T.C.
KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANA BİLİM DALI

AKILLI KİMLİK KARTLARININ GÜVENLİK VE MAHREMİYET AÇISINDAN İNCELENMESİ: KARAMAN İLİ ÖRNEĞİ

NESİBE MAHUR ŞAHİN

YÜKSEK LİSANS TEZİ

Danışman: Doç. Dr. Ali YILDIRIM

TEMMUZ - 2024

T.C.
KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

AKILLI KİMLİK KARTLARININ GÜVENLİK VE MAHREMİYET AÇISINDAN İNCELENMESİ: KARAMAN İLİ ÖRNEĞİ

YÜKSEK LİSANS TEZİ

Nesibe Mahur ŞAHİN

Enstitü Anabilim Dalı: Siyaset Bilimi ve Kamu Yönetimi
Enstitü Bilim Dalı : Kamu Yönetimi

"Bu tez 26/07/2024 tarihinde yüzyüze olarak savunulmuş olup aşağıdaki isimleri bulunan jüri üyeleri tarafından Oybirliği / Oyçokluğu ile kabul edilmiştir."

JÜRİ ÜYESİ	KANAATİ

ETİK BEYAN METNİ

Enstitünüz tarafından Uygulama Esasları çerçevesinde alınan Benzerlik Raporuna göre yukarıda bilgileri verilen tez çalışmasının benzerlik oranının herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve Etik Kurul Onayı gerektiği takdirde onay belgesini aldığımı beyan ederim.

Etik kurul onay belgesine ihtiyaç var mıdır?

Evet ■

Hayır □

(Etik Kurul izni gerektiren araştırmalar aşağıdaki gibidir:

- Anket, mülakat, odak grup çalışması, gözlem, deney, görüşme teknikleri kullanılarak katılımcılardan veri toplanmasını gerektiren nitel ya da nicel yaklaşımlarla yürütülen her türlü araştırmalar,
- İnsan ve hayvanların (materyal/veriler dahil) deneysel ya da diğer bilimsel amaçlarla kullanılması,
- İnsanlar üzerinde yapılan klinik araştırmalar,
- Hayvanlar üzerinde yapılan araştırmalar,
- Kişisel verilerin korunması kanunu gereğince retrospektif çalışmalar.)

Nesibe Mahur ŞAHİN

26.07.2024

ÖNSÖZ

Akıllı kart teknolojileri, özellikle teknolojik gelişmelerin çok hızlı yaşandığı günümüzde giderek daha fazla önem kazanmaktadır. Bu teknolojilerin alt kümesi olan akıllı kimlik kartları ise, bireylerin kimlik doğrulama süreçlerinde merkezi bir rol oynamaktadır. Günümüzde, bu kartların güvenlik ve mahremiyet açısından sunduğu avantajlar ve potansiyel riskler hem bireylerin hem de kurumların dikkatini çekmektedir. Bu bağlamda, "Akıllı Kimlik Kartlarının Güvenlik ve Mahremiyet Açısından İncelenmesi: Karaman İli Örneği" başlıklı bu çalışma, akıllı kartların ve özellikle akıllı kimlik kartlarının önemini vurgulayarak, Karaman ilinde bu teknolojiler hakkındaki genel bilgi durumunu anlamayı ve değerlendirmeyi amaçlamaktadır.

Bu zorlu ve detaylı çalışma sürecinde yanımda olanlara minnettarlığımı ifade etmek istiyorum. Değerli danışmanım Sayın Doç. Dr. Ali Yıldırım'a, bilgi birikiminden derinlemesine faydalandığım ve bu süreçte beni destekleyip motive eden rehberliği için teşekkür ederim. Ayrıca, çalışmamı objektif bir bakış açısıyla değerlendirerek yapıcı eleştirilerini paylaşan ve bilge gözlemleriyle çalışmama önemli katkılarda bulunan çok değerli jüri üyesi Dr. Dilek Çelik'e teşekkür ediyorum.

Özel bir teşekkürü de zorlu süreçte sabır ve anlayışlarıyla her daim yanımda olan çok kıymetli aileme borçluyum. Bu destek, bu yoğun süreçte beni daha da güçlendirdi.

Umarım ki, bu çalışma akıllı kimlik kartlarının güvenlik ve mahremiyet açısından daha iyi anlaşılması konusunda yeni ufuklar açmamıza vesile olur.

