daha üstündür.

Biyometrik sistemlerin kendilerine özgü birçok avantajlı ve faydalı yanı olduğu değerlendirilmiştir. Göç kontrol mekanizmasında kullanılan biyometrik sistemlerin avantajlarına bakıldığında bazı yeni durumlarla karşılaşılmaktadır.

Vize işlemlerinde ve sınır kontrollerinde biyometri kullanımının önemli bir avantajı seyahat belgelerinin ve vizelerin sahteciliğe karşı korunaklı olmasıdır.

Biyometrik özellikler seyahat belgelerinin sahteciliğe karşı güvenliğini yükseltmektedir. Çünkü biyometrik sistemler ile pasaport ve seyahat belgeleri daha detaylı incelenmektedir (JRC, 2008: 27). Biyometrik sistemlerin kullanımı ile sadece belgelerin orijinallik kontrolü yapılmayıp aynı zamanda belgeyi taşıyan kişinin de doğrulanması işlemleri yapılmaktadır. Bütün bunlar iç güvenliğe katkı sağlamaktadır.

Vize işlemlerinde ve sınır kontrollerinde biyometri kullanımının avantajlarına bir başka örnek olarak ayrımcılığın önlenmesi sayılabilir (Redpath, 2007: 31; Kajevic, 2006: 17–18). Biyometrik sistemler kullanıldığında sınır kapılarında geçişler otomatik olmaktadır. Görevlilerin kişisel yorum ve değerlendirmelerine gerek kalmadığı gibi biyometrik sistemlerin kullanımı ile göçmenler ve mülteciler kendilerini tartışmasız bir şekilde daha doğru şekilde ifade edebilmektedirler (Thomas, 2005: 388). Dolayısıyla kişisel değerlendirmeler sonucu olabilecek ayrımcılık yaşanmamaktadır.

Göç kontrol mekanizmasında kullanılan biyometrik sistemlerin önemli bir avantajı, iltica edenlerin geri dönüş ülkelerini bulma konusunda sağladığı kolaylaştırmadır (Thomas, 2005: 387). İltica edenlerin bilgileri kolay erişilebilir veri tabanında tutularak, geldikleri gerçek ülke belirlenmekte, başarısız sığınmacıların iade işlemleri kolayca yapılabilmektedir (Kajevic, 2006: 388). Ülkeler, sınır dışı etmek istedikleri yabancıların hangi ülke vatandaşı olduğunu bilmeden kişileri sınır dışı edememektedir. Diğer yandan, iltica eden kişiler de bu durumu bildiklerinden mensup oldukları milliyetin tespit edilmemesi için pasaport veya seyahat belgelerini kaybetmektedirler. Böylece, *EURODAC*¹¹⁶, *VIS*¹¹⁷ ve *SIS II*¹¹⁸ sistemlerine kaydedilen biyometrik sistemler yasadışı göçü önleme işlemlerine de katkı sağlamaktadır (Thomas, 2005: 387).

Biyometrik sistemlerin sınır kapılarında sağladığı bir başka avantaj sık seyahat eden yolcular içindir (Kajevic, 2006: 388). Sık seyahat eden yolcular talep etmeleri halinde, önceden kayıt yaptırmak şartıyla sınır kapılarında kendileri için

¹¹⁶ Eurodac, Dublin II düzenlemesine göre iltica başvurularının kaydedildiği sistemdir. İltica başvurularında sorumlu ülkeyi bulmak amacıyla tüm Üye Devletlerin kullanabildiği ilk ortak AB Otomatik Parmak İzi Tanımlama Sistemi (AFIS)'dir.

¹¹⁷ Schengen Sözleşmesine göre vize başvurularının kaydedildiği sistemdir.

¹¹⁸ Schengen Bilgi sisteminin yenilenmiş halidir. Schengen üyesi ülkelerin sınırlardaki kabul, ret ve alarm gibi işlemlerinin kaydedildiği ve yetkililerin eriştiği bir bilgi bankasıdır.

özel olarak hazırlanmış kapılardan biyometrik sistemleri kullanarak hızlıca geçebilmektedir.

4.2. DEZAVANTAJLAR

Biyometri teknolojisinin ve biyometrik sistemlerin birçok önemli üstünlüğüne rağmen en temel eksikliği ve dezavantajı doğruluk oranının yüzde yüz olmaması sayılabilir (JRC, 2008: 108; Thomas, 2005: 379). Burada kastedilen doğruluk en son sonuç başarı kararıyla ilgilidir. Özellikle büyük biyometri uygulamalarında yani on binlerce veya yüz binlerce birey için uygulanan biyometrik sistemlerde %1’lik bir hata çok fazla sayıda yanlış sonuç üretebilmektedir.

Biyometrik sistemlerin kayıt veya karşılaştırma gibi aşamalarında hatalar olabilmektedir. Kayıt aşamasında veya karşılaştırma aşamasında farklı oranlarda yanlışlıklar olabilmektedir. Kayıt aşamasında yaşanan problemlere örnek olarak karşılaştırma yapabilmek için yeterli kalitede biyometrik resmin alınamaması verilebilir (Redpath, 2005: 15). Biyometrik süreçlerin başlangıç noktası olan kayıt aşamasındaki kayıt kalitesi veya bir başka deyişle biyometrik resim kalitesi sonuç başarı oranını etkileyen en önemli faktörlerden birisidir (Kaymaz, 2010: 2). Birinci bölümde değinildiği üzere, toplam başarı üzerinden değerlendirmede kullanılan hata türleri vardır. Bu hata türlerinden birisi olan FNMR (*False Non-Match Rate*) oranları “*Biometrics at the Frontiers Assessing the Impact on Society*” isimli raporda belirtildiğine göre Parmak İzi Tanımada %2,5 iken, Yüz Resmi Taramada %4’tür (JRC, 2005: 60).

Biyometri teknolojisinin ve biyometrik sistemlerin önemli bir başka dezavantajı da teknolojiye özel eksiklikleridir (Kajevic, 2006: 18). Biyometri teknolojisine özel eksiklikler olarak başarı oranından, biyometrik verinin kalitesinden ve kullanılan algorithmadan kaynaklanan hatalar olarak sıralanabilir. Örneğin, Hollanda hükûmeti tarafından hazırlatılan bir raporda, gözlük giyen kişilerin yüz tanıma sistemlerinde %45 oranında hata mesajıyla karşılaşmaları biyometrik türün başarı oranındaki eksikliğine bir örnektir (Kajevic, 2006: 19).

Biyometri teknolojisinin ve biyometrik sistemlerin bir başka dezavantajı maliyettir (JRC, 2005: 38; JRC, 2008: 27). Biyometrik sistemlerin her tanımlama

sisteminde olduğu gibi bir maliyeti bulunmakla birlikte özellikle biyometri türüne göre sistemin masrafı ciddi oranda artabilmektedir. Biyometrik sistemlerin maliyeti vize ücretlerinde artış olarak vize başvurusu yapanlara yansıtılabilmektedir (JRC, 2008: 27). Biyometrik sistemlerin toplam maliyeti sadece sistemlerin maliyeti değil, yedek olarak kurulan alternatif sistem ve biyometrik sistemleri kullanan nitelikli personel maliyetini de kapsamaktadır (JRC, 2005: 98). Diğer taraftan, biyometrik sistemlerin sınır kontrollerinde kullanılabilmesi önemli miktarda bir bütçeyi gerekli kılmasından dolayı her ülke bu tür altyapıyı kuramamaktadır. Bu durum gelişmiş ülkeler ile diğer ülkeler arasında bir fark oluşturmakta ve sınır kontrolleri açısından eşitsizliğe sebep olmaktadır (Thomas, 2005: 390).

Diğer yandan biyometri teknolojisine ait bazı dezavantajlar göç kontrol işlemlerinde de geçerlidir. Örneğin, kişisel verilerin korunması problemi hem teknolojiye hem de göç yönetimine ait bir problemdir.

Vize işlemlerinde ve sınır kontrollerinde biyometrinin kullanımının önemli bir dezavantajı fonksiyonel hata diye de isimlendirilen, biyometrik bilgilerin toplanma maksadının haricinde ve izin verilmeyen sebeplerle kullanılmasıdır (Thomas, 2005: 379). Vize işlemlerinde ve sınır kontrollerinde toplanan biyometrik verilerin kişinin rızası olmadan başka bir amaç için kullanılabilmesi mümkündür (Redpath, 2005: 11).

Fonksiyonel hata, *BioSec*¹¹⁹ isimli Avrupa Komisyonu destekli proje tarafından kullanılan bir kavramdır. Sınır güvenliğinde fonksiyonel hata sınır kapılarındaki biyometrik sistemler tarafından toplanan biyometrik verilerin kullanılması sonucu ortaya çıkmaktadır. Kişisel bilgiler olarak değerlendirilen biyometrik bilgilerin başka alanlarda kullanılmasına örnek, toplanan biyometrik verilerin havayolu şirketleri ve kolluk kuvvetleri (Redpath, 2007: 31) tarafından kullanılması sayılabilir. Fonksiyonel hata, uluslararası uygulamalarda görülebildiği gibi ülke içi uygulamalarda da görülebilmektedir (Redpath, 2005: 10). Örneğin, göç

¹¹⁹ BioSec araştırma projesi, Avrupa Komisyonu 6. Çerçeve Programı tarafından ortaklaşa finanse edilen ve dokuz ülkeden 23 kuruluşun katılımıyla Haziran 2004 ile Eylül 2007 tarihleri arasında çalışan bir projedir. BioSec projesi teknolojinin standartlarını belirlemek, eğitim materyalleri hazırlamak ve biyometrik sistemlerin değerlendirme şartlarını belirlemek üzere yürütülmüştür. BioSec araştırma projesi bulguları bir kitapta yayınlanmıştır (Petrovska-Delacr  taz, Dijana; Chollet, G  rard; Dorizzi, Bernadette (Der.), (2009), *Guide to Biometric Reference Systems and Performance Evaluation*, London:Springer).

işlemlerinde toplanan biyometrik verilerin suçun önlenmesi veya suçlunun bulunması amacıyla devletler tarafından kullanılabilmesi mümkündür.

Sınır kontrollerinde toplanan biyometrik verilerin başka sistemlerle beraber çalışmadığı durumlarda fonksiyonel hata daha da büyüebilmektedir. Sistemlerin ortak çalışması; bir cihazın birçok yerde aynı yol, yöntem ve cihazlarla sorunsuz olarak çalışabilmesidir (JRC, 2005: 38).

Göç yönetiminde biyometrik sistemlerin kullanımına ilişkin uluslararası ölçekte standartlar olmadığı için ürünlerin, markaların ve ülkelerin farklı uygulamaları olmaktadır. Standartların olmayışı sonucu ortaya çıkan durum, farklı ülkelerde çalışan çeşitli biyometrik sistemlerin birlikte uyum içerisinde çalışamaması, yani bir sistemde kullanılan bir cihazın başka bir sistemde okunamaması gibi olabilmektedir (Redpath, 2005: 31).

Ortak çalışma problemi olduğu durumlarda biyometrik veriler tek başına yeterli olmamakta, bundan dolayı kişi hakkında daha fazla kişisel bilgi ile işlem yapılmaktadır. Bu durum, Avustralya, Kanada ve Amerika Birleşik Devletleri'nde uygulanan Yolcuların Detaylı İzlenmesi Programı (*Advanced Passenger Screening Program*) kapsamında yaşanmıştır (Thomas, 2005: 391). Bahsedilen uygulamalarda sistemler sorunsuz bir şekilde beraber çalışmadığından dolayı yolcuları belirleyebilmek için yolculara ait kişisel bilgiler fazladan kaydedilmektedir.

Biyometrik sistemlerde kullanılan ürünlerin örneğin pasaportlardaki hafıza kartının birçok sınır kapısındaki sistemlerle okunabilir olmasının yani ortak çalışmasının kolaylık gibi bir avantajı olmakla birlikte özellikle uluslararası platformda kişisel verilerin korunması açısından dezavantajı olabilmektedir (JRC, 2005: 38). Kişiye ait özel bilgilerin, her sistem tarafından okunabildiği durumlarda gerekli önlemler alınmazsa kişisel bilgilere birçok kişi ya da kuruluş tarafından ulaşılabilme riski bulunmaktadır.

Bütün bu problemlerden dolayı, Uluslararası Sivil Havacılık Örgütü ICAO, sivil havacılıkta ulaştırma güvenliğinin artırılması için vize işlemlerinde ve sınır kontrollerinde kullanılan biyometrik sistemlerin uluslararası alanda birlikte çalışabilir durumda olmasını tavsiye etmektedir (T-PD, 2005: 9). Birlikte çalışma prensiplerini daha iyi belirleyebilmek için bu alandaki ilgili otoriteler olan Avrupa Birliği, Avrupa

Konseyi, Ekonomik Kalkınma ve İşbirliği Örgütü ve Uluslararası Sivil Havacılık Örgütü yakın işbirliği içerisinde çalışmalıdır.

Biyometrik verilerin toplama sebebi haricinde kullanılması kural eksikliğinden veya denetim eksikliğinden kaynaklanabilmektedir (Redpath, 2005: 11). Biyometrik verilerin toplanması ve kullanılmasına ilişkin devletler sıkı kurallar belirler ve belirlenen kuralları iyi uygularsa fonksiyonel hata yani biyometrik verilerin toplanma sebebi haricinde kullanılması sorunu daha az yaşanabilir.

Biyometrik verilerin toplanma sebebi haricinde kullanılması, Avrupa Birliği Avrupa Birliği Mülteciler Veri tabanı *Eurodac* veri tabanı için geçerli olduğu gibi (Thomas, 2005: 388) Amerika Birleşik Devletleri *IDENT*¹²⁰ veri tabanı için de (Thomas, 2005: 393) geçerlidir. Londra’da 2005 yılı Temmuz ayında gerçekleştirilen bombalı terör saldırısı soruşturulurken, Vize Bilgi Sistemi *VIS*, Geliştirilmiş II. Kademe Schengen Bilgi Sistemi *SIS II*, Avrupa Birliği Mülteciler Veri tabanı *Eurodac* ve Polis veri tabanlarının hepsine birden erişilmiştir (Thomas, 2005: 394). Kişilere ait toplanan kişisel verilere erişim, bazı durumlarda politik kararlar sebebiyle genişletilmiş olarak yapılabilmektedir. Yolcu Bilgilerinin Paylaşılması gibi Avrupa Birliği ile Amerika Birleşik Devletleri arasında kolluk kuvvetleri düzeyinde başka bilgi değişim sistemleri mevcuttur.

Vize işlemlerinde ve sınır kontrollerinde biyometri kullanımının mahremiyetle ilgili oluşturduğu bir endişe, toplanan biyometrik veriler sonucu kişilerin dolaylı olarak izlenebilmesidir (JRC, 2005: 98). Özellikle, üçüncü ülke vatandaşlarından vize kontrol işlemleri esnasında elde edilen detaylı bilgiler, yabancı kişilerin izlenmesi sonucunu doğurabilmektedir (Redpath, 2005: 11). Sınır kapılarında toplanan veriler, üçüncü ülke vatandaşlarının ülke içindeki hareketlerini de takip etme imkânı sunmaktadır (Redpath, 2007: 31). Toplanan biyometrik veriler ile oluşturulan veri tabanını kullanarak devlet görevlilerinin gizlice kişileri izleyebilmeleri mümkündür.

Vize işlemlerinde ve sınır kontrollerinde biyometrinin kullanımının bir başka dezavantajı da, toplanan biyometrik verilerin kişilere özel daha başka bilgileri açığa

¹²⁰ ABD IDENT veri tabanı kullanımı: Örneğin, ziyaretçinin bir suçlu ya da terörist olduğu olasılığını belirlemek için FBI veri tabanının yanı sıra 20’den fazla diğer devlet veritabanları ile çapraz kontroller yapılmaktadır (Thomas, 2005: 393).

çıkartabilme ihtimalleridir (Redpath, 2007: 31). Toplanan biyometrik veriler sonucu, kişilere ait sağlık gibi diğer verilerin asıl maksat olmasa dahi ortaya çıkabilmesi mümkündür (JRC, 2005: 45–46). Örneğin, iris tarama sistemlerinde iris bilgileri kişinin sağlığı hakkında başka bilgileri yani kişinin kalıcı hastalıklarını da ortaya çıkartabilmektedir (Redpath, 2005: 11; Hornung, 2007: 249). İris bilgileri kişilere ait şeker hastalığına ve hipertansiyona,¹²¹ HIV¹²² hastalığına işaret edebildiği bilimsel çalışmalarla gösterilmektedir. Bir başka çalışma sonucu, belirli türde parmak izi olan kişilerin %50 oranında bir çeşit mide hastalıkları olduğu gösterilmiştir (JRC, 2005: 46).

Bir başka dezavantaj biyometrik verilere yetkisiz kişilerin erişebilmesidir (Redpath, 2007: 31). Yetkisiz erişim deyince akla ilk gelen biyometrik verilere erişim yetkisi olmayan havayolu şirketleri gibi yetkisiz kişi ve kuruluşların da ulaşabilmesidir (Redpath, 2005: 10). Yetkisiz erişim, birden fazla aktörün biyometrik verilere ulaşma imkânından kaynaklanabilmektedir. Sınır yönetiminde biyometrik verilere sadece görevli devlet kurumları değil aynı zamanda seyahat belgelerinin kontrolünü yapan görevli havayolu şirketleri elemanları da ulaşabilmektedir (Redpath, 2005: 12). Bu durum, yani birden çok aktörün biyometrik verilere ulaşabilmesi yetkisiz erişim sorunu yaşanma ihtimalini artırmaktadır.

Diğer yandan başka bir yetkisiz erişim yöntemi de seyahat belgelerindeki biyometrik verileri uygun araçlarla uzaktan okuyarak olmaktadır. Seyahat belgelerinde bir dönem kullanılan RFID bütünleşmiş devreleri içindeki bilgiler kriptolanmış değil ise 20 metre uzaktan okunabilmektedir (Thomas, 2005: 391; Hornung, 2007: 256). Bu sorun daha sonradan halledilmiştir. Yetkisiz erişim sadece bilgilere erişmek anlamında değil aynı zamanda sabotaj şeklinde verilerin imha edilmesi olarak da uygulanabilir.

Biyometrinin diğer bir dezavantajı istemci veya sunucu saldırısı olarak tabir edilen sistemsal bir aldatmaca yapılabilir olmasıdır (Kajevic, 2006: 18). İstemci saldırısı, bir kişinin kaydedilmiş sinyal bilgisinin biyometrik sisteme başka bir kişiyiymiş gibi tanıtılarak sistemin kandırılmaya çalışılmasıyla olur. Sunucu saldırısında kandırılmaya çalışılan sunucudur. Bir kişi geçerli bir biyometrik örneği

¹²¹ J D Woodward, Jr, N M Orlans ve P T Higgins’den akt. Hornung, 2007:249.

¹²² A Albrecht’ten akt. Hornung, 2007:249.

alıp (örneğin parmak izinin kopyası) sunucuya orijinal biyometrik verinin kendisi olduğuna inandırmasıdır. Bu durum veri tabanına müdahale edip, değişiklik yaparak olabilmektedir.

Vize işlemlerinde ve sınır kontrollerinde biyometri kullanımının birçok dezavantajı yukarıda sayılmıştır. Dezavantajlar sıralamaya devam edilse yeni başlıklar bulunabilmektedir. Sayılanlar biyometri sisteminin kullanımın birçok riski olduğunu anlatmaya yeterlidir. Göç yönetiminde kullanılan biyometrik sistemlerin dezavantajlarının yanı sıra temel bir eksiklik olmasa bile bu tür sistemlere ilişkin bazı sorunlar olduğunu da kabul etmek gerekir.

Bu sorunlar; süre, yaş aralığı, doğru ve güncel bilgi olması, bilgilerin saklanma usulü, bilgilerin paylaşılma usulü ve politikanın şeffaf olması olarak sayılabilmektedir (Redpath, 2005: 13). Kişisel veri olarak değerlendirilen biyometrik verilerin nasıl ve nerede saklanacağı, paylaşılma usulü ve imha usulü önemli başlıklardır. Önemli bir başka sorun, hangi yaş aralığındaki kişilerin biyometrik bilgilerinin toplanacağıdır. Yapılan araştırmalar sonucu, Avrupa Birliği düzenlemeleri¹²³ 6 yaş altındaki çocukların parmak izlerinin alınmayacağını öngörmektedir. Saklanan biyometrik bilgilerin doğru ve güncel bilgiler olması önemlidir. Güncel olmayan biyometrik bilgilerin saklanması kullanıcılar açısından ciddi mağduriyetler doğurma ihtimali bulunmaktadır.

EC 444/2009 sayılı Avrupa Birliği düzenlemesi; biyometrik verilerin nerede ve nasıl saklanacağı kararını üye ülkelere bırakmıştır. Biyometrik sistem kullanımı sonucu büyük veri tabanları oluşmaktadır (Redpath, 2007: 31). Bu veri tabanlarının güvenliğinin sağlanması önemli bir konudur. Birçok ülke, biyometrik veriyi merkezi bir biyometrik veri tabanında saklarken, Almanya gibi bazı ülkeler merkezi bir biyometrik veri tabanının yasal olmadığını değerlendirmektedir (Hornung, 2007: 254).