Saygılarımla,

Nesibe Mahur ŞAHİN

İÇİNDEKİLER

ÖNSÖZ ..... **i**
İÇİNDEKİLER ..... **i**
KISALTMALAR ..... **iv**
TABLO LİSTESİ ..... **v**
ŞEKİL LİSTESİ ..... **vi**
ÖZET ..... **vii**
ABSTRACT ..... **viii**
GİRİŞ **1**
1. BÖLÜM: ARAŞTIRMA TASARIMI VE METODOLOJİ **3**
1.1. Araştırmanın Amacı ve Önemi 3
1.2. Araştırmanın Yöntemi 3
1.3. Araştırmanın Evreni ve Örneklemi 4
1.4. Araştırma Deseni 4
1.5. Veri Toplama Araçları 5
1.6. Verilerin Analizi 9
1.7. Araştırmanın Geçerlik ve Güvenirliği 11
1.8. Araştırmanın Sınırlılıkları 13
1.9. Araştırma Sorusu ve Hipotezler 13
2. BÖLÜM: AKILLI KİMLİK KARTLARI KAVRAMSAL ÇERÇEVE **15**
2.1. Akıllı Kart Teknolojilerine Giriş 15
2.2. Akıllı Kartların Kullanım Alanları 15
2.3. Akıllı Kimlik Kartlarının Tanımı ve Özellikleri 16
2.4. Akıllı Kimlik Kartı Tipleri 17
2.5. Akıllı Kimlik Kartlarının Tarihçesi ve Evrimi 18
2.5.1. Global Perspektifte Akıllı Kimlik Uygulamaları 19
2.5.2. Türkiye Özelinde Uygulama: Türkiye Cumhuriyeti Kimlik Kartı ... 22
2.6. Akıllı Kimlik Kartı İçeriği ve Sistemin Yapısı 23
2.6.1. MERNİS 24
2.6.2. Kart Yönetim Sistemleri 24
2.6.3. Elektronik Kimlik Doğrulama Sistemi 25
2.6.4. Emniyet Trafik Kontrol Sistemi 25
2.6.5. Sağlık Bilgi Sistemi 26

2.6.6. Nakit Akış Sistemi 27
2.7. NFC (Near Field Communication-Yakın Alan İletişimi) ve Akıllı Kimlik Kartları 27
2.8. Akıllı Kimlik Kartlarının Avantajları ve Potansiyel Riskleri 30
2.8.1. Akıllı Kimlik Kartlarının Avantajları 30
2.8.2. Akıllı Kimlik Kartlarının Potansiyel Riskleri (Dezavantajları) 32
3. BÖLÜM: MAHREMİYET VE GÜVENLİK BAĞLAMINDA AKILLI KİMLİK KARTLARI **34**
3.1. Mahremiyetin Tanımı ve Toplumsal Önemi 34
3.2. Mahremiyetin Tarihsel Gelişimi ve Kökenleri 35
3.3. Küresel Mahremiyet Normları ve İlkeleri 36
3.3.1. GDPR'nin İncelenmesi ve Etkileri 36
3.3.2. Birleşmiş Milletler Mahremiyet İlkeleri 36
3.3.3. Diğer Küresel Anlaşmalar ve İlkeler 38
3.4. Akıllı Kimlik Kartları ve Mahremiyet İlişkisi 39
3.5. Akıllı Kimlik Kartlarının Mahremiyet Perspektifinden Hukuki Analizi 41
3.5.1. Kişisel Verilerin Korunması Bağlamında Akıllı Kimlik Kartları 43
3.5.2. Mahremiyet İhlalleri ve Hukuki Sonuçları 44
3.5.3. Karşılaştırmalı Hukukta Akıllı Kimlik Kartları ve Mahremiyet 45
3.5.3.1. ABD 45
3.5.3.2. Almanya 46
3.5.3.3. İngiltere 46
3.6. Akıllı Kimlik Kartları ve Güvenlik 47
3.6.1. Sistemin Güvenlik Özellikleri 48
3.6.2. Akıllı Kimlik Kartlarında Güvenlik İle İlgili Endişeler 50
3.6.2.1. Kart Kaybı ve Çalınması Durumu 50
3.6.2.2. Yetkisiz Erişim Riskleri 50
3.6.2.3. Veri Sızıntısı Tehlikesi 51
3.6.2.4. Kartın Fiziksel Kopyalanması ve Sahtecilik 52
4. BÖLÜM: BULGULAR **53**
4.1. Demografik Bilgiler 53
4.2. Katılımcı Yanıtları 55
4.2.1. Katılımcıların Akıllı Kimlik Kartlarının Mahremiyetine Yönelik Farkındalık Algısı 63