Merkezi biyometrik veri tabanı güvenlik endişeleri açısından da tartışmalı bir konudur (Redpath, 2007: 31). Çünkü merkezi veri tabanında biyometrik bilgilere ilave olarak kişisel bilgiler de saklanmaktadır (Hert, 2005: 9).

Merkezi veri tabanına iyi bir alternatif, akıllı kart (*smartcard*) teknolojisidir (Thomas, 2005:396–397). Akıllı kartlara biyometrik veriler kaydedilmekte ve

¹²³ EC 444/2009.

kıyaslama akıllı karttaki verilerle yapılmaktadır. Biyometrik veriler akıllı kartlarda saklandığında, verilerin başkaları tarafından silinme ihtimali daha düşük olmaktadır (Hert, 2005: 10).

Biyometri uygulamalarında kullanılan akıllı kartların bazı sorunları da bulunmaktadır. Örneğin, kişiler akıllı kartlardaki bilgileri okuyamamakta, içinde hangi verinin olduğunu bilememekte ve güvenlik önlemlerinin yeterli olup olmadığını tespit edememektedir (Liu, 2009: 246). Akıllı kartlarda (*smartcard*) gereğinden fazla yer alanının olması da ayrı bir tartışma konusudur. Fazla yer alanı, daha fazla kişisel bilginin kaydedilebilmesi demektir. ICAO'nun biyometrik pasaportlarda 32 KB önerisine rağmen Amerika Birleşik Devletleri'nde 64 KB ve Avrupa Birliği'nde 32KB kayıt alanı kullanılmaktadır.

Biyometrik verilerin güvenliğinin sağlanması açısından bir alternatif biyometrik verinin yerine tek yönlü bir fonksiyon (*hash*) değerinin saklanmasıdır (Clarke, 2001). Bu durum merkezi veri tabanı olduğu durum için de akıllı kart teknolojisi olduğu durum için de geçerli olabilmektedir. Tek yönlü fonksiyon değerinin biyometrik veri yerine saklanması yetkisiz kişilerin erişimine de bir çözüm olabilmektedir.

Biyometrik sistemlerin her zaman başarılı olmadığı daha önceden tartışılmıştır. Yanlış kabul ve yanlış ret, tarama işleminde veya üyelik işleminde hata olabilecek hata türleridir. Göç kontrol mekanizmasında kullanılan biyometrik sistemlerin ayrı yan etkileri de olabilmektedir. Sistemin ürettiği hata dışında, seyahat belgesinin değiştirilmiş olması, kayıt ünitesinin arızalı olması veya yazılımsal hatalar da görülebilmektedir. Kişiler, biyometrik sistemlerin kendi bilgilerini yanlış okuduğunu düşündükleri durumlarda itiraz edebilmekte ve klasik yöntemlerle kontrol işlemlerinin yeniden yapılmasını talep edebilmektedir (Redpath, 2007: 33). Sınır geçiş işlemleri sırasında kişiler sorun yaşadıkları zaman bir anlamda kişilerin hakkına tecavüz edilmiş olmaktadır (Hornung, 2007: 255).

Biyometrik sistemlerin ileri teknoloji olması itibarıyla uygulayıcıların da kalifiye personel olması gerekliliği de dolaylı olarak bir dezavantaj sayılabilir. Biyometrik sistemleri kullanan personel belirli eğitimleri almak durumundadır.

Sistemin yanlış sonuç ürettiği veya sınır görevlisinin şüphe duyduğu durumlarda alternatif yöntem öngörülebilir. Alternatif yöntem, seyahat eden kişiyi ve

seyahat belgesini ayrıca klasik yöntemlerle incelemek şeklinde yapılabilir (Redpath, 2005: 16).

Seyahat eden kişi, vize veya seyahat belgesi başvurusu esnasında da sorun yaşayabilir ve sisteme kayıt yaptıramayabilir (Redpath, 2007: 33). Ayrıca, biyometrik sisteme üyelik aşamasında problem olduğu durumlarda, sınır kapısında alternatif yöntem olan klasik inceleme yapılması zorunludur. Dolayısıyla biyometrik sistemlerin kullanıldığı sınır kapılarında alternatif yöntem olan klasik inceleme mekanizması bulundurulmalıdır (JRC, 2005: 98). Bazen cihazlarda hata olabildiği gibi bazı durumlardaki kişiler için de (fiziki engeli olan kişiler veya çocuklar) biyometrik sistem başarılı bir şekilde çalışmamaktadır.

Biyometrik sistemin var olduğu sınır kapılarında dahi ikincil olarak klasik inceleme alt yapısının kurulması bir ihtiyaçtır. Sınır kapılarında alternatif yöntemin kurulması; ekstra iş gücü, zaman kaybı ve maliyet demektir. Alternatif yöntem, kişilerin haksızlığa uğramaması için hazırlanmalıdır.

Dezavantajlar sıralanırken özellikle mahremiyetin ihlali ve kişisel verilerin korunması konuları, önemi itibarıyla biyometrinin insan haklarına etkisi başlığı altında ilerleyen sayfalarda tartışılmaktadır.

4.3. İNSAN HAKLARINA ETKİSİ

Biyometrik veriler kişilerin vücut özelliği ile ilgilidir. Kişiler için en özel yerin kişinin vücudu olduğunu söyleyenler bulunmaktadır (T-PD, 2005: 6). Dolayısıyla kişinin en özel olan vücuduna ait biyometrik verilerin toplanması kişinin insan hakkıyla¹²⁴ doğrudan ilgilidir. Çünkü insan haklarının öznesi kişidir (Khanat, 2005: 76). Kişinin özel olan vücuduna ait biyometrik verilerin toplanması, bazı kişiler için önemli görülme bile, bazı kişiler parmak izinin alınmasını, yüz resminin taranmasını ve iris bilgisinin kıyaslanmasını insan onuruna yapılmış bir müdahale olarak görebilmektedirler. İnsanın vücut veya davranışsal özelliklerinin biyometrik

¹²⁴ “İnsan hakları insana sadece insan olduğu içi tanınan haklardır.” GÜNDÜZ, Aslan, (1993), Gelişmiş Batı Avrupa Ülkelerinde İnsan Haklarının Korunması: Avrupa İnsan Hakları Sözleşmesinin Sağladığı Yarı-Süpranasyonel Himaye, Türklerde İnsani Değerler ve İnsan Hakları, 3.Kitap, Türk Kültürüne Hizmet Vakfı Yayınları, İstanbul, s.25.

sistemlerde kullanılması kùltùrlere, toplumlara, kiřilere hatta zamana gùre farklı farklı deęerlendirilebilmektedir.

Biyometrik sistemlerin kiřiler, yani kullanıcılar tarafından kabul gùrmesinde önemli bir aktùr mahremiyete iliřkin konuların ön planda tutulmasıyla ilgilidir. Mahremiyete iliřkin en öncelikli konu, biyometrik sistemlerin ürettięi kiřilere ait özel biyometrik verilerdir (JRC, 2005: 37). Üretilen biyometrik verilerin iyi korunmadıęını düşünen kiřiler biyometrik sistemlere yeterince ilgi gùstermemekte ve gerekli desteęi vermemektedir.

Kiřiler biyometrik özellikli seyahat belgesine sahip deęilse veya sistem kendi bilgilerini doęru okuyamaz ise kiřinin serbestçe seyahat etme özgürlüęü etkilenmektedir. Sınır kontrollerinde ve vize işlemlerinde kullanılan biyometrik sistemler, hata durumunda kiřinin seyahat özgürlüęünü haksız olarak engelleyebilmektedir. Seyahat belgelerindeki biyometrik bilgilerin hatalı olarak okunması veya okunamaması gibi durumlar sonucu oluřan kiřinin seyahat özgürlüęünün engellenmesi durumu mahremiyetin ihlaline örnek olarak verilebilir (Redpath, 2005: 10).

Sınır kontrollerinde ve vize işlemlerinde kullanılan biyometrik sistemlerin bilgilerinin merkezi bir biyometrik veri tabanında tutulması, kiřisel verilerin gizlilięinin korunması aęısından önemli bir konudur (Redpath, 2007: 31). Merkezi veri tabanındaki biyometrik bilgiler iyi korunamaz ise sonuç kiřisel bilgilerin korunamaması olarak ortaya çıkmaktadır. Dolayısıyla kiřinin hakkı korunamamıř olmaktadır.

Biyometrik sistem kullanımının insan haklarına olumsuz etkilerine örnek olarak, mahremiyetin ihlali ve kiřisel bilgilerin korunmasındaki zafiyetler sayılabilmektedir.

4.3.1. Mahremiyet Hakkı (*Right to Privacy*)

Mahremiyet (*privacy*), net bir şekilde tanımlanmakta zorlanılan bir konudur (Kajevic, 2006: 10). Mahremiyet, kiřinin kendisiyle ilgili konulara ilgisiz bařka kiřilerin dâhil olması veya karıřması olarak ifade edilmektedir (*Subcommittee on Biometrics*, 2006: 23). Bir bařka anlatımla; mahremiyet kiřinin kiřisel bilgilerinin,

kişisel haberleşmesinin, fiziksel mevcudiyetinin ve kişisel alanının başkasının müdahalesinden korunması demektir (Redpath, 2007: 31). Crompton (2002), mahremiyeti, kişinin iletişiminin, bilgilerinin, vücudunun ve çevre alanının müdahalelere karşı korunması olarak tanımlamıştır (Crompton, 2002: 9).

Mahremiyet hakkı (*right to privacy*), uzun zamandır konuşulan ve birçok defa tanımlanan bir konudur. Bu konudaki en eski yazılardan ve en basit tanımlamalardan birisi, Samuel Warren ve Louis Brandeis'in *Harvard Law Review* dergisinde 1890 yılında yazdıkları yazıda¹²⁵ kullandıkları "Mahremiyet hakkı, yalnız kalabilme hakkıdır." ifadesidir. Yalnız kalabilme hakkı, hem fiziksel hayatta hem de bilgi ve iletişim teknolojilerinde başkalarının müdahalelerinden korunma hakkıdır.

Mahremiyet kısaca, kişinin özeli demektir. Kişinin özeli veya mahremiyeti daha çok evi olarak düşünülmeyle birlikte, artık kişiye ait kişisel bilgiler de kişiye özel mahrem bilgiler olarak kabul edilmektedir. Kajevic'e (2006) göre, mahremiyetin üç ana çalışma alanı bulunmaktadır. Bunlar: çevresel mahremiyet, kişisel (vücut) mahremiyet ve bilgi mahremiyetidir (Kajevic, 2006: 10). Crompton (2002) Kajevic (2006) tarafından ifade edilen üç alana bir alan daha eklemektedir. Crompton (2002) haberleşme mahremiyetinin, mahremiyetin çalışma alanlarına müstakilen eklenmesi gerektiğini belirtmektedir (Crompton, 2002: 9).

Günümüz dünyasındaki gelişmelere ve mahremiyetle ilgili yapılan tartışmalara bakıldığında Crompton'un 2002 yılında yaptığı önerinin daha doğru olduğu görülmektedir. Bilgi ve iletişim alanındaki baş döndürücü gelişmeler, bilgi mahremiyeti yani kişisel verilerin korunmasını ve haberleşme mahremiyeti yani haberleşme özgürlüğünü kişiler için önemli bir gündem maddesi haline getirmiştir.

Mahremiyet önemli bir kavram olmakla birlikte son dönemlerde yaşanan teknolojik gelişmeler, bilgi ve iletişim teknolojilerinde üretilen ve kullanılan bilgiler, bilgi mahremiyetinin önemini artırmaktadır (Subcommittee on Biometrics, 2006: 40). Bilgi mahremiyetinin pratikteki uygulaması kişisel verilerin korunması şeklinde olmaktadır. Biyometrik veriler kişisel veriler olarak kabul edilmektedir (Liu, 2008: 48). Böylece, biyometrik verilerin korunması bilgi mahremiyetinin önemli bir

¹²⁵ Warren, Samuel ve Brandeis, Louis, (1890), "The Right to Privacy", *Harvard Law Review*, Cilt IV 1890-91, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html, (Erişim Tarihi: 10 Ocak 2011).

uygulamasıdır. Dolayısıyla biyometrik sistemler de mahremiyet hakkı (*right to privacy*) kapsamında değerlendirilebilmektedir (Subcommittee on Biometrics, 2006: 31).

Sınır kontrolleri de bir anlamda mahremiyete müdahale olarak değerlendirilebilir. Özellikle biyometrik sistemler kullanıldığında, kişilerin resmi çekilmekte, parmak izi alınmakta ve seyahat belgelerindeki biyometrik bilgiler okunmaktadır. Bu işlemleri yapmaya devletlerin hakkı bulunmakla birlikte, yapılan bütün işlemler ölçülü bir şekilde yapılmalıdır.

Amerika Birleşik Devletleri Anayasa'sında mahremiyet kelimesi kullanılmamaktadır (Subcommittee on Biometrics, 2006: 30). Fakat Amerika Birleşik Devletleri Anayasası'nın bazı maddelerinde mahremiyetin korunmasına ilişkin hükümler bulunmaktadır. Amerika Birleşik Devletleri Yüksek Mahkemesi söz konusu maddelerden yola çıkarak kişilerin mahremiyetlerine saygı gösterilmesi hakkı olduğunu kararlarında belirtmektedir (Subcommittee on Biometrics, 2006: 30).

Amerika Birleşik Devletleri Yüksek Mahkemesi, kişilere ilişkin özel bilgilerin bilgisayar sistemlerinde veya devlet arşivlerinde çok miktarda bulundurulmasının kişilerin mahremiyetine tehlike oluşturabileceğini 1977 yılında verdiği bir kararda kabul etmiştir (Supreme Court, *Whalen v. Roe*, United States Supreme Court Reports (U.S.), 1977, Vol. 429: 589).

Mahremiyet hakkı, çeşitli bölgesel ve uluslararası sözleşmelerde korunmuştur. Bunlar; BM İnsan Hakları Evrensel Beyanname'si'nin (*Universal Declaration of Human Rights*) 12. maddesi (Redpath, 2007: 31), BM Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'nin (*International Covenant on Civil and Political Rights*) 17. maddesi (Redpath, 2007: 31) ve Avrupa İnsan Hakları Sözleşmesi'nin (*European Convention on Human Rights*) 8. maddesi gibi hükümler mevcuttur. Bunlara ilaveten, göçmenler ile ilgili hakların tanımlandığı BM Tüm Göçmen İşçilerin ve Aile Fertlerinin Haklarının Korunmasına Dair Uluslararası Sözleşme'nin 14. maddesinde (Redpath, 2007: 32) özel hayatın korunması tanımlanmaktadır.

İnsan Hakları Evrensel Beyannamesi - Madde 12

Hiç kimsenin özel yaşamına, ailesine, evine ya da yazışmasına keyfi olarak karışamaz, onuruna ve adına saldırılamaz. Herkesin, bu gibi müdahale ya da saldırılara karşı yasa tarafından korunma hakkı vardır.

Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme - Madde 17

1. Hiç kimsenin özel hayatına, ailesine, evine ya da haberleşmesine keyfi ya da yasadışı olarak müdahale edilemez; hiç kimsenin şeref ve itibarına yasal olmayan tecavüzlerde bulunulamaz.

2. Herkesin, bu gibi müdahalelere ya da tecavüzlere karşı yasalarca korunma hakkı vardır.

Avrupa İnsan Hakları Sözleşmesi (AİHS) - Madde 8 Özel Hayatın ve Aile Hayatının Korunması

1. Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda, zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir.

AİHS Madde 8/2 mahremiyete müdahalenin istisnasını düzenlemektedir. Devletler mahremiyete, gerekli durumlarda, dengeli bir şekilde, kanunla tanımlanmış hallerde, ölçülü ve ayrımcılığa kaçmadan müdahale edebilirler.

BM Tüm Göçmen İşçilerin ve Aile Fertlerinin Haklarının Korunmasına Dair Uluslararası Sözleşme - 14. Madde

Tüm Göçmen İşçilerin ve Aile Fertlerinin Haklarının Korunmasına Dair Uluslararası Sözleşme (*the UN International Convention on the Protection of the*

Rights of All Migrant Workers and Their Families - ICMW) 2003 yılında yürürlüğe girmiştir (Thomas, 2005: 2). Sözleşmenin 14. maddesi ile düzenli ve düzensiz göçmenlerin ikisi için de mahremiyet hakkı bulunduğu kabul edilmektedir.

On dördüncü madde de öngörülenler: Hiçbir göçmen işçinin veya aile ferdinin özel hayatına, ailesine, konutuna, mektuplaşmasına veya diğer şekilde haberleşmesine keyfî ve gayri kanunî müdahalelerde bulunulamaz; şeref ve haysiyetlerine gayri kanunî saldırılar yapılamaz. Her bir göçmen işçi ve aile ferdi bu tür saldırılara ve müdahalelere karşı kanunun öngördüğü korumadan yararlanma hakkına sahiptir.

4.3.2. Kişisel Verilerin Korunması

Son dönemlerde bilgi ve iletişim teknolojilerinde yaşanan gelişmeler mahremiyetin önemli bir uygulama alanı olan bilgi mahremiyetinin daha çok gündemde olması sonucunu doğurmuştur (Subcommittee on Biometrics, 2006: 40). Bilgi mahremiyeti ise kişisel verilerin korunması ile sağlanmaktadır. Biyometrik veriler kişisel veriler olarak kabul edilmektedir (Liu, 2008: 48). Böylece, biyometrik verilerin korunması bilgi mahremiyetinin önemli bir uygulaması olmaktadır. Biyometrik sistemlerin dezavantajlarının doğurduğu endişeyi önleme yöntemlerinden birisi mahremiyetin korunması ve kişisel verilerin korunması konusunda yapılan düzenlemelerdir (JRC, 2005: 98).

Ulusal ve uluslararası düzenlemelerde kişilerin hakkı olarak öngörülen mahremiyet hakkının korunmasına uygulamada bir örnek; kişiye ait kişisel bilgilerin korunmasıyla olmaktadır. Mahremiyet hakkı ve bilgilerin gizliliği, kişisel verilerin korunmasıyla sağlanmaktadır (Thomas, 2005: 378). Avrupa Birliği'nin 95/46/AT sayılı kişisel veriler yönergesinin amacı olan 1.nci maddesindeki¹²⁶ “kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini koruyacaktır” ifadesiyle Avrupa Birliği üyesi devletler, temel hak ve özgürlüklerden olan mahremiyet hakkını kişisel verileri koruyarak gerçekleştireceğini kabul etmektedir. Kişilere ait kişisel bilgiler, mahrem yani özel

¹²⁶ 95/46/AT sayılı ve “Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması” isimli Yönergenin (1)'nci maddesi, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT>, (Erişim Tarihi: 15 Ekim 2011).

bilgilerdir. Biyometrik sistemlerde kişilere ait özel kişisel bilgiler yoğun olarak bulunmaktadır.

Sınır kontrolleri ve vize uygulamalarında kişisel verilerin gizliliğinin korunmasında biyometrik sistemlerle beraber kullanılan merkezi büyük biyometrik veri tabanları da değerlendirilmelidir (Redpath, 2007: 31).

Diğer yandan, kişisel veri düzenlemelerinin biyometrik verileri kapsayıp kapsamadığı uzunca zamandır tartışılan bir konudur. Avrupa Birliği kişisel veri düzenlemesinde¹²⁷ biyometri teriminin bulunmaması (Hert, 2005: 13) biyometrik veri kişisel veri değildir diye düşünenlerin kullanabileceği bir argümandır.

Corien Prins biyometri teknolojisinin kişinin mahremiyet hakkıyla olan ilişkisini inceleyen ilk kişidir (Hert, 2005: 10). Prins biyometrik sistemlerin temel haklarla olan ilişkisini incelemiştir. Prins, Avrupa Birliği kişisel veri düzenlemesinin bazı tür biyometrik verileri kapsamadığını düşünmektedir (Hert, 2005: 16). Prins akıllı kartlardaki biyometrik veri şablonlarının tek başına kişiyi tanımlayamadığından ve kişiye ilişkin biyometrik veriye dönüştürülemediğinden dolayı 1998 tarihli çalışmasında¹²⁸ biyometrik verilerin kişisel veri olarak kabul edilemeyeceğini belirtmektedir. Bu yüzden Prins, her türlü biyometrik verinin, AİHS'nin 8. maddesi kapsamında biyometrik veri olarak kabul edilmemesi gerektiğini¹²⁹ iddia etmektedir.

Prins, iddiasını biyometrik şablonun kişiyi tanımlayan bir veriye dönüştürülemediği bilgisine dayandırmaktadır. Fakat biyometrik şablonun kişiyi tanımlayan bir veriye dönüştürülüp dönüştürülemeyeceği şu an için belirsizdir. Fakat teknolojiye göre bu durumun yeniden değerlendirilmesi gerekebilir. Gelişen teknoloji sonucu biyometrik şablon kişiyi tanımlayan bir veri olabilir.

Corien Prins'in yorumları, 11 Eylül 2001 terör olayından önce olması, teknolojinin 1998 yılındaki durumu itibarıyla yapılmış olması ve Avrupa düzenlemeleri bağlamında yapılan ilk çalışma olması göz önünde bulundurularak değerlendirilmelidir.

Prins'in yorumlarına farklı bir şekilde destek Anton Alterman'dan gelmektedir. Anton Alterman (2003), biyometrik verilerin kişilerin mahremiyeti ile

¹²⁷ AB kişisel veri düzenlemesi tabiri ile 95/46 sayılı yönerge kastedilmektedir.

¹²⁸ Prins'ten akt. Hert, 2005: 16.

¹²⁹ a.g.e., s.16.

ilişkisi konusunda çalışma yapan başka bir yazardır (Hert, 2005: 16). Alterman'ın (2003) çalışması sonucu vardığı düşünce, biyometri teknolojisinin kişilere mahremiyet problemi oluşturmamıştır (Alterman, 2003: 140). Biyometrik verilerin sadece kişilerle doğrudan irtibat kurmak, yani kişileri tanımlama imkânı olmamasından dolayı Alterman (2003) mahremiyet ve kişisel veriler açısından özel bir sorun olmadığını düşünmektedir (Alterman, 2003: 140). Çünkü bir bilginin kişisel bilgi olabilmesi için o bilginin her zaman ve her ortamda doğru olarak o kişiyi tanımlayabiliyor olması gerekmektedir (Crompton, 2002: 14). Bununla birlikte, teknolojiye gelişmeler biyometrik verilerin kişilerle daha doğru bir şekilde irtibat kurmaları sürecini doğurabileceğinden bu değerlendirmenin günümüz şartları açısından tekrar gözden geçirilmesi gerekmektedir.

Avrupa Birliği kişisel veri düzenlemesinde, biyometri terimi bulunmasa bile Paul De Hert (2005) Avrupa Birliği kişisel veri düzenlemesinde “bir kişiyle ilgili görüntü ve ses yakalanması, iletilmesi, kaydedilmesi, düzenlenmesi, kaydedilmesi ve saklanması (*capturing, transmitting, manipulating, recording, storing or communicating sound and image data relating to natural persons*)” ifadesinin anlam olarak biyometriyi kapsadığını düşünmektedir (Hert, 2005, ss:13–14).

Paul de Hert, biyometrik sistemlerde kullanılan verilerin kişisel bilgilerin korunması düzenlemeleri kapsamında olduğunu belirtmektedir (Hert, 2005: 13). Biyometrik veriler, hem içeriğinden hem de kullanım amacından dolayı kişisel veridir (Subcommittee on Biometrics, 2006: 36). Biyometrik veriler, her zaman ve şartta bir kişiyi net olarak tanımlamasa bile verilerin türü ve toplanma amaçları kişisel veri tanımına girmektedir (Subcommittee on Biometrics, 2006: 36).

Başbakanlık tarafından TBMM'ye 2008¹³⁰ yılında sevk edilen, kişisel veriler kanun tasarısının kişisel veri tanımına bakıldığında ve tanım değerlendirildiğinde biyometrik verilerin kişisel veriler olarak kabul edilebileceği ortaya çıkmaktadır.

Avrupa Birliği kişisel veri düzenlemesinde biyometrik veri tabiri bulunmamakla birlikte düzenlemelerin ruhunda olan bilgi toplumundaki gelişmeler kapsamında “gerçek bir kişiye ait ses ve resim verisinin yakalanması, iletilmesi,

¹³⁰ Başbakanlık'tan TBMM'ye 22 Nisan 2008 tarihinde gönderilen “Kişisel Verilerin Korunması Kanununu Tasarısı” Tanımlar kenar başlıklı madde 3 fıkra (ç)'de, kişisel veri, “Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgileri” ifade eder diye tanımlanmaktadır.

değiştirilmesi, kaydedilmesi, depolanması veya haberleşmesi"¹³¹ 95/46/AT sayılı kişisel veriler yönergesi uyarınca biyometrik veriler kişisel veri olarak değerlendirilmektedir. Kişisel veri tüzüğü'nün 2. maddesinin a fıkrasında,¹³² "kişisel veri"; "fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye ("veri öznesi") ilişkin herhangi bir bilgiyi kastedecektir" şeklinde tanımlanmaktadır.

Amerika Birleşik Devletleri Ulusal Bilim ve Teknoloji Konseyi'nin (*National Science and Technology Council-NSTC*) biyometri konusundaki alt çalışma komisyonu 2006 yılında hazırladığı raporda¹³³ biyometrik verilerin kişisel veri olduğu fikrine katılmıştır. Rapora göre, biyometrik bilgilerin kişileri her zaman doğru bir şekilde belirleyemediği bilinse bile genel olarak biyometrik bilgiler kişisel veri olarak kabul edilmektedir (Subcommittee on Biometrics, 2006: 35).

Biyometrik verilerin kişisel veri olarak korunması için yapılması gerekenler vardır. Öncelikle kişisel veri düzenlemelerinde değişiklik yapıp biyometrik verilerin de düzenleme kapsamına açık bir şekilde alınması sağlanmalıdır (Subcommittee on Biometrics, 2006: 76–86). Çünkü Avrupa Birliği kişisel veri düzenlemeleri açıkça biyometrik verileri kapsamamaktadır (JRC, 2005: 99). Ayrıca, ülkeler kişisel veri otoritelerinin yetki kapsamına biyometrik verilerin de alınmasını sağlanmalıdır.

Biyometrik sistemler sayısal veri üretmektedir (JRC, 2005: 37). Üretilen sayısal veriler kişilere özel verilerdir. Kişisel verilerin korunması açısından bu duruma bakıldığında cevaplanması gereken standart sorular bulunmaktadır. Örneğin, hangi veriler kaydedilmektedir? Veriler nerede ve nasıl kaydedilmektedir? Merkezi bir veri tabanındaki veya akıllı kartlardaki, verilere kimler hangi amaçlarla erişebilmektedir? şeklinde sorular akla gelmektedir. Örnek verilen ve ilgili diğer

¹³¹ 95/46/AT sayılı ve "Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması" isimli Yönergenin (14)'nci paragrafı, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT>, (Erişim Tarihi: 15 Ekim 2011).

¹³² 95/46/AT sayılı ve "Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması" isimli Yönergenin(2)'nci maddesinin a fıkrasında, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT>, (Erişim Tarihi: 15 Ekim 2011).

¹³³ Subcommittee on Biometrics, (2006), Privacy & Biometrics: Building a Conceptual Foundation, National Science and Technology Council (NSTC).

soruların cevapları biyometri türüne ve biyometrik sistemin yapısına göre ilgili mevzuat kapsamında cevaplandırılmalıdır.

Kişisel verilerin korunması açısından en zayıf düzenlemeler, muhtemelen Amerika Birleşik Devletleri düzenlemeleridir (Thomas, 2005: 391). Amerika Birleşik Devletleri'nde kişisel verilerin korunması konusunda genel düzenleme yerine olay bazlı ve endüstrinin öz düzenlemeleri tercih edilmektedir. Amerika Birleşik Devletleri, OECD kişisel verilerin korunması ilkelerine imza atan ülkelerden birisi olmasına rağmen o ilkeleri kanun olarak düzenlememiştir (Thomas, 2005: 391).

Avrupa Birliği'nde, Amsterdam Antlaşmasından itibaren, biyometrik sistemler de dâhil olmak üzere, bütün bilgi değişim platformlarında kaydedilen bilgilerin kişisel verilerin korunması şartlarına uyulması gerektiği bildirilmiştir. Bütün düzenlemelerde, kaydedilen kişisel verilerin 95/46/AT sayılı kişisel verilerin korunması yönergesine uygun olması ve Avrupa Birliği Veri Koruma Gözetmeni (*European Data Protection Supervisor-EDPS*) tarafından veri güvenliği açısından korunmasının denetlenmesi öngörülmektedir (Thomas, 2005: 391).

Avrupa Birliği kişisel veriler düzenlemeleri, biyometrik sistemler tarafından üretilen ve kullanılan kişisel veriler için yeterli düzeyde koruma öngörmemektedir (Kajevic, 2006: 24). Avrupa Birliği biyometrik pasaport düzenlemesi,¹³⁴bu kapsamda toplanan kişisel bilgilerin Avrupa Birliği kişisel verilerin korunması düzenlemelerine¹³⁵ uygun olarak korunmasını ve güvenliğinin sağlanmasını öngörmektedir. Biyometrik pasaport düzenlemesini¹³⁶ yapan Avrupa Komisyonu bu sistemlerde kullanılan biyometrik verilerin yeterli düzeyde ve kurallara uygun şekilde korunması için kişisel veri düzenlemelerinde de gerekli güncellemeleri kendisi yapmalıdır.

Avrupa Birliği kişisel veriler düzenlemeleri, insan hakları düzenlemelerindeki konuların hepsini yeterli düzeyde karşılamadığı ifade edilmektedir (Hert, 2005: 12). Avrupa Birliği kişisel veri düzenlemesi metninin temel eksiği metnin teknik bir

¹³⁴ EC 444/2009.

¹³⁵ 95/46/AT sayılı ve “Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması” isimli Yönerge, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT>, (Erişim Tarihi: 15 Ekim 2011).

¹³⁶ EC 2252/2004 ve EC 444/2009 sayılı düzenlemeler.

metin olmaması ve kapsamın belirlenmesi için birçok detay soruya (*processing* teriminden ne anlaşıyor, anonim veri ne demektir gibi) cevap bulunması gerekliliğidir (Hert, 2005:15–16). Düzenlemedeki bir başka eksiklik, hassas kişisel veri korunması konusudur. Direktifin 8. maddesine göre kişilerin ırk, etnik köken, politik görüş, dini görüş, grup üyeliği ve sağlık ile cinsel yönelim konusundaki verileri işlenememektedir (95/46 madde 8.1). Diğer yandan parmak izi ve yüz tanıma teknikleri, kişilerin ırk ve etnik kökeni konusunda bilgi ortaya çıkartabilmektedir (Prins'ten akt. Hert, 2005: 14). Örneğin, iris tarama sonucu elde edilen bilgiler kişinin sağlığı hakkında bilgi içerebilmektedir (Hornung, 2007: 249). Biyometrik verilerin kişisel veri olarak AİHS kapsamında olup olmadığı ayrı bir tartışma konusudur. AİHM çeşitli davalarda kişisel verilerin korunmasının AİHS 8. madde kapsamında olduğunu kabul etse bile her türlü kişisel verinin işlenmesinin AİHM tarafından korunmadığı bilinmektedir (Busch, 2006: 23). AİHM bazı kişisel verileri gündemine alırken bazı kişisel verilerin de AİHS kapsamı dışında olduğu görüşündedir. Mahkeme, işleme tabi tutulan verilerden kişinin özel hayatıyla ilgili olanlarının AİHS kapsamında olduğunu, kişinin özel hayatıyla ilgisi olmayan verilerin AİHS kapsamı dışında olduğu görüşündedir (Busch, 2006: 24).

Avrupa Birliği'nde biyometrik sistemlerde kişisel verilerin korunması kurallarının belirlenmesi ve uygulamaya önerilerde bulunmak üzere bazı projeler yapılmıştır. Yapılan projelerden bazıları FIDIS¹³⁷, BITE¹³⁸ ve PRIME¹³⁹ olarak sayılabilir (JRC, 2008: 83; Subcommittee on Biometrics, 2002: 83).

Avrupa'da üretilen biyometrik ürünlerin kabiliyetlerini test eden Avrupa Birliği Komisyonu tarafından finanse edilen bir başka proje *BioTesting Europe* projesidir (JRC, 2008: 87). Proje, Avrupa'da çok fazla sayıda ihtiyaç duyulan ve her geçen gün kullanımı daha da yaygınlaşan biyometrik ürünlerin kullanım kurallarının belirlenmesi ve test işlemlerinin Avrupa içinde yapılması için gerekli olan adımların belirlenmesini öngörmüştür (JRC, 2008: 87). Proje kapsamında Avrupa'daki birçok paydaşın görüşlerine başvurulmuştur. Örneğin, biyometrik sistem üreticileri, ürün test laboratuvarları, bağımsız uzmanlar, sınır görevlileri ve son kullanıcılar gibi çeşitli paydaşlar ile görüşülmüş, mülakat yapılmış ve sorular sorulmuştur (JRC,

¹³⁷ FIDIS: Future of Identity in the Information Society-fidis.net.

¹³⁸ BITE: Biometric Identification Technology Ethics.

¹³⁹ PRIME: Privacy and Identity Management for Europe.

2008: 87). Proje sonuçları 2008 yılı Haziran ayında bir raporla yayınlanmıştır. Proje sonuçlarında, özetle kullanımı yaygınlaşan biyometrik sistemlerin kullanım kurallarının ve test koşullarının Amerika Birleşik Devletleri etkisiyle oluşturulduğu ve Avrupa ihtiyaçlarının ihmal edildiği belirtilmektedir (JRC, 2008: 87).

Bütün bu tartışmalar, biyometrik verilerin türlere göre kişisel veri olup olmadığının belirlenmesi gibi bir noktaya kaymaktadır. Örneğin, Paul De Hert'in (2005) de belirttiği gibi kişilerin fiziki özelliklerini içeren biyometrik veriler kişisel veri, davranışsal özelliklerini içeren biyometrik veriler kişisel veri değildir gibi bir sonuç çıkabilmektedir (Hert, 2005: 17).

Kişisel verileri en yoğun ve kapsamlı biçimde işleyen kurum olan devletin, özel sektöre nispetle kişisel verilerin korunması konusunda daha fazla hassasiyet göstermesi gerekmektedir. Devletler verileri özellikle de kişisel verileri işlerken, 21. yüzyıldaki misyona uygun ancak belirli bir takım değerlere saygılı olarak davranmaları gerekmektedir.

Devletlerin kişisel verilerin kullanımına ilişkin uymaları gereken ilke ve kurallar uluslararası örgütler tarafından belirlenmiştir. OECD¹⁴⁰, Avrupa Konseyi¹⁴¹, BM¹⁴² ve AB¹⁴³ gibi kuruluşlar tarafından kişisel verilerin korunması kural ve uygulamaları çeşitli tarihlerde belirlenmiştir (Hert, 2005: 13). Kişisel verilerin korunması konusunda uluslararası örgütlerin belirlediği kurallar, ülkeler tarafından kendi ulusal düzenlemeleri hazırlanırken kaynak olarak kullanılmaktadır. Avrupa'da kişisel verilerin ülkeler arasında değişimini öngören kurallar ilk defa Ekonomik Kalkınma ve İşbirliği Örgütü OECD tarafından 1980 yılında belirlenmiştir (Subcommittee on Biometrics, 2002: 33). OECD kuralları, ülkelerin veri değişimini etkin bir şekilde yapabilmeleri için kişisel verilerin korunması düzenlemeleri arasında bir uyum olmasını vurgulamaktadır.

¹⁴⁰ OECD Kişisel Veriler Kılavuz İlkeleri, 23 Eylül 1980, Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, Paris, OECD, 1980, 9–12, *International Legal Materials*, 1981, I, 317.

¹⁴¹ AK 108 Sayılı Sözleşme, Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, Ocak 28, 1981, European Treaty Series, no. 108, *International Legal Materials*, 1981, I, 422.

¹⁴² BM Kişisel Veriler Kılavuz İlkeleri, Guidelines concerning computerized personal data files, 14 Aralık 1990.

¹⁴³ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, Official Journal of the European Communities, L 281, 23 November 1995, 31-50 (further cited as "Data Protection Directive").

Türkiye'nin de üyesi bulunduğu Avrupa Konseyi, Kişisel Verilerin Gizliliğinin Korunmasına ilişkin 108 sayılı sözleşmeyi 28 Ocak 1981 yılında onaylamıştır (*Treaty 108: Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, January 28, 1981, European Treaty Series, no. 108; International Legal Materials, 1981, I, 422*).

OECD ve Avrupa Konseyi gibi Birleşmiş Milletler de otomatik olarak işleme tabi tutulan kişisel verilerin korunması konusunda uyulacak minimum kuralları belirlemişlerdir (Redpath, 2007: 31).

Bilgisayar ve bilgisayar sistemlerinde üretilen veya kullanılan kişisel verilerin korunmasına ilişkin uluslararası örgütlere ait tavsiye kuralları ilerleyen sayfalarda detaylı olarak incelenmektedir.

4.3.2.1. Kişisel Veri Düzenlemeleri

Uluslararası örgütler bilgisayar sistemleri tarafından otomatik olarak işleme tabi tutulan kişisel verilerin kullanımına ilişkin genel ilke ve kuralları belirlemişlerdir. Belirlenen genel kurallar, elde edilen kişisel verilerin ancak belirli ve yasal bir sebeple toplanabileceği, bildirilen maksat haricinde kullanılamayacağı, güvenli bir şekilde saklanacağı ve güncel olması gerektiği gibi konularla ilgilidir (Thomas, 2005: 391). Bu bölümde, bu kuralların neler olduğu ve biyometrik sistemler için nasıl uygulanabileceği tartışılmaktadır.

Kişisel nitelikli verilerin korunması, Avrupa Konseyi'nce 28 Ocak 1981 tarihli "Kişisel Verilerin Otomatik İşlemine Dayanan Bireylerin Korunmasıyla İlgili Sözleşmesi" adlı 108 Sayılı Avrupa Konseyi Sözleşmesi'yle düzenlenmiştir.

24 Ekim 1995 tarihli "Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafikğine İlişkin" Avrupa Birliği Yönergesinde (95/46/AT), kişisel veriler konusu Avrupa Birliği düzeyinde ilk defa 1995 yılında düzenlenmiştir.

Avrupa Birliđi 95/46/AT Sayılı Kişisel Veri Yönergesi

24 Ekim 1995 tarihli, “Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiğine İlişkin Yönergesi”nde (95/46/AT) öngörülen düzenlemelerin özeti aşağıdadır. Bu Yönergenin temel amacı 1. maddede belirtildiğı üzere, kişisel verilerin işlenmesi sırasında kişi hak ve özgürlüklerinin korunmasını sağlamak ve üye devletlerarasında serbest veri trafiğini temin etmektir.

Yönergenin 6. maddesinde veri koruma ilkeleri belirtilmiştir. Bunlar;

- Kişisel verilerin işlenmesi yasal olmalıdır. Yani veri öznesinin rızası olmalıdır. Ayrıca öznenin kişisel hakları ihlal edilmemelidir.
- Veriler, dürüstlük kuralına uygun olarak ve hukuka uygun amaçlar için işlenmelidir.
- Veriler elde edildikleri amaç için kullanılmalıdır.
- Veriler ihtiyacı karşılayacak kadar toplanmalıdır.
- Veriler güvenli bir şekilde saklanmalı ve kişisel verilerin işlenmesi güvenli bir şekilde yapılmalıdır.
- Veriler amaç ortadan kalkınca imha edilmelidir.
- Veri öznesi bilgilendirme, hakkındaki bilgilere erişme ve bilgilerin silinmesi ve düzeltilmesi haklarına sahiptir.

Yönergenin 2. maddesinde, bazı temel kavramların tanımı yapılmıştır. Üçüncü maddede Yönerge hükümlerinin gerçek kişiler için geçerli olduğu belirtilmiştir. Yönergenin 28. maddesinde, bağımsız denetleme otoritesinin kurulması öngörülmüştür. Bu kurum hükümetten talimat almamalı, kendi bütçesi ve kendi personeli olmalıdır. Ayrıca Yönerge kişisel verilerin korunması sırasında kişilerin korunmasını sağlamak için bağımsız ve danışma niteliğı olan bir çalışma grubunun kurulmasını öngörmüştür. Önemli diğeri bir nokta da, kişisel verilerin üçüncü ülkelere transferi, o ülkede aynı seviyede veri koruma düzenlemesi bulunmuyorsa yapılmaması şeklindedir.

28.01.1981 tarih ve 108 sayılı “Kişisel Verilerin Elektronik Ortamda İşlenmesi Bağlamında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi”

Kişisel nitelikli verilerin korunması, Avrupa Konseyi’nce 28 Ocak 1981 tarihli "Kişisel Verilerin Otomatik İşlemine Dayanan Bireylerin Korunmasıyla İlgili Sözleşmesi" adlı 108 Sayılı Avrupa Konseyi Sözleşmesi’yle düzenlenmiştir. Özel hayata saygı değerlerinin ve kişiler arası sınırsız bilgi akışının yeniden yapılandırılması çerçevesinde imzalanan Sözleşme kişisel verilerle ilgili başlıca konuları içermekte ve bilgilerin otomatik işleme tabi tutulmasını düzenlemektedir.