4.2.2. Akıllı Kimlik Kartlarının Mahremiyet ve Güvenlik Arasındaki İlişki 66

4.2.3. Akıllı Kimlik Kartlarının Kullanımı ve Mahremiyet Endişeleri Arasındaki İlişki 68

4.2.4. Akıllı Kimlik Kartlarının Yasal Düzenlemelere İlişkin Güvenilirliği ve Mahremiyet Algısı Arasındaki İlişki 70

4.3. Katılımcı Önerileri 71

5. BÖLÜM: SONUÇ ve DEĞERLENDİRME 75

KAYNAKÇA 80

EK 86

ÖZGEÇMİŞ 89

KISALTMALAR

AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
DLPS	:	Data Leak Prevention Systems-Veri Sızıntısı Önleme Sistemleri
DPA	:	Differential Power Analysis-Farklılık Güç Analizi
ECHR	:	European Court of Human Rights-Avrupa İnsan Hakları Sözleşmesi
EKDS	:	Elektronik Kimlik Doğrulama Sistemi
GB	:	Gigabyte
GDPR	:	General Data Protection Regulation-Genel Veri Koruma Yönetmeliği
ICAO	:	International Civil Aviation Organisation- Uluslararası Sivil Havacılık Organizasyonu
ICC	:	Entegre Devreli Kart
KİK	:	Körfez Arap Ülkeleri İş Birliği Konseyi
KVKK	:	Kişisel Verilerin Korunması Kanunu
MERNİS	:	Merkezi Nüfus İdaresi Sistemi
NFC	:	Near Field Communication-Yakın Alan İletişimi
OAS	:	Organization of American States-Amerikan Devletleri Örgütü
POS	:	Point Of Sale-Satış Noktası
RAM	:	Random Access Memory-Rastgele Erişim Belleği
RFID	:	Radio Frequency Identification- Radyo Frekansı Tanımlama
ROM	:	Read-only Memory-Sadece Okunabilir Bellek
SCADA	:	Supervisory Control And Data Acquisition-Gözetim Kontrol ve Veri Toplama
SIM	:	Subscriber Identity Module-Abone Kimlik Modülü
SNIC	:	Smart National Identity Cards-Akıllı Ulusal Kimlik Kartı
T.C.	:	Türkiye Cumhuriyeti
TÜBİTAK	:	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UN	:	The United Nations-Birleşmiş Milletler (BM)
UNPPG	:	The United Nations Privacy Policy Group-BM Gizlilik Politikası Grubu

TABLO LİSTESİ

Tablo 1. Katılımcı ve Görüşme Bilgileri 9
Tablo 2. Katılımcıların Demografik Bilgileri 53
Tablo 3. Katılımcı Görüşlerine İlişkin Tablo..... 55
Tablo 4. Hipotezlere İlişkin Tablo 73

ŞEKİL LİSTESİ

Şekil 1. ID-1 Kart Görünümü 18
Şekil 2. Türkiye'de Akıllı Kimlik Kartlarının Kronolojik Olarak Gelişimi 19
Şekil 3. Türkiye Cumhuriyeti Kimlik Kartı Görseli Ön ve Arka Yüz 23
Şekil 4. NFC Teknolojisi Kullanım Alanları 28
Şekil 5. NFC ile Akıllı Kimlik Kartı Doğrulama İşlemi 29

ÖZET

Başlık: Akıllı Kimlik Kartlarının Güvenlik ve Mahremiyet Açısından İncelenmesi: Karaman İli Örneği

Yazar: Nesibe Mahur ŞAHİN

Danışman: Doç. Dr. Ali YILDIRIM

Kabul Tarihi: **Sayfa Sayısı:**

Bu araştırma, vatandaşların akıllı kimlik kartlarına ilişkin mahremiyet algılarını ve güvenlik endişelerini incelemeyi amaçlamaktadır. Karaman il merkezinde yaşayan ve 18 yaşından büyük 30 reşit bireyden oluşan bir örneklem grubu üzerinde yapılan çalışmada, katılımcılara yarı yapılandırılmış görüşme formuyla 15 açık uçlu soru yöneltilmiştir. Araştırma sonuçları, katılımcıların genel olarak akıllı kimlik kartlarının güvenlik önlemlerini yetersiz bulduklarını ve çalınması veya kaybolması gibi durumlarda ciddi sorunlar yaşanabileceği endişesi taşıdıklarını ortaya koymaktadır. Bu bağlamda, katılımcılar resmi bilgilendirmenin eksikliğini ve daha etkili güvenlik önlemlerinin alınması gerekliliğini vurgulamışlardır. Mahremiyet konusunda, katılımcılar kişisel verilerin izinsiz erişime karşı korunması gerektiğini ve kartlardaki bilgi gizliliğinin daha etkin bir şekilde sağlanması gerektiğini belirtmişlerdir. Bazı katılımcılar, bilgi gizliliğini artırmak için kartlarda daha az bilgi bulunması gerektiğini önermişlerdir. Öneriler kısmında, katılımcılar daha etkili güvenlik önlemleri, şeffaf bilgilendirme süreçleri ve mahremiyetin korunması için daha sıkı yasal düzenlemeler talep etmektedir. Ayrıca, kişisel verilerin sınırlı tutulması, daha güçlü şifreleme yöntemlerinin kullanılması ve izinsiz erişimi engellemek için ek önlemler alınması gerektiği önerilmiştir. Sonuç olarak, bu çalışma, vatandaşların akıllı kimlik kartlarıyla ilgili güvenlik ve mahremiyet konularında ciddi endişeler taşıdığını göstermektedir. Bu endişelerin giderilmesi için daha etkili güvenlik önlemleri alınması, şeffaf bilgilendirme süreçlerinin sağlanması ve mahremiyetin korunması için daha sıkı yasal düzenlemelerin hayata geçirilmesi gerekmektedir. Bu önerilerin, akıllı kimlik kartlarının güvenliği ve kullanımıyla ilgili politika yapıcılar ve ilgili kurumlar tarafından dikkate alınması gerekmektedir.