Avrupa Konseyi 108 sayılı sözleşmesi, kişisel verilerin korunmasıyla ilgili olarak uluslararası alanda ilk bağlayıcı belgedir. Türkiye bu sözleşmeyi imzalamış ama onaylamamıştır. Bu sözleşmenin Türkiye tarafından onaylanması ve yürürlüğe girmesi için Kişisel Verilerin Korunması Kanunu’nun kabul edilmesinin önemi büyüktür. Sözleşmenin 4. maddesinde, taraflarca verilerin korunmasına ilişkin ilkelere işlerlik kazandırılması için gerekli tedbirlerin en geç Sözleşmenin kendileri bakımından yürürlüğe girdiği tarihte almaları öngörülmüştür. Böylece Sözleşmenin aradığı bu yükümlülük, Kişisel Verilerin Korunması Kanununun kabul edilmesiyle yerine getirilmiş olacaktır.

Bu sözleşmede de verilerin niteliğine ilişkin bir takım ilkeler öngörülmüştür:

- Kişisel veriler, meşru ve yasal yoldan elde edilmeli ve işleme tabi tutulmalıdır.
- Kişisel veriler belli ve elverişli olmalı ve kaydedildikleri amaca göre aşırı olmamalıdır.
- Kişisel veriler doğru ve güncellenmiş olmalı ve ilgili kişilerin kimliklerini belirtecek bir biçimde ve kaydedildikleri nihai amaç için gerekli görülen süreyi aşmayacak şekilde muhafaza edilmelidir.

Aslında veri koruması Türkiye’nin gündemine 1981 yılında imzalanan “Kişisel Verilerin Otomatik Olarak İşlenmesine İlişkin Olarak Bireylerin Korunması Hakkındaki 1981 tarihli Avrupa Konseyi Sözleşmesi” ile girmiştir. Ancak imza tarihinden itibaren 2012 yılı Nisan ayına kadar Türkiye söz konusu Sözleşmeyi onaylamadığı gibi, Avrupa Birliği Direktifleri doğrultusunda da veri korumasına ilişkin olarak iç hukukta herhangi bir yasal düzenleme yapmamıştır. Bu alanda

birçok yasalaştırma denemesi yapılmasına rağmen, kişisel verilerin korunması konusunda Türkiye’de dikkate değer herhangi bir gelişme 2012 yılı Nisan ayına kadar yaşanmamıştır. Kişisel verilerin korunması konusunda bir düzenleme yapılması kamuoyunun da önemle beklediği bir konudur.

Avrupa Konseyi Bakanlar Komitesi, biyometrik veri kullanımının (parmak izi, iris tanıma, yüz tanıma, el geometrisi, vb.) veri koruma ilkelerine etkisi üzerine bir rapor hazırlamak üzere Kişisel Verilerin Otomatik Olarak İşlenmesi Konusunda Bireylerin Korunması (T-PD) Danışma Grubu’na¹⁴⁴ 2003 yılında görev vermiştir (T-PD, 2005: 1). Bu kapsamda Veri Koruma Proje Grubu (CJ-PD), uzmanlara bir rapor hazırlatmıştır. Danışma Grubu (T-PD), biyometri konusunda sürmekte olan tartışmalara ve uluslararası örgütler tarafından yürütülen projelere katkıda bulunmak amacıyla hazırlanan raporu, 2-4 Şubat 2005 tarihindeki 21. toplantısında kamuoyuyla paylaşmıştır (T-PD, 2005: 1).

Uzmanlar tarafından hazırlanan rapora göre, Avrupa Konseyi 108 Sayılı Sözleşmesi hangi kişisel verilerin işlenebileceği veya işlenemeyeceği sorusuna basit bir cevap vermemektedir (T-PD, 2005: 3). Uzmanlar, 108 sayılı sözleşmenin kişisel verilerin otomatik olarak işleme tabi tutulması kavramının bilinmediği bir tarihte hazırlanmasına rağmen genel olarak bütün durumlara uygulanabilecek sadelikte hazırlandığını belirtmektedir. Rapor hazırlanırken göz önünde bulundurulmuş diğer düzenlemeler, Polis Sektöründe Kişisel Verilerin Kullanımını Düzenleyen 17 Eylül 1987 tarihli Tavsiye No R(87) 15 ve Değerlendirme Raporları¹⁴⁵ ile Akıllı Kartlar Konusunda Kişisel Verilerin Korunması İçin 2004 tarihli İlkeler Rehberliği¹⁴⁶ isimli düzenlemelerdir.

Veri Koruma Proje Grubu (CJ-PD) himayesinde hazırlanan raporda sunulan öneriler ise (T-PD, 2005, ss:22–23):

- Biyometrik veri insan vücudundan alınan özel bir kategori olarak kabule dilmelidir. Biyometrik özellikler yaşlanma, hastalık veya cerrahi müdahale ile bozulabilmekle birlikte genel olarak hayat boyunca değişmez.

¹⁴⁴ Sözleşmeyle ilgili görüşler vermek üzere Danışma Grubu kurulmuştur.

¹⁴⁵ Polis sektöründe kullanılan kişisel verilerin düzenlenmesine ilişkin (87) 15 sayılı tavsiye (17 Eylül 1987).

¹⁴⁶ Akıllı kartlarda kullanılan kişisel verilerin korunmasına ilişkin kılavuz ilkeler (2004).

- Biyometrik sistemler hakkında deęerlendirmede bulunurken, insanın özel hayatına daha az mdahale eden alternatiflerinin olup olmadıęına bakılmalıdır.
- Biyometri sadece kullanım kolaylıęından dolayı seilmemelidir.
- Biyometrik sistemler tarafından retilen veriler sadece belirli, aık ve meşru amalar iin işlenmelidir.
- İşlenen biyometrik veriler ilgili ve yeterli olmalıdır. İhtiyatan fazla veri işlenmemelidir.
- Biyometrik veriler retilirken kişilere sistemin amacı hakkında bilgi verilmelidir.
- Kişilerin kendilerine ait sistemlere erişim hakkı olmalıdır.
- Biyometrik sistemler ve biyometrik verilerle ilgili baęımsız denetim sistemleri teşvik edilmelidir.

4.3.2.2. Kişisel Veri İlkeleri

Kişisel verilerin korunması konusunda dzenlemelere rehber olmak veya uygulamaya yn vermek zere uluslararası kuruluşlar tarafından bazı ilkeler belirlenmiştir. İlk olarak Ekonomik Kalkınma ve İşbirlięi Örgt OECD tarafından kişisel verilerin korunmasında uyulması gereken ilkeler 1980 yılında “Kişisel Verilerin Sınıraşan Trafięi ve Verilerin Korunmasına İlişkin Kılavuz İlkeler” ismi altında belirlenmiştir. Daha sonradan 1990 yılında Birleşmiş Milletler Genel Asamblesi, “Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Ynlendirici İlkeler” ismiyle kişisel verilerin korunması ilkelerini ayrıntılandırmıştır.

Ekonomik İşbirlięi ve Kalkınma Örgt OECD, 23 Eylül 1980 tarihli “Kişisel Verilerin Sınıraşan Trafięi ve Verilerin Korunmasına İlişkin Kılavuz İlkeler”¹⁴⁷ isimli belgesiyle, uluslararası dzeyde kişisel verilerin korunması çerevesinde ilk defa aşıęıdaki sekiz ilkeyi belirlemiştir:

¹⁴⁷ OECD, 2004: 7; Redpath, 2005: 12.

- **Veri Toplamasının sınırlı olması ilkesi:** Bu ilkeye göre, kişisel verilerin toplanmasına sınır getirilmelidir. Kişisel verilerin toplanması, sadece hukuka uygun olarak dürüst araçlarla, gerektiğinde veri süjesinin rızası veya bilgisi dâhilinde gerçekleşmelidir.
- **Veri Kalitesi İlkesi:** Kişisel veriler amacına uygun olmalı ve bu amaç için gerekli ölçüde, tam ve güncel olmalıdır.
- **Amacın belli olması ilkesi:** Kişisel verilerin toplandığı amaç en geç verilerin toplanma anında belirlenmiş olmalıdır.
- **Kullanmanın sınırlı olması ilkesi:** Bu ilkeye göre kişisel veriler, ifşa edilemez, emre amade halde tutulamaz.
- **Veri güvenliği ilkesi:** Bu ilkeye göre kişisel veriler, kaybolma, yetkisiz kişiler tarafından ulaşılma, tahrip edilme, kullanılma, değiştirilme veya ifşa edilme gibi rizikolara karşı uygun güvenlik önlemleri vasıtasıyla güvence altına alınmalıdır.
- **Açıklık ilkesi:** Bu ilkeye göre kişisel verilere ilişkin olarak, işlemler ve önlemler genel olarak açıklık politikası çerçevesinde gerçekleştirilmelidir.
- **Bireyin Katılımı İlkesi:** Bireyin katılım hakkı çerçevesinde birey her şeyden önce esas veri sorumlusu vasıtasıyla ya da başka bir usulle kendisini ilgilendiren verilerin mevcut olup olmadığının onaylanmasını talep hakkına sahiptir.
- **Hesap Verilebilirlik İlkesi:** Esas veri sorumlusu yukarıdaki ilkelerin hayata geçirilebilmesi için gerekli önlemlere riayet etmesi bakımından hesap verebilir durumda olmak zorundadır.

1990 yılında Birleşmiş Milletler Genel Asamblesi Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler adını taşıyan belgede bu ilkeleri öncelikli olarak ayrıntılandırmıştır. Aşağıda sözü edilen ilkelerin kısa bir açıklaması verilmektedir:

- **Yasallık ve Dürüstlük:** Kişisel veriler, kanuna aykırı ve dürüst olmayan yollarla toplanmamalı ayrıca toplanış amacına, temel haklarla ve özgürlüklerle ilgili ilkelere aykırı olarak kullanılmamalıdır.
- **Doğruluk:** Toplanan verilerin doğruluğu kontrol edilmelidir. Bu verilerin doğru ve eksiksiz olarak saklandığını kontrol etmek ve güncelliğini sağlamak

için saklandığı süre zarfında bu veriler, düzenli olarak kontrole tabi tutulmalıdır.

- Amacın Belirli ve Haklı Olması: Kişisel verilerin hangi haklı amaçla toplandığı başlangıçta kesin olarak belirlenmeli ve bu amaç bütün ilgililere açık olarak bildirilmelidir.
- İlgili Kişilerin Erişme Hakkı: Kişisel veri ile ilgili kişi kimliğini kanıtlamak koşulu ile kendisi hakkında toplanan bilgilerin ne gibi bir işleme tabi tutulduğunu öğrenebilmeli ve bu verilerin anlaşılabilir biçimdeki bir örneğini aşırı bir masraf ve zaman kaybı olmadan elde edebilmelidir.
- Ayrımcılıktan Kaçınma: Kişinin etnik kökeni, ırkı, cinsel yaşamı, dini veya felsefi inançları gibi duyarlılık konularla ilgili bilgiler ancak yasanın izin verdiği haklı ve gerekli durumlarda toplanmalıdır.
- İstisna Koyma Yetkisi: Görevli makamlara, ulusal güvenliği, kamu düzenini, halk sağlığını, genel ahlakı korumak veya diğer kişilerin hak ve özgürlüklerine zarar vermemek amacıyla Yasallık ve Dürüstlük, Doğruluk, Amacın Belirli ve Haklı Olması, İlgili Kişilerin Erişme Hakkı ilkeleri ile ilgili önlemlerden ayrılma yetkisi tanınabilir. Ancak bu yetkinin kapsamı ve sınırları kanunda açıkça belirlenmelidir. Ayrımcılıktan kaçınma ilkesine getirilecek istisnanın her hâlükârda temel hak ve özgürlüklere aykırı olmaması gerekir.
- Güvenlik: Kişisel verilerin toplanması, saklanması ve işlenmesi ile görevli bütün kurum ve kişiler bu verilerin, doğal afetlerin, kazaların, insanların işleyecekleri hataların ve kusurların doğuracağı tehlikelere karşı korunması için her türlü önlemi almalıdır.
- Denetim ve Yaptırım: Kişisel verilerin korunması ile ilgili düzenlemelerde öngörülen ilke ve kuralların uygulanması, önlemlerin alınması ve gerekli denetimlerin yapılması sorumluluğu; tarafsız, yetkin ve adil bir makama verilmelidir.
- Sınır Ötesi Veri Aktarımı: Kişisel verilerin saklanmakta olduğu ülkeden başka bir ülkeye aktarılması için her iki ülkenin ulusal mevzuatlarının bu aktarmaya izin vermesi gerekmektedir. Bunun yanında, verinin gönderileceği

ülkenin bu veri için sağladığı korumanın verinin bulunduğu ülkede sağlanan korumadan daha aşağı düzeyde olmaması da gerekir.

Verilerin doğru ve adil olarak işleme tabi tutulması için ilgili kişinin verilerin işlenmesinin varlığından ve kendisiyle ilgili verilerin neden toplanacağından haberdar olabilecek bir durumda olması gerekmektedir. Veri toplama koşullarını dikkate alarak ilgili kişiye tam ve doğru bilginin verilmesi de verilerin işleme tabi tutulmasında temel hak ve hürriyetlerin korunması açısından kabul edilen konular arasında yer almaktadır.

4.3.2.3. Kişisel Verilerin Korunması Konusunun Değerlendirilmesi

Kişinin özeli olarak değerlendirilen mahremiyet, kişinin kişisel bilgilerinin, kişisel haberleşmesinin, fiziksel mevcudiyetinin ve kişisel alanının başkasının müdahalesinden korunması demektir. Kişinin özeli veya mahremi olarak artık evi kadar kişiye ait kişisel bilgiler de kişiye özel mahrem bilgiler olarak kabul edilmektedir. Son dönemlerde yaşanan teknolojik gelişmeler, bilgi ve iletişim teknolojilerinde üretilen ve kullanılan bilgiler, bilgi mahremiyetinin önemini artırmaktadır.

Biyometrik sistemler de mahremiyet hakkı (*right to privacy*) kapsamında değerlendirilebilmektedir. Biyometrik veriler kişisel veriler olarak kabul edilmektedir. Böylece, biyometrik verilerin korunması, bilgi mahremiyetinin önemli bir uygulaması olmaktadır.

Sınır kontrollerinde, kişilerin resmi çekilmekte veya kişilerin parmak izi alınmakta olduğundan bu uygulamalar, bir anlamda mahremiyete müdahale olarak değerlendirilebilir. Devletlerin bu işlemleri yapmaya hakkı bulunmakla birlikte, yapılan bütün işlemler ölçülü bir şekilde yapılmalıdır. Kişisel verileri en yoğun ve kapsamlı biçimde işleyen kurum olan Devletin, özel sektöre nispetle kişisel verilerin korunması konusunda daha fazla hassasiyet göstermesi gerekmektedir. Özetle, devletlerin güvenlik ihtiyacı ile kişilerin mahremiyet hakkı dikkatli bir şekilde dengelenmelidir (Khanat, 2008: 85).

Kişilerin, mahremiyetlerine saygı gösterilmesi hakkı olduğunu yüksek mahkemeler dile getirmektedir. Mahremiyet hakkı, Birleşmiş Milletler ve Avrupa İnsan Hakları Sözleşmesi gibi çeşitli bölgesel ve uluslararası sözleşmelerle korunmaktadır.

Avrupa Birliği'nin 95/46/AT sayılı kişisel veri yönergesinde biyometrik veri tabiri bulunmamakla birlikte, düzenlemelerin ruhu ve düzenlemelerde kullanılan kavramlar uyarınca biyometrik veriler kişisel veri olarak değerlendirilmektedir. Avrupa Birliği kişisel veri düzenlemeleri, biyometrik sistemler tarafından üretilen ve kullanılan kişisel veriler için yeterli düzeyde koruma öngörmemektedir.

Devletlerin kişisel verileri kullanımına ilişkin uymaları gereken ilke ve kurallar Ekonomik Kalkınma ve İşbirliği Örgütü, Avrupa Konseyi, Birleşmiş Milletler ve Avrupa Birliği gibi uluslararası örgütler tarafından belirlenmiştir. Belirlenen genel kurallar, elde edilen kişisel verilerin ancak belirli ve yasal bir sebeple toplanabileceği, bildirilen maksat haricinde kullanılamayacağı, güvenli bir şekilde saklanacağı ve güncel olması gerektiği gibi konularla ilgilidir.

Kişisel verilerin korunmasına ilişkin konular, bilgisayarlar tarafından otomatik olarak işleme tabi tutulan verilerde olduğu gibi elle, otomatik olmayan bir şekilde işleme tabi tutulan veriler için de değerlendirilmelidir. Önümüzdeki süreçte önem arz edecek konulardan bir başkası ise, çok fazla sayıda biyometrik örnek kullanılan uygulamalarda kişisel verilerin korunması için fazladan nelerin yapılması gerektiğinin belirlenmesi olacaktır. Bahsedilen son iki konu, bu tez kapsamında tartışılmamaktadır.

4.4. ETKİNLİK

Göçte biyometri önerilirken bu uygulamanın üstünlükleri ön plana çıkartılmıştır ama incelendiğinde dezavantajlarının daha fazla ve daha ön planda olduğu görülmektedir. Amerika Birleşik Devletleri'nde etkinlik araştırması yapılmadan süreç başlatılmasına rağmen, Avrupa Birliği düzeyinde sisteme ilişkin sorunlar, düzenlemelerin başlangıçta güncellenmesi ve uygulamanın ertelenmesi sonucunu doğurmuştur.

Avrupa Birliđi, göç yönetiminde biyometrik sistemlerin kullanılmasını öngören düzenlemeler üye ülkelerin vatandaşlarının tepkisini çekmeyecek şekilde, aşamalı olarak yapmıştır. Üstelik biyometrik sistem düzenlemelerinin tartışılmasına ve eleştirilmesine uzun zaman ayrılmıştır. Düzenlemelerin yapılması ile uygulama başlamadan düzenlemelerde deđişiklik yapılması ve uygulamanın düzenlemeden yıllar sonra başlaması da bunun bir göstergesidir.

Biyometrik sistemlerin devlet güvenliğine özellikle sınır güvenliğine çok katkısı olduđu söylenmesine rağmen bu sistemlerin vatandaşların veya vatandaş olmayan kişilerin haklarına ne kadar etkisi olduđu detaylı olarak tartışılmalıdır (Redpath,2007: 30).

Rebekah Thomas, Amerika Birleşik Devletleri'nde ve İngiltere'de uygulanan biyometrik sistemlerin terörizm veya yasadışı göçün azaltılmasına katkıda bulunduđuna ilişkin çok az kanıt bulunduđunu söylemektedir (Thomas 2005: 6).

Diđer taraftan, biyometrik sistem kullanımının güvenlik sağlama ve göç yönetimine ciddi katkılar sağlamadıđı ve yasadışı göçü önlemede önemli başarılar elde etmediđi de iddia edilmektedir. Avrupa Parlamentosu Liberal Demokrat Parlamenti ve Adalet ve İnsan Hakları Sözcüsü Londra Parlamenti Sarah Ludford, Avrupa Birliđi'nin biyometrik veri tabanı olan Vize Bilgi Sistemi VIS (*European Visa Information System*) veri tabanının kuruluş tartışmalarında, Avrupa Birliđi'ne gelen göçmenlerin %99,99'unun yasal göçmenler olduđunu, kurulacak biyometrik veri tabanının Avrupa Birliđi'ne gelen göçmenlerin sadece %0,01'ini oluşturan yasadışı göçmenler ve suçlular için kurulduđunu hatırlatmaktadır (Euractiv, 2007).

Amerika Birleşik Devletleri İç Güvenlik Örgütü'nün (DHS-US Homeland Security Department) verilerine göre, biyografik bilgiler ve biyometrik tanımlayıcılar kullanılarak yabancı ziyaretçilerin ülkeye giriş ve çıkışlarını izleyen US-VISIT programının uygulamaya başlama tarihi olan Ocak 2004 tarihi ile Mart 2005 tarihi arasında 200'den fazla kişi tutuklanmıştır (Thomas 2005: 6). Tutuklanan kişiler ise hükümlü tecavüzcüler, uyuşturucu tacirleri, kredi kartı sahtekârlıđı suçluları, silahlı soyguncular ve çok sayıda yasadışı göçmen ve vize dolandırıcılık girişiminde bulunan bireylerdir. US-VISIT programı sebebiyle tutuklama sayısı olan 200, Amerika Birleşik Devletleri Sınır Görevlilerince 2004 yılında yasadışı göçmenlerden

sınırdaki toplam yakalama sayısı olan 1.264.232 sayısı¹⁴⁸ kıyaslanamayacak kadar küçüktür.

Ayrıca, Amerika Birleşik Devletleri US-VISIT programı Ocak 2004-Mart 2005 tarihleri arasında 2,5 milyondan fazla ziyaretçiye ilişkin veriyi işlemiş ve bu tarih aralığında hiç bir terör şüphelisini tespit etmemiştir (Thomas, 2005: 382).