Anahtar Kelimeler: Akıllı Kartlar, Akıllı Kimlik Kartı, Güvenlik, Mahremiyet, Reşit Bireyler.

ABSTRACT

Title of Thesis: Investigation of Security and Privacy Views of Minors on Smart ID Cards: The Case of Karaman

Author of Thesis: Nesibe Mahur ŞAHİN

Supervisor: Assoc. Prof. Ali YILDIRIM

Accepted Date: **Number of Pages:**

This study aims to examine the privacy perceptions and security concerns of citizens regarding smart identity cards. Conducted on a sample group consisting of 30 adult individuals aged 18 and over residing in the city center of Karaman, the research employed a semi-structured interview form comprising 15 open-ended questions. The findings of the study reveal that participants generally find the security measures of smart identity cards inadequate and express concerns about potential serious problems in case of theft or loss. In this context, participants emphasized the lack of official information and the necessity for more effective security measures. Regarding privacy, participants stated that personal data should be protected against unauthorized access and emphasized the need for more effective safeguarding of information privacy on cards. Some participants suggested reducing the amount of information on cards to enhance data privacy. In the recommendations section, participants called for more effective security measures, transparent information processes, and stricter legal regulations to protect privacy. Additionally, it was suggested to limit personal data, employ stronger encryption methods, and implement additional measures to prevent unauthorized access. In conclusion, this study demonstrates that citizens harbor serious concerns regarding the security and privacy aspects of smart identity cards. To address these concerns, it is essential to implement more effective security measures, ensure transparent information processes, and enact stricter legal regulations to safeguard privacy. These recommendations should be taken into account by policymakers and relevant authorities in ensuring the security and appropriate usage of smart identity cards.

Keywords: Smart Cards, Smart Identity Card, Security, Privacy, Adult Individuals.

GİRİŞ

İnsanın temel ihtiyaçları fizyolojik, güvenlik, sevgi, kendini gerçekleştirme, aidiyet, bilmek ve anlamak şeklinde sıralanabilir (Maslow, 1943). Bu ihtiyaçlar, biri giderildiğinde diğeri ortaya çıkan bir piramit şeklinde örgütlenmektedir. Başka bir ifade ile, insan fizyolojik ihtiyaçlarını karşıladıkça güvenlik ihtiyacı, güvenlik ihtiyacını karşıladıkça sevgi ve diğerleri gibi ihtiyaçlar ortaya çıkmaktadır. Fizyolojik ihtiyaçlar, temel beslenme, su, barınma, giyim ve uyku gibi öncelikli gereksinimlerdir. Bunların dışında kalan, aidiyet gibi, ihtiyaçlar ise bir kimlik tanımlayıcısını gerektiren ihtiyaçlardır. Kimlik, bireyin kendini nasıl tanımladığı ve diğerlerinden nasıl ayrıldığıyla ilgilidir. Temelde, kimlik bir şeye ait olma ihtiyacının bir sonucu olarak gelişir (Yıldız, 2007, s. 9).

İnsanların göçebe yaşamdan yerleşik düzene geçmeleri, topluluklar halinde yaşamalarını sağlamış ve nüfus yoğunluğunu artırmıştır. Bu durum, bir arada yaşayan insanların birbirlerinden ayrılabildiği ortamların oluşmasına yol açmıştır. Ancak artan topluluklar ve benzerlikler, tanımlama sürecini karmaşık hale getirmiştir. Soyadı gibi eski bir gelenek, bireylerin aile kimliğini ve kökenini belirtmek için kullanılmıştır. Ancak artan nüfusla birlikte soyadının tekil tanımlama için yetersiz olduğu anlaşılmıştır. Bu durum, bireyleri tekil olarak tanımlamak ve toplumsal yaşamı kolaylaştıracak yeni yöntemlerin geliştirilme ihtiyacını ortaya çıkarmıştır. Bu yöntemlerin karmaşıklığı azaltması ve hızlı bir şekilde uygulanabilir olması önemlidir.

Kimlik kartları, kamu yönetimi için önemli bir araç olup, insanları ayırt etmeye yardımcı olmaktadır. Ancak, bazı kimlik kartlarının aynı bilgileri içermesi ve güvenlik eksiklikleri nedeniyle sahtecilik ve dolandırıcılık gibi sorunlar yaşanmaktadır. Bu nedenle, güvenlik önlemlerini artırmak amacıyla akıllı kimlik kartları geliştirilmiştir. Akıllı kimlik kartları, özel bir algoritma içeren 11 haneli numara ile oluşturulmuş çipli kartlardır ve birçok alanda kullanılabilirlik sağlamaktadır. Ancak, bu kartlar kullanımıyla birlikte bazı sakıncalar da ortaya çıkmaktadır. Özellikle algoritmaların kullanılması ve biyometrik izlerin takibi, mahremiyet ihlallerine ve kişisel özgürlüklerin sınırlanmasına neden olabilmektedir. Akıllı kartlardaki güvenlik açıkları genellikle hukuki süreçlere

taşınmaktadır; bu sorunun ana nedenlerinden biri de tüm vatandaşlara ait bilgilerin tek bir merkezi biyometrik veri tabanında toplanmasıdır (Teeluckdharry, 2022). Bu bağlamda bu çalışmanın ana amacı akıllı kimlik kartları hakkındaki farkındalığı artırmak ve mahremiyet ve güvenlik bakımından akıllı kimlik kartlarını detaylı incelemektir.