Biyometrik sistemlerin yasadışı göçü önlemede katkısı olabileceği düşüncesi göç yönetiminde tartışılan bir konudur. Göç kontrol mekanizması olarak biyometrik sistemlerin kullanılabileceği fikri ilk önce Amerika Birleşik Devletleri'nde gündeme gelmiştir. Amerika Birleşik Devletleri sınır kontrollerinde biyometrik sistemler yaklaşık sekiz yıldır kullanılmaktadır. Geçen bu süre boyunca biyometrik sistemlerin yasadışı göçmenleri ve ülkeye giren teröristleri önleme konusundaki başarısı tartışılmaktadır.

On bir Eylül 2001 terör olayından sonra Amerika Birleşik Devletleri'nde önemli bir güvenlik politikası haline gelen göç politikasında değişiklik öngören birçok reform yapılmıştır. Göç politikasındaki değişikliklerden birisi sınır güvenliğini artırarak yasadışı göçmen sayısını azaltmak ve muhtemel teröristlerin ülkeye girişini engellemek şeklinde özetlenebilmektedir (Aslan, 2010: 47). Dolayısıyla göç politikası ile Amerika Birleşik Devletleri ulusal güvenlik politikası arasında sıkı bir ilişki kurulmuştur. Bununla birlikte uzmanların değerlendirmelerine göre, sınır güvenliğinin ve uygulanan güvenlik artırıcı yöntemlerin başarısı sınırlarda yakalanan insan sayısına göre ölçülmektedir (Haddal, 2010: 11).

Sınır güvenliğinin artırılması adına yapılan önemli bir değişiklik, US-VISIT programının devreye alınmasıdır. US-VISIT programı kapsamında ülkeye giriş yapan kişilere, biyografik bilgiler ve biyometrik tanımlayıcılar kullanılarak sınır kontrol işlemleri yapılmaktadır (Thomas, 2005: 399). Özetle, başta US-VISIT programı olmak üzere, sınır güvenliği adına alınan önlemler yasadışı göçmenlerin ülkeye girişini azaltmak amacıyla uygulanmaktadır.

Diğer yandan, US-VISIT programının 2004 yılından itibaren uygulanma döneminde Amerika Birleşik Devletleri'nde bulunan yasadışı göçmen sayısında bir azalma olmamıştır. 11 Eylül sonrası sınır güvenliğini artırma adına yapılan

¹⁴⁸ US Department of Homeland Security, Office of Immigration Statistics, 2010-Year Book of Immigration Statistics.

reformların tam olarak uygulanmadığına veya başarıya ulaşmadığına bir örnek, 2004 ile 2008 yılları arasında Amerika Birleşik Devletleri'nde yaşayan yasadışı göçmen sayısının 8–11 milyon civarında olması gösterilebilir (Khanat, 2008: 59).

Amerika Birleşik Devletleri'nde yaşayan yasadışı göçmen sayısı net olarak bilinmese bile devlet yetkilileri, araştırma kuruluşları ve akademisyenler çeşitli tahminlerde bulunmaktadır. Amerika Birleşik Devletleri Göçmen ve Vatandaşlık Bürosu (*INS-Immigration and Naturalization Service*¹⁴⁹), Amerika Birleşik Devletleri'nde yaşayan yasadışı göçmen sayısını 1995 yılında 5 milyon¹⁵⁰ ve 2000 yılında 7 milyon olarak tahmin ettiklerini açıklamıştır.¹⁵¹ Amerika Birleşik Devletleri İç Güvenlik Örgütü, Amerika Birleşik Devletleri'nde bulunan yasadışı göçmen sayısını 2005 yılında 10,76 milyon, 2007 yılında 11,8 milyon ve 2010 yılında 10,79 milyon olarak tahmin etmektedir.¹⁵² NY Times gazetesi yazarı Julian Preston, 2011 yılı Şubat ayında yazdığı bir makalede Pew Araştırma şirketinin yaptığı bir araştırmada Amerika Birleşik Devletleri'nde yaşayan yasadışı göçmen sayısının 2007 yılında zirve yaparak 12 milyona çıktığını düşündüklerini açıklamıştır.¹⁵³ Benzer bir şekilde, FAIR araştırma kuruluşu, 2007 yılında Amerika Birleşik Devletleri'nde bulunan yasadışı göçmen sayısını 13 milyon olarak tahmin etmektedir.¹⁵⁴

Verilen rakamlardan da anlaşılacağı üzere Amerika Birleşik Devletleri'nde yaşadığı tahmin edilen yasadışı göçmen sayısı 11 Eylül 2001 tarihinden sonra artarak devam etmiş, 2007 yılında zirve yapmış ondan sonraki yıllarda ise bir miktar düşmüştür. Görüldüğü gibi, göç kontrol mekanizmasında kullanılan biyometrik sistemlerin kurulum amaçlarından birisi olarak gösterilen yasadışı göçmenlerin ülkeye girişini engelleme konusunda herhangi bir yarar getirmemiş hatta biyometrik

¹⁴⁹ INS 2002 yılında DHS bünyesine alınmıştır.

¹⁵⁰ US Department of Homeland Security, Office of Immigration Statistics, <http://www.dhs.gov/xlibrary/assets/statistics/illegal.pdf>, (Erişim Tarihi: 15 Mart 2012).

¹⁵¹ How Many Illegal Immigrants? <http://www.fairus.org/issue/how-many-illegal-immigrants?A=SearchResult&SearchID=1641944&ObjectID=5123814&ObjectType=35>, (Erişim Tarihi: 15 Mart 2012).

¹⁵² a.g.e.

¹⁵³ 11.2 Million Illegal Immigrants in U.S. in 2010, Report Says; No Change From '09, <http://www.nytimes.com/2011/02/02/us/02immig.html>, (Erişim Tarihi: 15 Mart 2012).

¹⁵⁴ How Many Illegal Immigrants? <http://www.fairus.org/issue/how-many-illegal-immigrants?A=SearchResult&SearchID=1641944&ObjectID=5123814&ObjectType=35>, (Erişim Tarihi: 15 Mart 2012).

sistemlerin kurulum tarihinden hemen sonra Amerika Birleşik Devletleri'nde yaşamakta olduğu tahmin edilen yasadışı göçmen sayısında artış bile olmuştur.

Amerika Birleşik Devletleri'nde yaşamakta olduğu düşünülen yasadışı göçmen sayısı sınır görevlileri tarafından sınır kapılarında yakalanan yasadışı göçmen sayısı hariç tutularak verilmektedir. Diğer yandan, Amerika Birleşik Devletleri İç Güvenlik Örgütü tarafından açıklanan, sınır kapılarında görevlilerce yakalanan yasadışı göçmen sayısını incelemek yapılan değerlendirmeye katkı sağlamaktadır. Aşağıda Amerika Birleşik Devletleri İç Güvenlik Örgütü tarafından 2011 yılında yayımlanan 2010 Göç İstatistiği raporundaki son on yılda sınır görevlilerince yakalanan yasadışı göçmen sayısı verilmektedir.¹⁵⁵

ABD Sınır Görevlilerince Yakalanan Yasa Dışı Göçmenler

Yıl	Sayı
2000	1.814.729
2001	1.387.486
2002	1.062.270
2003	1.046.422
2004	1.264.232
2005	1.291.142
2006	1.206.457
2007	960.756
2008	791.568

¹⁵⁵ US Department of Homeland Security, Office of Immigration Statistics, 2010-Year Book of Immigration Statistics.

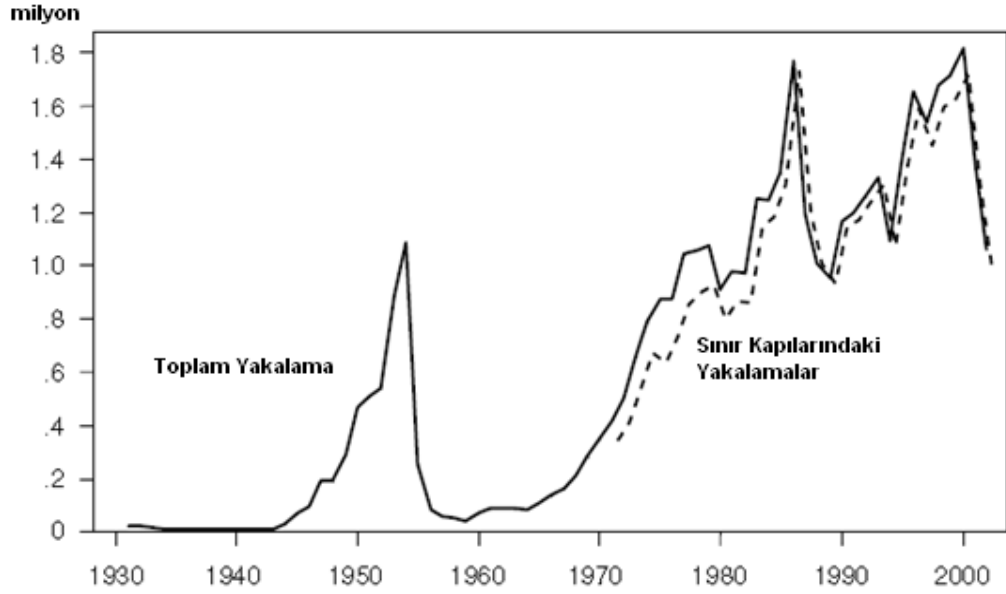
2009	613.003
------	---------

Tablo 5: ABD Sınır Görevlilerince Yakalanan Yasa Dışı Göçmenler¹⁵⁶

Tablo 5'deki rakamlara bakıldığında, 2000 yılında Amerika Birleşik Devletleri sınır görevlilerince yakalanan yasadışı göçmen sayısı 1.814.729 iken bu sayı 2005 yılında 1.291.142'e düşmüş ve 2007 yılından itibaren bir milyonun altına inmiştir. 2009 yılındaki sayı ise 2000 yılında yakalanan yasadışı göçmen sayısının nerdeyse üçte biri olan 613.003'e düşmüştür. Amerika Birleşik Devletleri'nde yakalanan yasadışı göçmen sayısı 2000 ile 2009 yılları arası sürekli düşmüştür. Bu düşüş genel bir eğilim olabilir diye de düşünülebilir. Daha önceki tarihlerde yakalanan yasadışı göçmen sayısına bakmak bir fikir verebilir.

Gordon H Hanson, Amerika Birleşik Devletleri İç Güvenlik Örgütü verilerine dayanarak, 1930 ile 2000 yılları arasında sınır görevlilerince Amerika Birleşik Devletleri sınır kapılarında yakalanan yasadışı göçmen sayısına ilişkin bir grafik sunmaktadır (Hanson, 2004: 348).

¹⁵⁶ a.g.e.



Şekil 7: 1930–2000 Yılları Arası ABD’de Yakalanan Yasa Dışı Göçmenler¹⁵⁷

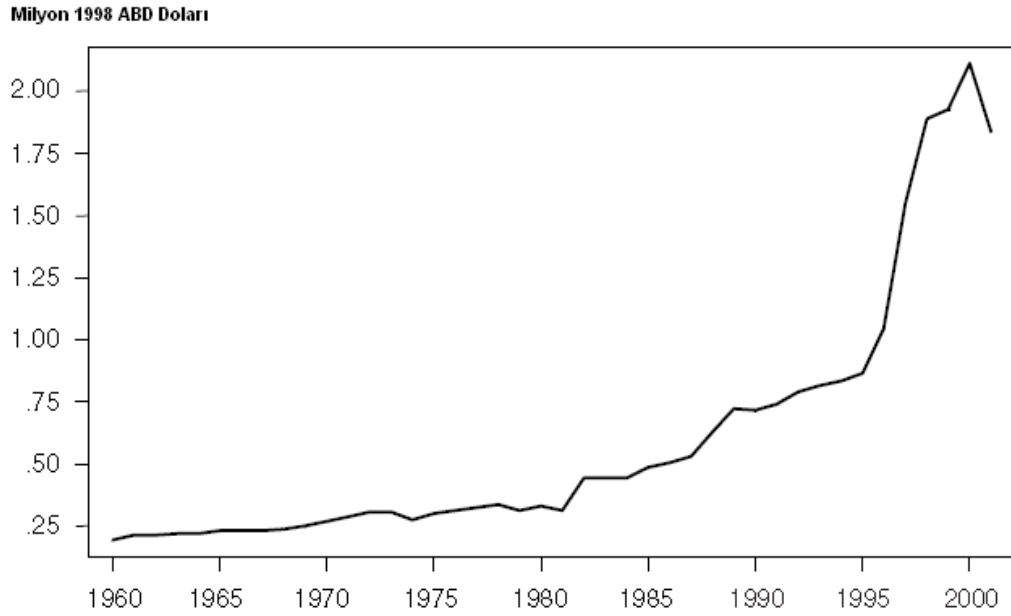
Şekil 7 incelendiğinde Amerika Birleşik Devletleri sınır görevlileri 1930 ile 2000 yılları arasında sınır kapılarında genel anlamda artan bir sayıda yasadışı göçmenleri yakalamaktadırlar (Hanson, 2004: 348). Yasadışı göçmenlerin sınır kapılarında yakalanması konusunda Amerika Birleşik Devletleri’nde yakalama sayısı uzunca zamandır her geçen yıl genel anlamda artmaktadır. Biyometrik sistemlerden sonra bu grafiğin daha yoğun bir şekilde artış trendinde olması beklenirken bilakis yakalama oranı düşmüştür. Tabii burada başka faktörler de söz konusu olabilir.

Sınır kontrolleri için kullanılan biyometrik sistemlerin kurulum tarihi olan 2004 yılından sonra Amerika Birleşik Devletleri’nde hem yasadışı göçmen sayısı artmış hem de sınır kapılarında yakalanan yasadışı göçmen sayısı azalmıştır. Bu durum, Amerika Birleşik Devletleri’nde uygulanan biyometrik sistemlerin yasadışı göçü önleme konusunda başarı yakalayamadığının önemli bir göstergesidir.

Diğer yandan önceki bölümlerde de değinildiği gibi, sınır kapılarında kurulan biyometrik sistemlerin maliyeti de yüksektir. Gordon H Hanson, Amerika Birleşik Devletleri Adalet Bakanlığı verilerine dayanarak 1960–2000 yılları arasında Amerika

¹⁵⁷ US Department of Homeland Security, Office of Immigration Statistics, 2010-Year Book of Immigration Statistics.

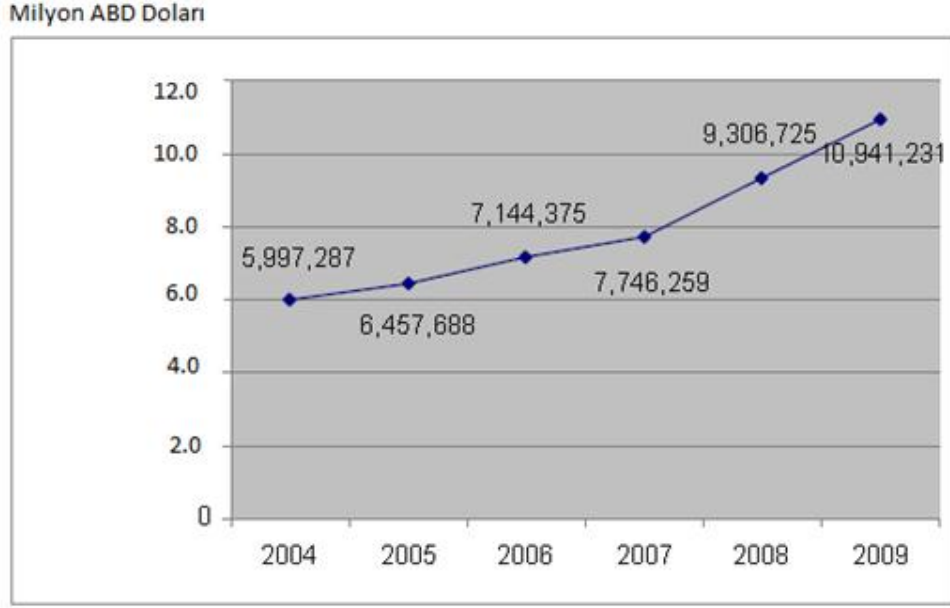
Birleşik Devletleri devletinin göç kontrolü için harcadığı bütçeyi grafik olarak göstermektedir (Hanson, 2004: 349).



Şekil 8: ABD Devletinin 1960–2000 Yılları Arası Göç Harcamaları¹⁵⁸

Şekil 8’deki görselde görüleceği üzere 1960 ile 2000 yılları arasında Amerika Birleşik Devletleri devletinin göç kontrolü için harcadığı para sürekli artmaktadır. Tabii bu grafik 11 Eylül 2001 olayları öncesi durumu göstermektedir. 2000 yılında göç yönetimi için harcanan para 2 milyon ABD doları civarındadır. Sınır kapılarında biyometrik sistemlerin kurulmaya başladığı 2004 yılından itibaren Amerika Birleşik Devletleri yönetiminin göç harcamaları aşağıdaki şekilde gösterilmektedir.

¹⁵⁸ US Department of Justice, Budget summary, <http://www.usdoj.gov/jmd/>, (Erişim Tarihi: 20 Ocak 2012).



Şekil 9: ABD Devletinin 2004–2009 Yılları Arası Göç Harcamaları¹⁵⁹

Şekil 9'daki görselden de görüleceği üzere, 2004 ile 2009 yılları arasında Amerika Birleşik Devletleri'nin göç kontrolü için harcadığı para, aynen daha önceki dönemlerde olduğu gibi sürekli artmaktadır. Bu dönem 2004 yılında başlayan US-VISIT programı sonrası döneme denk gelmektedir. Amerika Birleşik Devletleri sınır kapılarında sınır kontrol işlemleri için kurulan biyometrik sistemler bu dönemde olmuştur. Amerika Birleşik Devletleri yönetiminin 2000 yılında göç kontrolü için harcadığı para 2 milyon dolar civarında iken bu rakam 2004 yılında 6 milyon dolara ve 2009 yılında ise yaklaşık 11 milyon dolara varmaktadır. Sınır kapılarında biyometrik sistemlerin kurulması ve daha fazla ve nitelikli personel istihdamı göç yönetimi için harcanan paranın katlanması sonucunu doğurmaktadır.

Avrupa Birliği sınır kapılarında yakalanan yasadışı göçmenler hakkında bilgi Avrupa Birliği Bütünleşmiş Sınır Yönetimi Birimi FRONTEX tarafından 2008 yılından beri toplanmaktadır. Avrupa Birliği Bütünleşmiş Sınır Yönetimi Birimi tarafından sınır kapılarında yakalanan yasadışı göçmen sayısı kamuoyuyla paylaşılmaktadır. Avrupa Birliği sınır kapılarında 2008 ile 2011 yılları arasında yakalanan yasadışı göçmen sayıları hakkında bilgi aşağıda tablo olarak sunulmaktadır.

¹⁵⁹ Meissner ve Kerwin, 2009: 9.

AB Sınır Kapılarında Yakalanan Yasa Dışı Göçmen Sayıları

Yıl	Sayı
2008	159.881
2009	104.599
2010	104.051
2011	140.980

Tablo 6: AB Sınır Kapılarında Yakalanan Yasa Dışı Göçmenler¹⁶⁰

Avrupa Birliği Bütünleşmiş Sınır Yönetimi Birimi FRONTEX, Avrupa Birliği üye ülkelerinden dış sınırlarda yakalanan yasadışı göçmenler hakkındaki aldığı bilgileri üç aylık raporlar halinde yılda dört defa yayınlamaktadır. Ayrıca, yılda bir defa yıllık risk analizi raporları yayınlamaktadır. Tablo 6’da kullanılan veriler Nisan 2012 tarihinde yayınlanan 2012 Yıllık Risk Analiz Raporundan ve 2011 yılı üç aylık raporlarından faydalanılarak hazırlanmıştır.

Avrupa Birliği dış sınırlarında yakalanan yasadışı göçmen sayısı 2008 yılında 159.881 iken bu sayı 2009 yılında 104.599’a ve 2010 yılında ise 104.051’e düşmüştür. Yakalanan yasadışı göçmen sayısı, 2011 yılında 2009 ve 2010 yıllarına göre %35 artış olmakla birlikte, 2008 yılı rakamına göre %11 düşerek 140.980 sayısına ulaşmıştır. Amerika Birleşik Devletleri sınır kapılarında yakalanan yasadışı göçmen sayısında artış olmadığı gibi aynen Avrupa Birliği’nde de deniz, kara ve hava sınır kapılarında yakalanan yasadışı göçmen sayısında biyometrik pasaport kullanımından sonra bir artış olmamıştır.

Göç kontrol mekanizmasında kullanılan biyometrik sistemler sınır güvenliğinin artırılması amacıyla uygulamaya konmuştur. Uygulanan yöntemin başarısı yakalanan yasadışı göçmen sayısının düşürülmesi ve yakalanan sahte seyahat belgelerinin sayısının artmasıyla ölçülmektedir. Pasaportlarda ve seyahat

¹⁶⁰ FRONTEX, Annual Risk Analysis 2012, Frontex Reference Number: 5202, Varşova, Polonya.

belgelerinde kullanılan biyometrik sistemlerin avantajlarından birisi olarak biyometrik sistemlerin seyahat belgelerindeki sahteciliğe çözüm olması sayılmaktadır.