Çalışma beş bölümden oluşmaktadır. Birinci bölümde çalışmanın araştırma tasarımı ve metodolojisi ile ilgili bilgiler aktarılmış, araştırmanın önemi, amacı, modeli, örneklem grubu, araştırma soruları ve hipotezler üzerinde durulmuştur. Araştırmada veri toplama yöntemi olarak Karaman ilindeki 30 katılımcıyla yapılan yarı yapılandırılmış mülakatlar kullanılmıştır. İkinci bölümde akıllı kimlik kartlarıyla ilgili kavramsal çerçeve sunulmuştur. Üçüncü bölümde akıllı kimlik kartlarının mahremiyet ve güvenlik boyutları incelenmiştir. Mahremiyet kavramının tanımı, tarihsel gelişimi ve hukuki alt yapısı, akıllı kimlik kartları ile ilişkisi ve ayrıca akıllı kimlik kartlarının güvenlik sorunsalı detaylı bir şekilde ele alınmıştır. Dördüncü bölümde araştırma bulguları analiz edilmiş ve özetlenmiştir. Beşinci ve son bölümde ise akıllı kimlik kartlarının mahremiyet ve güvenliği ile ilgili çeşitli öneri ve eleştiriler sunulmuş ve araştırmanın sonuçları değerlendirilmiştir.

1. BÖLÜM: ARAŞTIRMA TASARIMI VE METODOLOJİ

1.1. Araştırmanın Amacı ve Önemi

Bu araştırmanın amacı, vatandaşların akıllı kimlik kartlarına yönelik mahremiyet algılarını ve bu kartların kullanımı sırasında kişisel verilerin korunması hakkındaki düşüncelerini detaylı bir şekilde incelemektir. Akıllı kimlik kartlarının günlük yaşamdaki yerinin ve öneminin giderek artması, bu çalışmanın önemini daha da artırmaktadır. Çalışma sonuçlarının, politika yapıcıların ve ilgili kurumların bu kartların daha güvenli ve mahremiyet odaklı kullanımını sağlamaya yönelik adımlar atmalarına yardımcı olabileceği düşünülmektedir.

1.2. Araştırmanın Yöntemi

Bu araştırma, nitel araştırma yöntemi kullanılmıştır. Nitel araştırma, bireylerin veya grupların sosyal ya da insani sorunlara yükledikleri anlamları ve bu sorunların derinlemesine incelenmesini hedefleyen yorumlayıcı ve kuramsal çerçeveler kullanarak başlar. Araştırmada, insanlara ve mekanlara duyarlı bir şekilde doğal ortamlarda veri toplama yöntemlerini tercih eder ve verileri analiz ederken tüme varım ve tümden gelim gibi yöntemlerle örüntüler ve temalar oluşturur (Cresswell, 2013, s. 44). Nitel çalışmalar, katılımcıların seslerini, araştırmacının derin düşüncelerini, problemin karmaşık açıklamalarını ve yorumlamalarını, literatüre katkı sağlamayı veya değişim çağrısı yapmayı içerebilir. Başka bir deyişle, nitel araştırmalar, gözlemler, görüşmeler ve doküman analizleri gibi nitel veri toplama yöntemlerini kullanarak algıları ve olayları kendi doğal ortamlarında gerçekçi ve bütüncül bir şekilde ortaya koymayı amaçlayan araştırma süreçleridir (Yıldırım, 1999, s. 10).

Nitel çalışma, bir problemi derinlemesine araştırmak ve bu süreçte gerekli olan zaman ve kaynakları sağlamak için güçlü bir bağlılık gerektirir. Bu nedenle, nitel yöntemler genellikle en kapsamlı nicel yöntemlerle birlikte kullanılır ve sadece bir alternatif olarak değerlendirilmemelidir. Nitel araştırmacılar, sahada uzun saatler geçirir, geniş bir veri yelpazesi toplar ve alanın sorunlarını inceleyerek erişim, yakınlık ve içeriden bir bakış açısı elde ederler. Topladıkları büyük veriyi analiz ederek temalar veya kategoriler oluşturur ve bu karmaşık süreç zaman alıcıdır. Bulguları desteklemek ve farklı bakış

açılarını yansıtmak amacıyla uzun metinler yazar ve katılımcıların görüşlerini ayrıntılı bir şekilde sunmak için bolca alıntıya başvururlar (Cresswell, 2013, s. 49).

Nitel çalışmalar, sosyal araştırmalarda sıklıkla kullanılan, tutum, davranış ve deneyimlerle ilgilenen, sözel verilerle yapılan ve yorumlamaya dayanan çalışmalardır. Bu tür çalışmalar, durum çalışması, örnek olay incelemesi, eylem araştırmaları, kültürel analiz, feminist araştırmalar ve gömülü teori gibi çeşitli alt kategorilere ayrılabilir (Padem vd., 2012, ss. 57-58).

1.3. Araştırmanın Evreni ve Örneklemi

Araştırmanın evrenini Karaman il merkezinde yaşayan 18 yaş üzeri vatandaşlar oluşturmaktadır.

Araştırmanın örneklemini ise, araştırmanın evreni içerisinden tabakalı basit rastgele örnekleme yöntemi baz alınarak seçilen ve 2024 yılında Karaman il merkezinde yaşayan 18 yaş üzeri 30 reşit bireyden (muhtemel veri kaybına karşı örneklem %10 arttırılmıştır) oluşmaktadır. Bu çerçevede araştırmaya katılacak kişilerin yaş, eğitim ve cinsiyet gibi kendi içinde benzerlikleri olan alt tabakaların ayrılması ve sonrasında bu tabakaların her birinden basit rastgele örnekleme uygun olarak katılımcılar seçilmiştir. Bu yöntemin seçilmesinde, çalışmaya katılan kişilerin, çeşitli demografik bilgilerine bağlı olarak, sorulara verdikleri yanıtlar arasında anlamlı bir fark yaratabileceği düşünülmüştür.

1.4. Araştırma Deseni

Nitel araştırmalarda, her ortam ve katılımcı için geçerli olan standart yöntemler bulunmadığından, her araştırma kendine özgü bir tasarım ve analiz türü ile gerçekleştirilir (Yıldırım & Şimşek, 2021, s. 43). Bu çalışma, Karaman ilinde basit rastgele örnekleme yöntemi baz alınarak seçilen kişilerle derinlemesine bilgi elde edinmek amacıyla fenomenoloji (olgu bilim) deseninden yararlanılmış bir nitel çalışmadır.

Fenomenoloji, bir grup insanın belirli bir fenomen hakkındaki deneyimlerini derinlemesine inceleyerek, bu deneyimlerin ortak anlamlarını ortaya koyar ve bu ortak anlamları daha geniş, evrensel bir açıklamaya dönüştürmeyi amaçlar (Cresswell, 2015, s. 77). Fenomenler, günlük yaşamda tecrübeler, olaylar, durumlar, algılar ve kavramlar şeklinde kendini gösterebilir ve insanlar bu fenomenlerle karşılaşmış olabilirler. Ancak

bu tanışıklık, fenomenleri tamamen anladıkları anlamına gelmez. Bu yüzden, fenomenoloji deseni, insanların farkında olduğu ancak derinlemesine bilgiye sahip olmadığı ya da tam olarak kavrayamadığı konulara odaklanır (Yıldırım & Şimşek, 2021, s. 72).

Bu çalışmayla, Karaman İlinde ikamet eden 18 yaş üzeri bireylerin akıllı kimlik kartlarına yönelik mahremiyet algılarını ve bu kartların kullanımı sırasında kişisel verilerin korunması hakkındaki düşüncelerini detaylı bir şekilde incelemek amaçlandığından araştırmanın fenomenoloji deseni ile yürütülmesinin uygun olacağı düşünülmüştür. Kısacası fenomenolojiyi "İnsanların farkında olduğu ancak derinlemesine kavrayamadığı ya da ayrıntılı bilgiye sahip olmadığı konulara yönelir." şeklinde özetlenen çalışmanın bu desen ile uyumlu olduğu değerlendirilmiştir.

1.5. Veri Toplama Araçları

Fenomenoloji araştırmalarında temel veri toplama yöntemi görüşmedir. Bu yöntem, fenomenlerle ilgili yaşantıları ve anlamları açığa çıkarmak için araştırmacının iletişim kurma, esneklik sağlama ve derinlemesine inceleme yapma imkanlarını sunar (Yıldırım & Şimşek, 2021, s. 74).

Çalışmada, nitel araştırma yöntemleri arasında yer alan "Yarı yapılandırılmış Mülakat Tekniği" kullanılmıştır. Bu teknik, araştırılan konunun tüm yönlerini kapsayan, açık uçlu sorularla yapılan ve detaylı yanıtlar alınmasını sağlayan birebir görüşmelerle bilgi toplanmasını mümkün kılar. Açık uçlu sorular, katılımcıların kendi deneyimlerini ve duygularını daha ayrıntılı bir şekilde paylaşmalarına olanak tanır, bu da daha derin ve anlamlı analizler yapılabilmesine yardımcı olur (Patton, 2018, s. 4).