Avrupa Birliği Bütünleşmiş Sınır Yönetimi Birimi FRONTEX Nisan 2012 tarihinde 2012 Yıllık Risk Analiz Raporunu yayınlamıştır. Raporda bilgi verilen ve değerlendirme yapılan başlıklardan bir başkası ise Avrupa Birliği dış sınırlarında yakalanan sahte seyahat belgeleridir. Aşağıdaki tabloda 2009 ile 2011 yılları arasında Avrupa Birliği dış sınırlarında yakalanan sahte seyahat belgelerinin rakamları sunulmaktadır.

AB Sınır Kapılarında Yakalanan Sahte Seyahat Belgesi Sayıları

Yıl	Sayı
2009	8.094
2010	9.567
2011	9.682

Tablo 7: AB Sınır Kapılarında Yakalanan Sahte Seyahat Belgeleri¹⁶¹

Avrupa Birliği Bütünleşmiş Sınır Yönetimi Birimi FRONTEX yakalanan sahte seyahat belgesi sayılarını 2009 yılından itibaren yayınlamaktadır. Avrupa Birliği dış sınırlarında yakalanan sahte seyahat belgesi sayısı, 2009 yılında 8.094 iken bu sayı 2010 yılında %18 artarak 9.567 rakamına ulaşmış ve 2011 yılında ise bir önceki yıla göre %1 artış sağlayarak 9.682 rakamına ulaşmıştır. Özetle, 2010 yılında 2009 yılına göre artış olmakla birlikte bu artış süreklilik sağlamamış ve 2011 yılı rakamı ile 2010 yılı rakamı neredeyse aynı kalmıştır.

Yukarıdaki değerlendirmelerde olduğu gibi sınır kapılarında güvenliği artırmak ve yasadışı göçü engellemek üzere kurulan biyometrik sistemlerin

¹⁶¹ FRONTEX, Annual Risk Analysis 2012, Frontex Reference Number: 4591, Varşova, Polonya.

kurulumundan sonra sınır kapılarında yakalanan yasadışı göçmen sayısı her geçen yıl azalmış ve yakalanan sahte seyahat belgesinde ise düzenli ve yüksek oranda bir artış sağlanamamıştır.

Özetle, biyometrik sistemlerin çeşitli sorunları olmasına rağmen artan bir şekilde yaygınlaşması birçok kişinin verdiği tepkiyi haklı çıkartır niteliktedir. Çünkü biyometrik sistemler teknolojik olarak gelişme sürecindedir. Diğer taratan, biyometrik sistemlerin vatandaş veya vatandaş olmayan kişilerin haklarını ne ölçüde etkilediği kamuoyunda yeterince tartışılmamıştır. Son olarak, biyometrik sistemlerin hedeflenen amaçlara göre kapsamlı bir etkinlik analizi henüz yapılmamıştır.

Ayrıca, biyometrik sistemlerin uluslararası ölçekte birlikte ortak çalışabilirlik kurallarının belirlenmesi uygulamayı rahatlatacaktır. Avrupa Birliği'nin biyometrik sistemlere ilişkin aşamalı ve Amerika Birleşik Devletleri'ne göre yavaş tutumu kamuoyunun tepkisini nispeten hafifletir bir tutum sergilemektedir.

Biyometrik sistemler tarafından üretilen biyometrik verilerin kişisel veri olduğu genel olarak kabul edilen bir yaklaşımdır. Biyometrik sistemlerin yaygınlaşmasına paralel olarak kişisel veri düzenlemelerinin içerisine biyometrik verilerin dâhil edilmesi gereklidir.

Genel olarak seyahat belgelerinde, vize işlemlerinde ve sınır kapılarında kullanılan biyometrik sistemlerin bütün avantaj ve dezavantajları özellikle mahremiyetin ihlali göz önünde bulundurularak, göç kontrol mekanizmasında biyometrik sistemlerin kullanım ilkelerinin belirlenmesi ve bütün ülkelerin bu kurallara uymasının sağlanması devletler ve kişiler açısından faydalı bir süreçtir.

4.5. AVANTAJLAR İLE DEZAVANTAJLARIN DEĞERLENDİRİLMESİ ve ÖNERİLER

Göç kontrol mekanizmasında kullanılan biyometrik sistemlerin tahmin edilenden farklı olarak dezavantajları, avantajlardan oldukça fazladır. Göç kontrol mekanizmasında kullanılan biyometrik sistemlerin üstünlük ve eksiklikleri kamuoyunda yeterince tartışılmamıştır (Kajevic, 2006: 24). Özellikle kişisel veri olarak değerlendirilen biyometrik verilerin korunması konusunda uluslararası alanda net bir politika henüz belirlenmemiştir. Bütün bu tartışmalar kapsamında

görülmektedir ki, birçok avantajlı yanı olmasına rağmen biyometrik sistemler henüz tartışmasız kabul edilebilir bir teknoloji değildir.

Robert Clarke, göç yönetiminde kullanılan biyometrik sistemlerle ilgili yaptığı çalışmalar sonucu ulaştığı sonuçları öneri listesi olarak 2001 yılında yazdığı bir makalede yayınlamıştır. Clarke tarafından 11 Eylül 2001 terör olayından önce yapılan öneri listesi aşağıdaki gibidir (Clarke, 2001):

- Hiçbir biyometrik veri depolanmamalıdır. Bunun yerine sadece biyometrik özelliklerin tek yönlü bir fonksiyon (*hash*) ile elde edilen sonuçları saklanabilir.
- Hiçbir merkezi veri tabanı kullanılmamalıdır. Bunun yerine biyometrik veriler sadece kişinin kontrolü altında olan bir cihaz üzerinde depolanmalıdır.
- Biyometrik ölçüm aletleri tasarım standartları belirlenmelidir. Biyometrik cihazlardaki biyometrik özelliklere erişim şartları belirli olmalıdır.
- Tasarım standartlarına uymayan biyometrik ölçüm cihazlarının imali, ithali, kurulumu, kullanımı ve veri tabanı oluşturulması yasaklanmalıdır.
- Biyometrik ölçüm aletlerinin standartlara uyup uymadığı denetlenmelidir.
- Biyometrik ölçüm aletleri iki yönlü kimlik doğrulaması yapmalıdır. Cihazların doğruluğu ile içindeki bilgilerin doğruluğu test edilmelidir.

Brown ve Brook'un 2003 yılında "Eğer yakın zamanda politika belirlenmezse, son on yıldır kullanılan bu teknoloji kendi politikasını belirleyecektir."¹⁶² cümlesiyle belirttiği gibi biyometrik sistemlerin kullanımına ilişkin uluslararası bir politika devletler, uluslararası örgütler ve teknoloji firmaları tarafından beraberce belirlenmelidir. Brown ve Brook'un yaklaşık on yıl önce kullandıkları bu ifade hala geçerliliğini korumaktadır (Brown ve Brook, 2003: 5). Bu konuda politika belirlemeye dönük çeşitli çalışmalar bulunmaktadır.

BioSec isimli Avrupa Komisyonu destekli proje, biyometrik sistem kullanım politikasının ve standartlarının Avrupa Birliği düzeyinde belirlenmesi için yürütülmüştür. Aynı şekilde, Avrupa'da üretilen biyometrik ürünlerin kabiliyetlerini

¹⁶² Brown ve Brook, 2003: 5.

ve performanslarını test eden Avrupa Birliği Komisyonu tarafından finanse edilen bir başka proje *BioTesting Europe* projesidir. Bütün bu çalışmalarla birlikte, uluslararası düzeyde biyometrik sistemlerin kullanımına ve denetlenmesine ilişkin net bir politika henüz mevcut bulunmamaktadır.

Risklerinin çok ve ciddi olması, farklı ülkeler tarafından kullanılması, çeşitli markalar tarafından kendi kurallarının belirlenmesi, kişisel verilerin yoğun olarak kullanılması ve bu verilerin korunmasına ilişkin ilkelerinin uygulamaya dönük netleştirilmemiş olması, göç politikaları, sınır güvenliği ile vize işlemlerinde ve sınır kontrollerinde biyometri uygulamalarına ait uluslararası düzeyde politikanın oluşturulmasını zorunlu kılmaktadır ve bu politikaya uygun çerçeve kuralların belirlenmesini gerektirmektedir.

Jillyane Redpath, 2005 yılında Uluslararası Göç Örgütü (*International Organization for Migration-IOM*) için hazırladığı kitapçıkta göç kontrol mekanizması için oluşturulacak çerçeve politikanın unsurlarını aşağıdaki gibi önermektedir (Redpath, 2005: 14):

- Biyometrik sistem üreticilerinin sorumluluğunu ve hesap verebilirliğini sağlayacak uygun mekanizmalar oluşturulmalıdır.
- Mahremiyet ve kişisel veriler kurallarına uygun biyometrik sistemlerin kurulmasını denetleyecek ulusal düzeyde bağımsız kontrol organları tesis edilmelidir.
- Biyometrik verilerin ve bu verilerin bulunduğu sistemlerin yeterli düzeyde güvenliği sağlanmalıdır.
- Göç sistemlerinde biyometri kullanımına ilişkin düzenlemeler bulunmalıdır. Düzenlemeler, kamu kurumlarını, özel sektörü ve verilere erişen üçüncü parti kuruluşları kapsamalıdır.
- Verilere ulaşım ihtiyaç olduğu ölçüde gereken miktarda olmalıdır.
- Toplanan veriler kullanım amacıyla orantılı olmalıdır. İhtiyaç olandan fazla veri toplanmamalıdır.
- Kişisel veriler ve mahremiyet ile ilgili düzenlemeler bulunmalı ve düzenlemeler vatandaşları ve yabancıları kapsamalıdır.

- Göç işlemlerinin uluslararası niteliği ve biyometrik verilerin ülkeler arasında paylaşılma durumu göz önünde bulundurularak, biyometrik sistemlerin kurulumu, kişisel verilerin korunması, mahremiyetin ihlali ve sistemlere ilişkin kuralları denetleyecek bağımsız bir uluslararası kuruluş oluşturulmalıdır. Bu kuruluş, bütün ülkelerin göç işlemleri için kurulan biyometrik sistemleri denetleyebilmelidir. Göç sistemlerinde biyometri kullanımına ilişkin standartları da bahsedilen kuruluş belirlemeli ve güncellemelidir.

Avrupa Komisyonu, Haziran 2004 tarihinde Ortak Araştırma Merkezi (*Joint Research Centre-JRC*) Gelecek Teknolojik Araştırmalar Enstitüsü'nden (*Institute for Prospective Technological Studies*) biyometri teknolojisinin gelecekteki etkilerinin neler olabileceğine ilişkin bir çalışma yapmalarını talep etmiştir. Uzmanlar tarafından “*Biometrics at the Frontiers Assessing the Impact on Society*” ismiyle hazırlanan 148 sayfalık rapor Şubat 2005'te yayınlanmıştır. Kapsamlı olarak hazırlanan raporda sunulan öneriler aşağıdadır (JRC, 2005: 10).

- Her biyometrik uygulamanın amacı açık olarak belirli olmalıdır. Biyometri kullanımı, vatandaş ile devlet arasındaki mevcut güven modelinin sorgulanmasına sebep olmaktadır. Böyle bir açıklık, özellikle kullanıcı kabulünü sağlamak için gereklidir.
- Biyometri mahremiyetin korunması için kullanılmalıdır. Biyometri kullanımı sonucu kişilere ait özel bilgiler yayılmamalıdır. Bunu önlemek için çoklu biyometrik özellik aynı anda kullanılabilir.
- Avrupa biyometri endüstrisinin ortaya çıkması sağlanmalıdır. Özellikle büyük ölçekli biyometri uygulamaları Avrupa biyometri sektörünün ortaya çıkması için bir fırsattır. Sektörün gelişmesi kullanıcı kabulünün sağlanmasına katkı sunacaktır.
- Biyometrik sistemler yüzde yüz başarıyla çalışmadığından alternatif kontrol sistemleri kurulmalıdır.

- Bazı konularda gelecekte daha fazla araştırma yapılması önerilmektedir. Araştırma yapılması için önerilen alanlar; Araştırma ve Teknolojik Gelişme, Çoklu Biyometrik Sistemler ve Büyük Ölçekli Saha Denemeleridir.

Jillyane Redpath tarafından 2005 yılında göç kontrol yönetiminin koordinasyonu için önerilen çerçeve politikada, mahremiyetin ihlali ile ilgili kurallar bulunmamaktadır. Redpath tarafından sayılan çerçeve politika ilkeleri içerisinde, mahremiyete özellikle de kişisel verilerin korumasına ilişkin, ibareler bulunmaktadır. Redpath, daha sonradan 2007 yılında çerçeve politikada bulunacak mahremiyetin ihlalini önlemeye ilişkin kuralları aşağıdaki gibi önermektedir (Redpath, 2007: 32):

- Göç işlemlerinde, vatandaşlar ve göçmenlerin biyometrik bilgileri hangi yaş aralığında (minimum ve maksimum yaş) toplanmalıdır? Toplanacak verilerin uzunluğu ne olmalıdır? Farklı seyahat belgeleri için farklı uzunlukta veriler mi toplanmalıdır?
- Biyometrik verilerin ve diğer bilgilerin doğru ve güncel olması için ne tür mekanizmalar oluşturulmalıdır?
- Biyometrik veri ile birlikte hangi tür veriler de toplanmalıdır?
- Toplanan biyometrik veriler hangi şartlarda ülke içinde ve uluslararası arenada paylaşılabilir?
- Biyometrik veriler ile ilgili politikalar hangi seviyede kamuoyuyla paylaşılmalıdır?

4.6. BÖLÜM ÖZETİ

Güvenlik başta olmak üzere birçok alanda kullanılan biyometrik sistemlerin çeşitli avantajları olduğu kadar dezavantajları da bulunmaktadır. Biyometri teknolojisinin avantajları da dezavantajları da göç yönetiminde kullanıldığında artmaktadır.

Biyometri teknolojisinin ve biyometrik sistemlerin öncelikli avantajları; hız, doğruluk ve güvenlidir. Biyometrik sistemlerin kullanım kolaylığı, biyometrik sistemlerde kullanılan kişi özelliklerinin değişmeden kalması, sahteciliğin önlenmesi ve işlemlerin otomatik yapılmasından dolayı sınır görevlilerinin inisiyatifinin azalmış

olması gibi başka üstünlükleri de vardır. Göç kontrol mekanizmasında kullanılan biyometrik sistemlerin önemli bir avantajı, iltica edenlerin geri dönüş ülkelerinin kolayca bulunmasıdır. Sık seyahat eden iyi niyetli yolculara sunulan otomatik geçiş kapıları ile işlemlerinin kolaylaştırılması da biyometri adına başka bir avantajdır.

Biyometrik sistemlerin kullanımının sorunlu olarak belirtilebileceği birçok yanı da mevcuttur. Biyometrik sistemlerin doğruluk oranının yüzde yüz olmaması temel bir sorundur. Örneğin, sınır kapılarındaki milyonlarca yolcu için uygulanan biyometrik sistemlerin başarı oranındaki küçük bir düşüş çok fazla sayıda yolcu açısından başarısız bir sonuçla karşılaşma oranını artırmaktadır. Bu durum güvenlik açısından sorun olduğu gibi yolcuların seyahat özgürlüğüne engel oluşturma gibi bir olumsuzluğa da sebep olmaktadır.

Biyometri teknolojisinin ve biyometrik sistemlerin bir başka dezavantajı maliyettir. Biyometrik sistemler yüksek maliyetlerle kurulmakta ve bu sistemlerin işletilmesi için de yüksek maliyetler gerekmektedir. Biyometri teknolojisi yüksek teknoloji olması itibarıyla, kullanıcıları yetiştirmiş ve yetenekli personel olmalıdır.

Biyometri teknolojisinin ve biyometrik sistemlerin göç yönetiminde kullanılmasının sonucu ilave bazı sorunlar daha ortaya çıkmaktadır. Örneğin, biyometrik bilgilerin toplama ve kullanım politikasının hala net olarak belirlenmemiş olması, yetkisiz kişilerin de biyometrik verilere erişebilir olması, biyometrik veriler ile hastalığın tespiti gibi kişilere ait özel bilgilerin de açığa çıkarılabilmesi veya biyometrik veriler aracılığıyla devlet kurumlarının kişileri gizlice izleyebilmesi göç yönetimi özelindeki sorunlar olarak sayılabilir.

Biyometri teknolojisinin ve biyometrik sistemlerin önemli bir dezavantajı mahremiyetin ihlali ve kişisel verilerin korunmasında yaşanan sorunlardır. Biyometrik sistemler ile sınır kapılarında toplanan biyometrik veriler, toplanma maksadı haricinde devlet görevlileri tarafından kullanılabilmesi kişilerin mahremiyet hakkı açısından önemli bir problemdir. Mahremiyet hakkı, vatandaşlar için de vatandaş olmayanlar için de bir haktır. Biyometrik sistemlerin kullanıldığı sınır kontrolleri bir anlamda kişinin mahremiyetine müdahaledir. Mahremiyet hakkının korunma yöntemlerinden birisi, kişiye ait kişisel bilgilerin korunmasıdır.

Biyometrik veriler kişilerin vücut özelliği ile ilgili olduğundan genel olarak kişisel veri olduğu kabul edilmektedir. Böylece, göç yönetiminde kullanılan

biyometrik sistemler tarafından üretilen biyometrik veriler için de kişisel verilerin korunması kuralları geçerlidir.

US-VISIT programı ile Ocak 2004 tarihi ile Mart 2005 tarihi arasında Amerika Birleşik Devletleri sınır kapılarında hiç bir terör şüphelisi tespit edilememiş sadece 200 civarında suçlu tutuklanmıştır (Thomas, 2005: 382). Tutuklama sayısı olan 200, Amerika Birleşik Devletleri sınır görevlilerince 2004 yılında sınırda yakalanan yasadışı göçmen sayısı olan 1.264.232 ile kıyaslanamayacak kadar küçüktür.

Rebekah Thomas (2005), uygulamanın başlamasından yaklaşık bir yıl sonra yaptığı değerlendirmede, Amerika Birleşik Devletleri göç yönetiminde kullanılan biyometrik sistemlerin terörizm veya yasadışı göçün azaltılmasına katkıda bulunduğu ilişkin çok az kanıt bulunduğunu belirtmektedir (Thomas, 2005: 382). Bu görüş uygulama sonuçlarından net olarak anlaşılmaktadır.

SONUÇ VE ÖNERİLER

Göç kontrol mekanizması olarak biyometrik sistemlerin kullanılması ilk olarak Amerika Birleşik Devletleri'nde uygulanmıştır. Amerika Birleşik Devletleri'nde sınır kontrollerinde biyometrik sistemler 2004 yılından beri kullanılmaktadır. Amerika Birleşik Devletleri'nde geçen sekiz yıl boyunca biyometrik sistemlerin yasadışı göçmenleri ve ülkeye giren teröristleri önleyip önleyemediği hala tartışılmaktadır.

Bu çalışmada, göç politikaları, sınır güvenliği ile vize işlemlerinde ve sınır kontrollerinde biyometri uygulamalarının kullanımı incelenmiştir. Biyometri uygulamaları tarafından üretilen ve kullanılan kişisel verilerin güvenliğinin sağlanması da değerlendirilen bir başka konudur.

Göç kontrol sisteminde güvenliği artırmak üzere kullanılan biyometrik sistemlerin, etkinliği ve göç yönetimine katkısı tartışılmıştır. Ayrıca, etkinlik tartışması biyometrik sistemlerin avantaj ve dezavantajları düzeyinde de incelenmektedir. Etkinlik tartışmasını sağlıklı olarak yapabilmek için Avrupa Birliği ve Amerika Birleşik Devletleri göç politikaları ile Avrupa Birliği ve Amerika Birleşik Devletleri'nde uygulamaya konan biyometrik sistemler açıklanmıştır. Özellikle Amerika Birleşik Devletleri'nde, göç yönetiminde kullanılan biyometrik sistemler teorik olarak başarılı olacağı öngörülerek kullanılmaya başlanmıştır.

Avrupa Birliği ve Amerika Birleşik Devletleri uygulamalarında yapılan düzenlemeler ve bu düzenlemeleri uygulamaya koymakla görevlendirilen kurumsal yapılar ile uygulamaların yapısı incelenmiştir. Uygulamalardaki sorunlar ile biyometrik sistemlerin göç yönetiminde kullanılmasının avantaj ve dezavantajları detaylı olarak tespit edilmiştir.

Bu konuları incelemek hem teorik hem de pratik boyutta katkılar sağlamaktadır. Teorik boyuttaki katkı, hem Avrupa Birliği hem de Amerika Birleşik Devletleri'ndeki yasal düzenlemeleri ve sorumlu aktörlerin görevlerini anlamamıza yardımcı olmaktadır. Pratik boyutta ise, hem Avrupa Birliği hem de Amerika Birleşik Devletleri'ndeki uygulamaların etkinliğini ve zayıf yanlarını anlamamıza yardımcı olmaktadır.

Bu çalışmada yapılan tartışmalar ve verilen bilgiler, 1 Haziran 2010 tarihinde Türkiye'de başlayan elektronik pasaport uygulamasına ve göç politikası için

yapılacak düzenlemelere destek sağlayacak mahiyettedir. Çalışma kapsamında, hem Avrupa Birliği hem de Amerika Birleşik Devletleri'ndeki yasal düzenlemeler ve sorumlu aktörlerin görevleri incelendiği gibi uygulanan sistemlerdeki açıklıkların ve sorunlu alanların tespiti yapılmıştır.

Göç kontrol mekanizmasında kullanılan biyometrik sistemlerin avantaj ve dezavantajları incelendiğinde görülmektedir ki, sanılanın aksine dezavantajlar avantajlardan daha fazladır. Uzmanların da belirttiği gibi, göç kontrol mekanizmasındaki biyometrik sistemlerin avantaj ve dezavantajları kamuoyunda yeterince tartışılmamıştır. Biyometrinin birçok avantajına rağmen, henüz tartışmasız kabul edilebilir bir teknoloji olmadığı görülmektedir.

Kişisel veri olarak değerlendirilen biyometrik verilerin güvenliği sağlanmalıdır. Özellikle merkezi veri tabanı kullanıldığında, biyometrik verilerin yetkisiz kişilerin eline geçme riski daha da artmaktadır.

Biyometrik sistem kullanılan sınır kapılarında, kişiden veya sistemden kaynaklanan bir sorun olduğunda, kişinin seyahat özgürlüğüne engel olacak bir durum yaşanmaması için sınır kapısında alternatif olarak kullanılabilecek klasik bir kontrol sistemi bulundurulmalıdır.

Tartışılan bir başka konu, göç kontrol mekanizmasında kullanılan biyometrik sistemlerin etkinliğidir. Biyometrik sistemlerin devlet güvenliğine, özellikle sınır güvenliğine çok katkısı olacağı söylenmiştir. Özellikle biyometrik sistemlerin göç yönetiminde ilk defa kullanılmaya başlandığı Amerika Birleşik Devletleri'nde biyometrik sistemlerin yasadışı göçle mücadelede önemli bir araç olduğu iddia edilmiştir.

Amerika Birleşik Devletleri'nde yapılan yasal düzenlemelere ve kurulan yeni kurumlara rağmen, 11 Eylül 2001 sonrası yapılan reformların sınır güvenliği konusunda başarıya ulaşmadığı dile getirilmektedir. Amerika Birleşik Devletleri'nde yaşayan yasadışı göçmen sayısının 11 Eylül 2001 sonrasında düşmemesi hatta artması başarısızlığa kaynak olarak gösterilmektedir.

Amerika Birleşik Devletleri'nde, uygulamanın başlamasından yaklaşık bir yıl sonra yapılan değerlendirmede göç yönetiminde kullanılan biyometrik sistemlerin terörizm veya yasadışı göçün azaltılmasına katkıda bulunduğu ilişkin çok az kanıt

bulunduđu belirtilmektedir. Rebekah Thomas'ın deęerlendirmesine katkı sunan bilgi, Amerika Birleşik Devletleri İç Güvenlik Örgütü tarafından yayınlanmıştır.

Avrupa Birlięi'nde, göç yönetiminde biyometrik sistemlerin kullanılmasını öngören düzenlemeler, tartışma, inceleme ile araştırmalar sonucu aşamalı olarak yapılmıştır. Avrupa Birlięi tarafından seyahat belgelerinde biyometrik özelliklerin standartlarını belirleyen düzenleme ilk defa 2004¹⁶³ yılında yapılmasına rağmen bu düzenlemenin en son güncelleme tarihi 2009 yılıdır.¹⁶⁴ Düzenlemenin ilk tarihi ile düzenlemede deęişiklik yapılması ve uygulamanın düzenlemeden yıllar sonra başlaması da bunun bir göstergesidir.

Dięer taraftan, Avrupa Parlamentosu Liberal Demokrat Parlamenterleri ve Adalet ve İnsan Hakları Sözcüsü Londra Parlamenterleri Sarah Ludford, Avrupa Birlięi'ne gelen göçmenlerin çok büyük bir kısmının yasal göçmenler olduğunu, kurulan biyometrik sistemin Avrupa Birlięi'ne gelen göçmenlerin sadece %0,01'ini oluşturan yasadışı göçmenler ve suçlular için kurulduğunu belirtmektedir.

Göç kontrol mekanizmasında biyometrik sistemlerin kullanımına ilişkin son on yıldır bazı araştırmacıların önerileri olduğu gibi yaptırılan bazı araştırmalar sonucu ortaya çıkan öneriler de bulunmaktadır. Bunlardan bazılarını örnek olarak vermek, bu çalışma kapsamında yapılacak öneriler için destek oluşturmaktadır.

Araştırmacı Robert Clarke'ın, 2001 yılında yaptığı öneriler hala geçerli önerilerdir. Listelenen öneriler konusunda uluslararası düzeyde henüz bir kabul olduğu konusunda bilgi bulunmamakla birlikte, bu önerileri yanlışlayan sonuçlar da henüz elde edilmiş deęildir.

Avrupa Komisyonu tarafından yaptırılan araştırmada kullanıcı memnuniyeti ve sektörün gelişmesi üzerinde durulmuştur. Daha önceden de ifade edildięi gibi Avrupa Birlięi, Amerika Birleşik Devletleri'nin aksine göç yönetiminde biyometrik sistemlerin kullanımı konusunda aşamalı ve ikna edici bir yöntem sergilemektedir.

Biyometri teknolojisi, güvenlik ve insan hakları gibi tüm tarafların ihtiyaçlarını ve haklarını uzlaştıran bir bağlam içinde çalışmalıdır. Bu konuda ortak bir zeminde buluşmak için yapılması veya bilinmesi gerekenler vardır.

¹⁶³ EC 22252/2004.

¹⁶⁴ EC 444/2009.

Göçmenlik reformu ve terörle mücadele yaklaşımı konuları iki farklı konu olarak değerlendirilmelidir. Amerika Birleşik Devletleri'nde yaşanan 11 Eylül 2001 terör olayından sonra Amerika Birleşik Devletleri, terörle mücadele ve yasadışı göçle mücadelenin beraberce belirlenmesi gerektiği fikrini bütün dünyaya kabul ettirmeye çalışmaktadır. Biyometrik sistemlerin göç kontrol mekanizmasında kullanılmaya başlanmasından bu yana, on yıl bile olmadan birçok tartışma yapılmakta ve biyometrik sistemlerin birçok dezavantajı uygulayıcıları zor durumda bırakmaktadır.

Biyometrik veri toplanma ve biyometrik verilerin kullanım uygunluğunu ölçmek için, sivil hak savunucuları orantılılık ilkesinin değerlendirilmesi amacıyla veri koruma organlarına müracaat edebilirler. Ayrıca, orantılılık ilkesi ile gündeme getirilen önlemlerin kullanım maksatlarına göre haklı olup olmadığı, uygulama sonuçlarının değerlendirilmesi ile daha kolay tespit edilebilir.

Biyometrik belgelerin kullanımı sonucu ortaya çıkan risk ile seyahat özgürlüğünün kısıtlanma durumu orantılı olmalıdır. Orantılılık ilkesi, biyometrik bilgilerin toplanmasının uygun ve meşru amaçlar için olmasını gerekli kılmaktadır. Biyometrik bilgiler, kullanılacağı amacın gerektirdiği ölçüde toplanması gerekmektedir. Bu tedbirler, güvenlik, gereklilik ve orantılılık gereksinimlerini karşılamak konusunda başarılı olmalıdır.

Avantajı ve dezavantajı çok olan biyometrik sistemlerin kullanımında devletin güvenlik talebi ile kişilerin mahremiyetlerinin ihlali arasında bir denge sağlanmalıdır. Devletlerin güvenlik beklentisi ile bireylerin mahremiyet talebi iyi dengelenmelidir. Devletin güvenlik sistemi için kişilerin mahremiyetleri ihlal edilemeyeceği gibi, kişilerin mahremiyetinin korunması için de devletin güvenlikten vazgeçmesi düşünülemez. Bu nedenle, belirli bir problem için çözüm olarak biyometrik sistem uygulanıp uygulanamayacağı düşünülürken, etik sorumluluk sergilenmesi gerekmektedir.

Biyometrik sistemler kullanılırken, devletler, biyometrinin getirdiği riskleri öngörmeli ve mahremiyetin korunması konusunda özen göstermelidir. Bununla birlikte, doğru kurallar ile kişisel verilerin korunması sağlanmalı ve mahremiyete müdahalenin sınırları iyi çizilmelidir.

Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesi biyometriyi kapsamaktadır. Çünkü biyometrik bilgiler kişinin özeli olan vücuduyla veya davranışlarıyla ilgilidir.

Dolayısıyla biyometrik bilgiler, kişisel bilgiler olarak değerlendirilmektedir. Bazı durumlarda biyometrik veriler, kişilere ait hastalık gibi ilgisiz bazı özel verilerin de ortaya çıkmasını sağlamaktadır. Ayrıca, biyometrik verilere seyahat acenteleri de erişebilmektedir. Bütün bunlar biyometrik verilerin korunmasının önemini ortaya koymaktadır. Kişisel veri olarak görülen biyometrik verilerin, kişisel verilerin korunması kurallarına tabi olması için kişisel verilerin korunması düzenlemelerinin kapsamına biyometrik veriler açıkça dâhil edilmelidir.

Unutulmamalıdır ki, yasadışı göçmenler daha çok yasal olmayan ve gizli yöntemlerle ülke içine girmektedir. Sınır kapılarında yasadışı göçmenlerin bulunması ihtimali düşüktür. Biyometrik kimlik kartlarının kaçak göçmenlerin çalışmalarını önleyeceğine inananlar hatırlamalıdır ki, yasadışı göçmenler, gizlice yaşamakta ve gizlice çalışmaktadırlar. Yasadışı göçmenlere herkes için geçerli olan kurallar uygulanmaya çalışılmamalıdır.

Biyometri yeni bir teknoloji olduğundan kullanıcı kabulü önemlidir. Biyometrik sistemler büyük ölçekli uygulamalarda kullanıldığında hata durumları iyi öngörülmelidir. Yoksa kullanıcıların tepkisini çeken bir sistem olabilir. Bu yüzden, biyometrik sistemlerin, öncelikli olarak gönüllü yolcular tarafından kullanılması bir avantaj olabilir. Sık seyahat eden iyi niyetli kullanıcılar sınır kapılarında kurulan biyometrik sistemlerin ilk gönüllüleri olabilir. Zaten Avrupa Birliği uygulaması da bu şekildedir. Zorunlu kullanımdan çok önce gönüllü kullanıcılar için otomatik geçiş sistemleri ile biyometrik sistemler kullanılmıştır. Örneğin, Amsterdam Schiphol Havalimanı'nda Privium isimli iris otomatik geçiş sistemi, 23 Ekim 2001 tarihinde test uygulamasına başlamıştır.

Biyometrik sistem kullanımı ile sınır kontrollerinin güvenliğini artıran ve seyahat belgelerini daha güvenli hale getiren devletler, biyometrik sistemler ve biyometri teknolojisi konularında diğer ülkelerle olan işbirliklerini artırmalıdır.

Göç yönetiminde biyometrik sistemlerin kullanımının birçok avantaj ve dezavantajı bulunmaktadır. Bütün bunların iyi dengelenebilmesi için, kurallar oluşturulmalı ve uygulamalar denetlenmelidir. Ülkeler, kendi içlerinde düzenleyici ve denetleyici kuruluş kurmaları gerektiği gibi, uluslararası düzeyde bir kuruluş tarafından bütün ülkelerdeki sistemlerin standartları belirlenebilir.

Daha önceki bölümlerde ifade edildiği gibi, Türkiye’de gerçek anlamda bir biyometrik pasaport uygulaması bulunmamaktadır. Türkiye’de 1 Haziran 2010 tarihinde başlayan uygulama tam anlamıyla biyometrik pasaport uygulaması değildir. Uygulama, daha çok elektronik pasaport uygulamasıdır. Özetle, yeni düzenlenen Türk pasaportlarında, biyometrik bilgiler olan parmak izi veya biyometrik resim özellikleri bulunmamaktadır. Yeni düzenlenen elektronik pasaportlar, Uluslararası Sivil Havacılık Örgütü ICAO’nun 9303 sayılı belgesi standartlarına göre hazırlanmış, makine tarafından otomatik olarak okunabilen ve içindeki bütünleşmiş devrede Türk pasaportu olduğunu belirten elektronik sertifika mevcut bulunan bir pasaporttur.

Yeni elektronik pasaport başvurusu yapan her vatandaş, bu işlem sırasında on parmağının birden parmak izi kaydını vermektedir. Vatandaşlar bu işlemin elektronik pasaport uygulamasının bir parçası ve zorunlu olduğunu düşünmektedirler. Diğer taraftan, Emniyet Genel Müdürlüğü Pasaport Daire Başkanı’nın da ifade ettiği gibi, elektronik pasaport alırken bütün parmakların parmak izi, sisteme tanıtılmakta ve bu veriler Emniyet Genel Müdürlüğü sistemlerine aktarılmakta ve elektronik pasaport için kullanılmamaktadır. On parmağın izinin pasaport için alınmadığı pasaport evraklarında uyarı olarak bulunmaktadır.

Türkiye’de sadece pasaportlarda değil Sosyal Güvenlik Kurumu ile Nüfus ve Vatandaşlık Genel Müdürlüğü gibi Kurumların uygulamalarında da kişilere ait biyometrik bilgilerin kullanılması planlanmaktadır. Bütün uygulamalar veya planlamalar göz önünde bulundurularak detaylı bir çalışma sonucu vatandaşlara ait biyometrik bilgilerin kamu kurumları tarafından kullanılmasına ilişkin düzenlemeler yapılmalıdır.

Düzenlemeler yapılırken diğer ülkelerde yaşanan sorunlar da göz önünde bulundurulmalıdır. Böyle detaylı bir çalışma ancak kurulacak kapsamlı bir komisyon tarafından yürütülmelidir. Türkiye’deki farklı biyometrik uygulamalarının en çok kişiyi etkileyen en kapsamlı proje bünyesinde diğer bütün projelerin birleştirilmesi gibi seçenekler gündeme getirilebilir. Çünkü ham mükerrer yatırım yapılmamış, hem kişiler daha az rahatsız edilmiş hem de kişisel bilgiler daha az yerde muhafaza edilmiş olacaktır.

Türkiye’de henüz kişisel verilerin korunmasına ilişkin hiçbir yasal düzenleme bulunmazken kişilerin vücuduna ait özel biyometrik bilgilerin korunması konusu yasal olarak korunmamaktadır. Zaten mevcut elektronik pasaport uygulaması için ayrı bir yasal düzenleme bulunmamaktadır. Bununla birlikte, Türkiye Avrupa Birliği uyum çalışmaları kapsamında bu dönemde özel bir iltica yasası çıkartma planlaması yapmaktadır. Biyometrik pasaport ile ilgili yapılacak düzenleme iltica yasası kapsamında da değerlendirilebilir.

Biyometrik pasaport uygulaması ile elektronik kimlik uygulamasının bir bütün olarak değerlendirilmesi de başka bir uygulama türü olabilir. Bazı ülkelerde, seyahat belgesi ile kimlik belgesi elektronik kimlik uygulaması bünyesinde birleştirilmektedir. Türkiye’de biyometrik pasaport uygulaması ile elektronik kimlik uygulamasının birleştirilmesi de düşünülebilecek bir konudur.

Göç yönetiminde biyometrik sistemlerin kullanımının dezavantajlarının avantajlarından daha fazla olduğu gerçeği ve uygulamanın yürütüldüğü ülkelerde yaşanan sorunlar düşünüldüğünde, bu çalışma kapsamında Türkiye için yapılacak öneri şu şekilde olabilir. Biyometrik sistemlerin göç yönetiminde kullanılma durumları olan biyometrik pasaport ve vize işlemlerinde, biyometrik kontrol işlemlerinden önce Avrupa Birliği ülkelerinde olduğu gibi gönüllü vatandaşların kayıt olabileceği, sınır kapılarında pasaport kontrol işlemlerini hızlandıracak otomatik geçiş sistemlerinin kurulmasıdır. Otomatik geçiş sistemlerinin, hem uygulamadaki aksaklıkların tespit edilip düzeltilmesine, hem altyapının kademeli olarak hazır hale getirilmesine, hem de vatandaşların biyometrik sistemlere olan bakış açısına ve genel olarak kamuoyu kabulünün sağlanmasına katkıları olacaktır.

Bu çalışmada varılan sonuç şu şekilde özetlenebilir. Biyometrik sistemlerin kullanımı sadece teknolojik bir sorun değildir. Aynı zamanda toplumun geneline hitap eden bazı zorlukları ve sıkıntıları barındırmaktadır. Bu sorunların uygun şekilde çözülmesi, biyometrik sistemlerin yaygın olarak kullanımını şekillendirecek ve yakın gelecekte ele alınması gereken biyometrik sistem kullanım politikasının belirlenmesine katkı sağlayacaktır.

Bu çalışmada bahsedilen sorunlarla mücadele için Avrupa Birliği ve Amerika Birleşik Devletleri uygulamalarındaki tecrübeler tartışılmıştır. Biyometrik sistem

kullanımının getirdiđi sorunlarla m¼cadele iin ¼nerileri kısaca tekrar etmek gerekirse:

- Biyometrik sistem kullanım gerekesi aık ve net olmalıdır.
- Biyometrik sistem kullanımı ile mahremiyete m¼dahale deđil mahremiyetin korunmasına destek olunmalıdır.
- Biyometrik sistem kullanılan sınır kapılarında alternatif olan klasik y¼ntem gibi esneklikler sađlanmalıdır.
- B¼y¼k ¼lekli uygulamalar konusunda daha fazla alıřmalar yapılmalıdır.
- Son olarak biyometrik sistem end¼strisi ve laboratuvar test ortamları sađlanmalıdır.

KAYNAKÇA

- Acer, Yücel; Kaya, İbrahim ve Gümüş Mahir, (2011), “Yasadışı Göç ve İltica Bağlamında Sınır Güvenliği: Avrupa Birliği Düzenlemeleri ve Türkiye”, Süleyman Özeren, M. Alper Sözen ve Oğuzhan Ömer Demir (Der.), *Yerelden Küresele Sınıraşan Suçlar*, Ankara: Polis Akademisi Yayınları, ss.149–168.
- Akçay, Muammer ve Çetinkaya, H. Hakan. (2012), “Kampüslerde Uygulanan Yeni Biyometrik Sistemler”, *Akademik Bilişim 2012 Bildirileri*, 1–3 Şubat 2012, Uşak Üniversitesi: Uşak.
- Alterman, Anton, (2003), “A Piece of Yourself: Ethical Issues in Biometric Identification”, *Ethics and Information Technology*, 2003, Cilt: 5, ss.139–150.
- Ashbourn, Julian, (2004), *Practical Biometrics: From Aspiration to Implementation*, Londra: Springer-Verlag.
- Aslan, Nazlı Sinem, (2010), *Migration And Security: History, Practice And Theory*, Bilkent Üniversitesi Ekonomik ve Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Ankara.
- Başlar, Kemal, (2005), “Uluslararası Hukuk ve İnternet”, *Uluslararası Hukuk ve Politika*, Cilt: 1, Sayı:1, ss.19–42.
- Bozkurt, Enver; Özcan, Mehmet ve Köktaş, Arif, (2008), *Avrupa Birliği Hukuku*, Ankara, Türkiye: Asil Yayınları.
- Broeders, Dennis, (2011), *Migration and Global Environmental Change: New Technologies and the Monitoring and Management of Migration Flows and Population Displacement*. Londra: UK Government Office for Science.
- Brown, David ve Brook, David, (2003), “Biometrics: Implications and Applications for Citizenship and Immigration”, *Report on a Forum Hosted by Citizenship and Immigration Canada*, 7–8 Ekim 2003, Kanada.
- Busch, Cristopher, (2006), “Facing the Future of Biometrics”, *EMBO Reports*, Cilt: 7, ss.23–25.