Nitel araştırmalarda, araştırmacının rolü nicel araştırmalardan oldukça farklıdır. Nicel çalışmalarda araştırmacı, belirli yöntemlerle dışarıdan gözlem yapar, veri toplar ve bu verileri sayısal olarak analiz ederken, nitel araştırmalarda araştırmacı sahada aktif olarak yer alır, deneklerle doğrudan etkileşimde bulunur ve gerekirse onların deneyimlerini bizzat yaşar. Araştırmacı, topladığı bakış açıları ve deneyimleri veri analizinde kullanır. Bilgi kaynaklarına yakın olmak, ilgili kişilerle iletişim kurmak, gözlemler yapmak ve belgeleri incelemek nitel araştırmalarda son derece önemlidir. Bu yüzden araştırmacı,

çalışma sürecinin doğal bir parçası olur ve bazen bilgi toplama aracı olarak görev yapar (Yıldırım, 1999, s. 11).

Araştırmacının rolü, verileri sadece düzenlemek değil, aynı zamanda bu verilerden anlamlı ve yeni kavramsal yapılar oluşturmak ve bunları araştırmak olarak tanımlanır. Bu, nitel araştırmaların derinlemesine ve bağlamsal bilgi sağlayabilen bir metodoloji olduğunu gösterir (Neuman, 2007, ss. 662-663). Bu süreç, araştırmacının notları tekrar tekrar dikkatle gözden geçirmesini ve veriler hakkında derinlemesine bir anlayış geliştirmesini içerir. Analiz tamamlandıktan sonra elde edilen veriler tablolar ve tartışmalarla birlikte bir rapor halinde sunulur (Güler vd., 2015, s. 44). Bu çalışmada, verilerin yazılı hali araştırmacı tarafından tatmin edici bir sonuç elde edilene kadar defalarca okunmuştur. Bu şekilde, verilerin arka planındaki olayları keşfetme ve genel bir anlam çıkarma süreci tamamlanmıştır. Ayrıca, dökümler kategorilere veya soru sırasına göre gruplanmadan doğrudan kodlama işlemi uygulanmıştır.

Araştırma soruları, katılımcıların akıllı kimlik kartları, mahremiyet ve güvenlik konularını çeşitli yönleri ile değerlendirmelerini sağlamaktadır. Aşağıda mülakat görüşmelerinde kullanılan sorular ile hedeflenen konular açıklanmıştır:

- ✓ **Genel Görüşlerin Alınması:**

İlk soru, katılımcıların akıllı kimlik kartları hakkında genel düşüncelerini anlamayı amaçlamaktadır. Bu soru, katılımcıların akıllı kimlik kartlarına ilişkin genel algılarını ve duygularını ifade etmelerine olanak tanımaktadır.

- ✓ **Kullanım Sıklığı:**

İkinci soru, katılımcıların akıllı kimlik kartlarını ne sıklıkla kullandıklarını belirlemek için sorulmuştur. Bu bilgi, kartların günlük hayattaki kullanım oranını ve önemini anlamak için kullanılmıştır.

- ✓ **Bilinç Düzeyi:**

Üçüncü soru, katılımcıların kişisel verilerini koruma konusundaki bilinç düzeylerini ölçmeyi hedeflemektedir. Bu soru, kullanıcıların güvenlik ve mahremiyet konularında ne

kadar bilgi sahibi olduklarını ve bu konuda ne kadar dikkatli davrandıklarını ortaya koymaktadır.

- ✓ **Güvenlik Önlemlerinin Etkililiği:**

Dördüncü soru, mevcut güvenlik önlemlerinin katılımcılar tarafında ne kadar etkili bulunduğunu sorgulamaktadır. Katılımcıların güvenlik önlemlerine dair algıları, bu önlemlerin yeterliliğini ve geliştirilmesi gereken alanları belirlemek açısından önem arz etmektedir.

- ✓ **Kayıp veya Çalınma Durumu:**

Beşinci soru, akıllı kimlik kartlarının kaybolması veya çalınması durumunda ortaya çıkabilecek güvenlik sorunlarını değerlendirmektedir. Bu soru, katılımcıların bu tür olaylara karşı ne derece endişeli olduklarını ve bu konuda alınabilecek önlemleri ortaya koymaktadır.

- ✓ **Özel Önlemler:**

Altıncı soru, katılımcıların kişisel bilgilerini korumak için aldıkları özel önlemleri belirlemeye yöneliktir. Bu soru, kullanıcıların kendi güvenliklerini nasıl sağladıklarını ve hangi yöntemleri kullandıklarını anlamak sorulmuştur.

- ✓ **Resmi Bilgilendirme:**

Yedinci soru, katılımcıların güvenlik ve mahremiyet konularında herhangi bir resmi bilgilendirme alıp almadıklarını sorgulamaktadır. Resmi bilgilendirme eksikliği, kullanıcıların bu konularda yeterince bilinçli olup olmadığını ve eğitim ihtiyacını ortaya koymaktadır.

- ✓ **Önerilen Önlemler:**

Sekizinci soru, akıllı kimlik kartlarının mahremiyetle ilgili endişeleri azaltmak için alınabilecek önlemleri sormaktadır. Katılımcıların önerileri, bu kartların güvenliğini artırmak için kullanılabilecek yeni öneriler sunmaktadır.