- Buz, Sema, (2008), “Türkiye Sığınma Sisteminin Sosyal Boyutu”, *TBB Dergisi*, Sayı: 76, ss.120–130.
- Carrera, Sergio, (2011), “The EU’s Dialogue on Migration, Mobility and Security with the Southern Mediterranean: Filling the Gaps in the Global Approach to Migration”, *Centre for European Policy Studies(CEPS) Policy Brief*, Sayı: 41.
- Commission, (2004), COM 2004/116, *Proposal for a Council Regulation on Standards for Security Features and Biometrics in EU Citizens’ Passports*, 18 Şubat 2004.
- Crompton, Malcolm, (2002), “Biometrics and Privacy The End of The World as We Know It or The White Knight of Privacy?”, *Biometrics – Security and Authentication Biometrics Institute Conference*, 20 Mart 2002, Sidney.
- Çiçekli, Bülent, (2003), “Uluslararası Terörizm Ve Uluslararası Göç: 11 Eylül Sonrası Terör Tehdidi ve Göç Kontrol Politikalarının Terörizmle Mücadelede Kullanımı”, *Avrasya Dosyası, Güvenlik Bilimleri Özel Sayı*, Yaz 2003, Cilt: 9, Sayı: 2, ss.170–194.
- Çiçekli, Bülent, (2005), “Yasa Dışı Göç, İnsan Kaçakçılığı ve İnsan Ticareti ile Mücadele ve Türkiye”, *Polis Bilimleri Dergisi*, Cilt: 7, Sayı: 1, ss.43–57.
- Das, Ravi, (2006), “An Introduction to Biometrics: A Concise Overview of the Most Important Biometric Technologies”, *Keesing Journal of Documents ve Identity*, Sayı: 17, ss.3–5.
- Demirci, M. Deniz, (2005), *Bilgisayar Destekli Ses Tanıma Sistemi Tasarımı*, İstanbul Üniversitesi Fen Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.
- DHS-Department of Homeland Security, (2010), *2009 Yearbook of Immigration Statistics: Office of Immigration Statistics*, Alexandria, Virginia: National Technical Information Service (NTIS).
- Doğan, Serap, (2007), *Avrupa Birliği’nde Göçün Güvenlikleştirilmesi*, Yıldız Teknik Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

- Durmuş, Sinem Özer, (2010), *İristen Kimlik Tanıma*, Kocaeli Üniversitesi Fen Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Kocaeli.
- Ergen, Burhan ve Çalışkan, Abidin, (2011), “Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri”, *6th International Advanced Technologies Symposium (IATS’11)*, 16–18 Mayıs 2011, Elazığ, ss.455–460.
- Ertem, Haşim Emre, (2007), *Illegal Immigration to EU Countries; New Asylum Policies in Spain and Germany*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.
- Feldman, Robin, (2004), “Considerations on the Emerging Implementation of Biometric Technology”, *25 Hastings Communications and Entertainment Law Journal*, Cilt: 25, ss.653–682.
- Frontex, (2007), *BIOPASS: Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports*, Varşova: Research and Development Unit of Frontex.
- Frontex, (2011a), *Annual Risk Analysis*, FrontexReference Number: 4591, Varşova: Risk Analysis Unit of Frontex.
- Frontex, (2011b), *Operational and Technical Security of Electronic Passports*, Varşova.
- Frontex, (2011c), *FRAN Quarterly Sayı: 3*, Frontex Reference Number: 107, Varşova: Risk Analysis Unit of Frontex.
- Frontex, (2012), *Annual Risk Analysis*, Frontex Reference Number: 5202, Varşova: Risk Analysis Unit of Frontex.
- Gellert, Raphaël ve Gutwirth, Serge, (2011), “Chapter 3, Privacy, Data Protection and Policy Issues in RFID Enabled E-Passports”, Rachel Finn ve David Wright (Der.), *Privacy and Emerging Fields of Science and Technology: Towards a Common Framework for Privacy and Ethical Assessment (PRESCIENT)*, Seventh Framework Programme for Research and Technological Development, Project number: 244779, Brüksel, ss.31–39.
- Grossman, Wendy, M., (2005), “Identifying Risks: National Identity Cards”, *Scripted*, Cilt: 2, Sayı: 1, Mart 2005, ss.4–19.

- Guild, Elspeth; Carrera, Sergio ve Geyer, Fyorian, (2008), "The Commission's New Border Package: Does It Take Us One Step Closer to a Cyber Fortress Europe?", *Centre for European Policy Studies(CEPS) Policy Brief*, Sayı: 154.
- Gümüř, Mahir ve Kara, Canan Öykü Dönmez, (2009), "İnsan Hakları Bağlamında Türkiye'de Sığınmacıların Yerleşimi ve Konut Sorunları", *Uluslararası Davraz Kongresi*, 24–27 Eylül 2009, Isparta, ss.2835–2853.
- Haddal, Chad C., (2010), *Border Security: The Role of the U.S. Border Patrol*. Washington, D.C.: Congressional Research Service.
- Hanson, Gordon H, (2004), "Challenges for US Immigration Policy", C. Fred Bergsten (Der.), *The United States and the World Economy: Foreign Economic Policy for the Next Decade*, Washington DC: Institute of International Economics, 2005, ss.343–372.
- Hanson, Gordon H, (2007), *The Economic Logic of Illegal Immigration*, CSR No 26, Nisan 2007, Council On Foreign Relations.
- Hert, Paul De, (2005), *Biometrics: Legal Issues and Implications, Background Paper for the Institute of Prospective Technological Studies*, DG JRC, Sevilla, European Commission.
- Hornung, Gerrit, (2007), "The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Standards", *Script-ed*, Cilt: 4, Sayı: 3, Eylül 2007, ss.246–259.
- ICAO-International Civil Aviation Organization, (2004), *Biometrics Deployment of Machine Readable Travel Documents*, Technical Report, Version 2.0 Tag 15, ICAO TAG MRTD/NTWG.
- ICAO-International Civil Aviation Organization, (2007), *Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation*, Technical Report, Sürüm: 1 Taslak: 1,4, ICAO TAG MRTD/NTWG.
- Juels, Ari; Molnar, David ve Wagner, David, (2005), "Security and Privacy Issues in E-Passports", *Securecomm '05 Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, 5-9 Eylül 2005, Atina, Yunanistan.

- JRC-Joint Research Centre, (2003), *Security and Privacy in the Post-September 11 Digital Age: A Prospective Overview*, European Commission.
- JRC-Joint Research Centre, (2005), *Biometrics at the Frontiers: Assessing the Impact on Society*, Spain, European Commission.
- JRC-Joint Research Centre. (2008), *Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats*, Spain, European Commission.
- Kajevic, Belhira, (2006), *Biometrics: A New Mean of Surveillance and Migration Control*, Malmö University Yayınlanmamış Yüksek Lisans Tezi, Malmö, İsveç.
- Kanat, Selim, (2005), *Terörizm, İnsan Hakları, Güvenlik: 11 Eylül Sonrası Meydana Gelen Değişiklikler*, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Isparta.
- Kartal, Harun, (2008), *Avrupa Birliği'nin Yasadışı Göç Politikası ve Türkiye'ye Yansımaları*, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Ankara.
- Kaya, Feridun, (2009), *Türkiye'de Kredi Kart Uygulaması*, Türkiye Bankalar Birliği, Yayın No: 263, İstanbul.
- Kaymaz, Sinan, (2010), *Çevrimdışı İmza Tanıma*, Marmara Üniversitesi Fen Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.
- Khanat, Arman, (2008), *11 Eylül Terörist Saldırıları Sonrasında ABD'nin Terörle Mücadele Stratejilerinde Yaptığı Değişikliklerin İnsan Hakları Uygulamalarına Etkisi*, Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara.
- Koyuncu, Seda Ayşe, (2006), *Göçmen Kaçakçılığı İle Mücadele Politikaları*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.
- Köktaş, Arif ve Yılmaz, Ömer, (2010), "Avrupa Birliği Bütünleşmiş Sınır Yönetimi Modeli: Schengen Sözleşmesinden Stockholm Programına", *Polis Bilimleri Dergisi*, Cilt: 12, Sayı: 2, ss.1–22.

- Kumar, V. Narendira; Sirinivasan, B. ve Narendran, P., (2012), “Efficient Implementation of Electronic Passport Scheme Using Cryptographic Security Along With Multiple Biometrics”, *Information Engineering and Electronic Business*, Cilt:1, ss.18–24.
- Liu, Yue, (2008), “Identifying Legal Concerns in the Biometric Context”, *Journal of International Commercial Law and Technology*, Cilt:3, Sayı:1, ss.45–54.
- Liu, Yue, (2009), “The Principle of Proportionality in Biometrics: Case Studies From Norway”, *Computer Law & Security Review*, Cilt: 25, ss.237–250.
- Liu, Yue, (2011), “Scenario Study of Biometric Systems at Borders”, *Computer Law & Security Review*, Cilt: 27, ss.36–44.
- Mansfield, Andrew J. ve Wayman, John L, (2002), *Best Practices in Testing and Reporting Performance of Biometric Devices Version 2.01*. Middlesex, İngiltere: National Physical Laboratory Report CMSC 14/02.
- Martin, Philip L, (2004), “The United States: The Continuing Immigration Debate”, Wayne Cornelius; Philip Martin ve James Hollifield (Der.), *Controlling Immigration: A Global Perspective*, Stanford, California, Stanford University Press, ss.51–90.
- Meissner, Doris ve Kerwin, Donald, (2009), *DHS and Immigration: Taking Stock and Correcting Course*, (2010), Alexandria, Virginia: National Technical Information Service (NTIS).
- Monger, Randall ve Mathews, Megan, (2011), *Annual Flow Report: Nonimmigrant Admissions to the United States: 2010*, Department of Homeland Security, Office of Immigration Statistics.
- Ng-Kruelle, Grace; Swatman, Paul A.; Hampe, J. Felix ve Rebne, Douglas, S., (2006), “Biometrics and e-Identity (e-Passport) in the European Union: End-User Perspectives on the Adoption of a Controversial Innovation”, *Journal of Theoretical and Applied Electronic Commerce Research*, Cilt:1, Sayı:2, ss.12—35.

- OECD, (2004), *Working Party on Information Security and Privacy: Biometric based Technologies*, DSTI/ICCP/REG(2003)2/FINAL, Paris, Fransa: Head of Publications Service, OECD.
- Özcabı, Yasin, (2007), *Kütlesel Göçlerin Ülkelerin Güvenlik İhtiyacı Üzerine Etkisi*, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.
- Özcan, Mehmet ve Yılmaz, Fatma, (2007), “Pendulum Swings in between Civil Rights and Security: EU Policies against Terrorism in the Light of the PNR Case”, *Uluslararası Hukuk ve Politika*, Cilt: 3, Sayı: 12, ss.99–118.
- Özeren, Süleyman ve Cinoğlu, Hüseyin, (2006), “Terörizm ve Amerika Birleşik Devletleri: 11 Eylül Öncesi ve Sonrası Terörle Mücadele Politikalarının Değerlendirilmesi”, İhsan Bal (Der.) *Terörizm*, Ankara: Usak Yayınları, ss.160–187.
- Pedreza, Juanita; Patricio, Miguel A.; Asis, Agustin De ve Jose, M. Molina, (2010), “Privacy and Legal Requirements for Developing Biometric Identification Software in Context-Based Applications”, *International Journal of Bio-Science and Bio-Technology*, Cilt 2, Sayı 1, Mart 2010, ss.13-24.
- Redpath, Jillyanne, (2005), “Biometrics And International Migration”, *International Migration Law*, International Organization for Migration (IOM), Sayı: 5, Cenevre, İsviçre, ss.1–31.
- Redpath, Jillyanne, (2007), “Biometrics And International Migration”, *Ann Ist Super Sanita*, Cilt: 43, Sayı 1: ss.27–35.
- Rudolph, Cristopher, (2006), *National Security and Immigration: Policy Development in the US and Western Europe since 1945*, Stanford, California, Stanford University Press.
- Sergio Carrera, (2011), “The EU’s Dialogue on Migration, Mobility and Security with the Southern Mediterranean: Filling the Gaps in the Global Approach to Migration”, *Centre for European Policy Studies(CEPS)*.

- Somuncu, Başak, (2006), *Türkiye'nin Avrupa Birliği'ne Tam Üyelik Sürecinde Uluslararası Göç Politikası*, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İzmir.
- Stock, Margaret, (2006), "Immigration and National Security: Post 9/11 Changes for the U.S.", James J. Forest, (Der.), *Homeland Security: Protecting America's Targets*. Praeger Security International, ss:118–125.
- Subcommittee on Biometrics, (2006), *Privacy & Biometrics: Building a Conceptual Foundation*, National Science and Technology Council (NSTC).
- Subcommittee on Biometrics, (2008), *Biometrics in Government: Post 9/11*, National Science and Technology Council (NSTC).
- Survey, (2004), "Biometrics and ePassports", *Biometric Technology Today*, Temmuz-Ağustos 2004, Cilt: 12, Sayı: 7, ss.19–11.
- Tanış, Metin, (28 Mart 2012), 1. Sınıf Emniyet Müdürü, Emniyet Genel Müdürlüğü Pasaport Daire Başkanı ile Yapılan Görüşme.
- Terzioğlu, Mehmet, (2002), "Yasadışı Göç, İnsan Ticareti ve İltica Konularında Ülkemizin Durumu ve Yapılan Çalışmalar", *Çağın Polisi Dergisi*, Yıl: 1, Sayı: 12, ss.15–19.
- Tetik, Erdoğan, (2004), "Kimlik Tespitinde Parmak İzi Arşivlerinin Gerekliliği ve Ülkemizdeki Durumun Değerlendirilmesi", *Çağın Polisi Dergisi*, Yıl: 3, Sayı: 35, ss.42–47.
- Thomas, Rebekah, (2005), "Biometrics, International Migrants and Human Rights", *European Journal of Migration and Law*, Cilt: 7, ss.377–411, 2005,Hollanda.
- T-PD- Consultative Committee of the Convention for the Protection of Individuals with Regard To Automatic Processing Of Personal Data, (2005). *Progress Report on the Application of the Principles Of Convention 108 to the Collection and Processing of Biometric Data*, Council of Europe.
- Uçan, Aytaç, (2010), *Pasaport Sahteciliği Dosyalarının Yeni Elektronik Pasaport Tanzim Sistemi Açısından Değerlendirilmesi*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Ankara.

- Uzun, Mehmet Semih, (2006), *Akıllı Kart Teknolojisiyle Geliştirilmiş Elektronik Pasaport ve Vize Sistemi*, Yıldız Teknik Üniversitesi Fen Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.
- Ünsal, Zeynep, (2007), *Güvenlik Eksenli Bir Bakış Açısından Avrupa’da Değişen Göç Politikaları*, Başkent Üniversitesi Avrupa Birliği ve Uluslararası İlişkiler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Ankara.
- Vakalis, Ioannis, (2011), “Privacy and Biometric Passports”, *The Scientific World Journal*, Cilt: 11, ss.478–489.
- Yadav, Shyam Sundar; Gothwal, Jitendra Kumar ve Singh, Ram, (2011), “Multimodal Biometric Authentication System: Challenges and Solutions”, *Global Journal of Computer Science and Technology*, Cilt: 11, Sayı 16 Eylül 2011, ABD.

İnternet Kaynakları

- Clarke, Robert, (2001), “Biometrics and Privacy”, <http://www.rogerclarke.com/DV/Biometrics.html> (Erişim Tarihi: 01 Ekim 2011).
- Commission. (2007), COM 2007/512, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Third Annual Report on Migration and Integration*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0512:EN:NOT> (Erişim Tarihi: 30 Ekim 2010).
- Commission, (2010), COM 2010/214, *Report from the Commission to the European Parliament and the Council - First Annual Report on Immigration and Asylum*, (2009), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0214:FIN:EN:PDF> (Erişim Tarihi: 30 Ekim 2010).
- Council, (2004), Council Regulation (EC) No 2252/2004 of 13 December 2004 on *Standards For Security Features And Biometrics in Passports And Travel Documents Issued By Member States*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:EN:PDF> (Erişim Tarihi: 1 Nisan 2009).
- Çehreli, Murat, (2011), “SGK, 2012'de Damar ile Kimlik Doğrulaması Yapacak”, <http://www.turk.internet.com/portal/yazigoster.php?yaziid=34969> (Erişim Tarihi: 20 Şubat 2012).
- Çiçekli, Bülent, (2004), “Impact of Turkish-EU Accession Process on the Development of Turkish Immigration Law”, *Legal Workshop on the Challenge of Migration to Legal Systems*, <http://www.turkishweekly.net/articles.php?id=21>, 29 Haziran-1 Temmuz 2004, Londra (Erişim Tarihi: 15 Ekim 2011).
- Drygajlo, Andrzej, (2009), “Biometrics Lecture Part1 2009–2010 2009-09-14, Speech Processing and Biometrics Group”, *Institute of Electrical Engineering, Ecole Polytechnique Fédérale de Lausanne (EPFL)*, <http://scgwww.epfl.ch/courses> (Erişim Tarihi: 14 Eylül 2009).

- EU Press Release, (2006), “New, Secure Biometric Passports in the EU, Strengthen Security and Data Protection and Facilitates Travelling”, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/872&type=HTML&aged=0&language=EN&guiLanguage=en> (Eriřim Tarihi: 14 Aralık 2011).
- EU Press Release, (2011), “EUROSUR: ‘Connecting the Dots’ in Border Surveillance (Eurosur Sınır Kontrol Sistemi Kuruluyor)”, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1528> (Eriřim Tarihi: 1 Mart 2012).
- Euractiv, (2007a), ”EU Backs Biometrics Visa Database”, <http://www.euractiv.com/en/security/eu-backs-biometrics-visa-database/article-164,422>(Eriřim Tarihi: 21 Kasım 2010).
- Euractiv, (2007b), ”EU Countries to Issue Biometric Passports by end 2005”,<http://www.euractiv.com/en/security/eu-countries-issue-biometric-passports-2005/article-117813>(1 Aralık 2011).
- Fano, Tomas, (2010), “Will 12 Million Illegal Immigrants in US Get Much Needed Relief in 2010?” <http://www.globalmobilityreport.com/50226711/will-12-million-illegal-immigrants-in-us-get-much-needed-relief-in-2010.php> (Eriřim Tarihi: 30 Ekim 2010).
- Frattini, Franco, (2005), “The Green Paper on an EU Approach to Managing Economic Migration”, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/05/364&format=HTML&aged=1&language=EN&guiLanguage=en> (Eriřim Tarihi: 04 Aralık 2011).
- Graham-Rowe, Duncan, (2003), “Biometric cards will not stop identity fraud”, <http://www.newscientist.com/article/dn4393> (Eriřim Tarihi: 1 Nisan 2009).
- Glten, Glmhan, (2011), “SGK, Vatandařı Artık Avu İinden Tanıyacak”, <http://haber.gazetevatan.com/sgk-vatandasi-artik-avuc-icinden-taniyacak/386249/2/Haber> (Eriřim Tarihi: 15 Nisan 2012).
- Hrriyet, (2010), “Turkey to Introduce Biometric Passports in June”, <http://www.hurriyetdailynews.com/n.php?n=turkey-to-introduce-biometric-passports-in-june-2010-03-25> (Eriřim Tarihi: 10 Kasım 2011).

- IOM -International Organization for Migration, (2011), “IOM 2011 Global Estimates and Trends”, <http://iom.int/jahia/Jahia/about-migration/facts-and-figures/lang/en> (Eriřim Tarihi: 28 Ocak 2012).
- McCabe, Kristen ve Meissner, Doris, (2010), “Immigration and the United States: Recession Affects Flows, Prospects for Reform”, Migration Policy Institute, <http://www.migrationinformation.org/Profiles/display.cfm?ID=766> (Eriřim Tarihi: 30 Ekim 2010).
- McGowan, William, (2003), “Postscript 9/11 Media Coverage of Terrorism and Immigration”, Center for Immigration Studies, Backgrounder, <http://www.cis.org/articles/2003/back603.html> (Eriřim Tarihi: 23 Kasım 2011).
- Posta, (2012), (http://www.posta.com.tr/turkiye/HaberDetay/SGK_avuc_ici_damar_okuma_sistemine_geciyor.htm?ArticleID=110545 Eriřim Tarihi: 15 Nisan 2012).
- PublicTechnology, (2007), “Biometric Eye-scanning Border-control System Goes Live at Gatwick Airport, <http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=9303> (Eriřim Tarihi: 19 Aralık 2011).
- Rissanen, Teemu, (2010), “Electronic identity in Finland: ID cards vs. bank IDs”, <http://rd.springer.com/article/10.1007/s12394-010-0049-8> (Eriřim Tarihi: 19 Kasım 2011).
- Roberts, Chris, (2005), “Biometrics”, <http://www.scribd.com/doc/51355755/biometrics> (Eriřim Tarihi: 10 Mart 2012).
- Saęlık Aktüel, (2012), (<http://www.saglikaktuel.com/haber/sgkdan-avuc-ici-tarama-1-temmuzda-24793.htm> Eriřim Tarihi: 15 Nisan 2012).
- Sosyal Güvenlik Kurumu, (2011), (<http://www.sgk.com.tr/560-Haber-sgk-vatandasi-artik-avuc-icinden-taniyacak.html> Eriřim Tarihi: 15 Nisan 2012).
- The National Commission on Terrorist Attacks upon the United States, (2004), (<http://www.9-11commission.gov/> Eriřim Tarihi: 25 Aralık 2010).

Warren, Samuel ve Brandeis, Louis, (1890), “The Right to Privacy”, *Harvard Law Review*, Cilt IV 1890–91”, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (Eriřim Tarihi: 10 Ocak 2011).