- ✓ **Veri Güvenliği Algısı:**

Dokuzuncu soru, katılımcıların kişisel verilerinin güvende olup olmadığını tespit etmek için sorulmuştur. Bu soru, mevcut güvenlik önlemlerinin katılımcılar tarafından nasıl algılandığını anlamak için önem arz etmektedir.

- ✓ **İzinsiz Erişim:**

Onuncu soru, kişisel verilerin izinsiz erişime karşı korunması hakkındaki düşünceleri sorgulamaktadır. Bu soru, güvenlik politikalarının ne kadar etkili olduğuna dair katılımcıların görüşlerini ortaya koymaktadır.

- ✓ **Çevrimiçi Kullanım Güvenliği:**

On birinci soru, akıllı kimlik kartlarının çevrimiçi kullanımı esnasında verilerin korunması için neler yapılabileceğini sorgulamaktadır. Bu soru, dijital güvenlik önlemlerinin geliştirilmesine yönelik katılımcı önerilerini içermektedir.

- ✓ **İzleme ve Takip:**

On ikinci soru, akıllı kimlik kartlarının izleme veya takip edilme olasılığı hakkında katılımcıların ne düşündüğünü tespit etmek amaçlı sorulmuştur. Bu soru, kartların mahremiyet ihlallerine yol açma potansiyelini değerlendirmektedir.

- ✓ **Mahremiyet Bilgileri:**

On üçüncü soru, katılımcıların dini bilgi, medeni durum gibi mahremiyet bilgilerinin tehlikede olup olmadığını sorgulamaktadır. Bu soru, kişisel bilgilerin ne kadar korunduğuna dair algıyı ölçmek için sorulmuştur.

- ✓ **Özel Hayatın Mahremiyeti:**

On dördüncü soru, akıllı kimlik kartlarındaki bilgilerin özel hayattaki mahremiyeti ihlal edip etmeyeceği konusunda katılımcıların düşüncelerini belirlemek için sorulmuştur. Bu soru, kullanıcıların özel hayatlarına yönelik endişelerini ortaya koymaktadır.

- ✓ **Ek Görüşler ve Öneriler:**

On beşinci ve son soru, katılımcıların eklemek istedikleri görüş ve önerileri sormaktadır. Bu soru, katılımcıların araştırma kapsamında ele alınmayan ancak önemli gördükleri konuları paylaşmalarına olanak tanımaktadır.

Bu sorular ile katılımcıların akıllı kimlik kartlarıyla ilgili güvenlik ve mahremiyet konularını kapsamlı bir şekilde değerlendirmeleri hedeflenmiştir.

Tablo 1. Katılımcı ve Görüşme Bilgileri

Katılımcı Kodu	Cinsiyeti	Eğitim Durumu	Çalıştığı Kurum	Görüşme Tarihi	Görüşme Süresi (Dakika)
K1	Erkek	Lise	Özel Sektör	16.04.2024	28
K2	Kadın	Ön Lisans	Özel Sektörü	16.04.2024	35
K3	Kadın	İlköğretim	Özel Sektörü	17.04.2024	22
K4	Kadın	Lisans	Özel Sektörü	17.04.2024	45
K5	Erkek	Lise	Kamu Sektörü	17.04.2024	41
K6	Erkek	Lisans	Özel Sektör	19.04.2024	36
K7	Kadın	Lise	Özel Sektör	19.04.2024	25
K8	Kadın	İlköğretim	Çalışmıyor	20.04.2024	22
K9	Kadın	Lisans	Özel Sektör	20.04.2024	43
K10	Kadın	Yüksek Lisans	Özel Sektör	22.04.2024	42
K11	Kadın	Lisans	Özel Sektör	22.04.2024	35
K12	Kadın	Lisans	Özel Sektör	27.04.2024	32
K13	Kadın	İlköğretim	Özel Sektör	27.04.2024	21
K14	Erkek	Lisans	Kamu Sektörü	27.04.2024	45
K15	Erkek	Lise	Kamu Sektörü	27.04.2024	30
K16	Kadın	Lisans	Özel Sektör	28.04.2024	25
K17	Erkek	Lise	Özel Sektör	28.04.2024	28
K18	Kadın	Doktora	Kamu Sektörü	30.04.2024	40
K19	Erkek	Lisans	Özel Sektör	02.05.2024	32
K20	Erkek	Yüksek Lisans	Kamu Sektörü	02.05.2024	35
K21	Kadın	Lisans	Özel Sektör	03.05.2024	25
K22	Kadın	Lisans	Özel Sektör	03.05.2024	32
K23	Erkek	Lisans	Kamu Sektörü	03.05.2024	26
K24	Erkek	Lise	Kamu Sektörü	05.05.2024	28
K25	Kadın	Lisans	Çalışmıyor	07.05.2024	36
K26	Erkek	Lise	Özel Sektörü	07.05.2024	34
K27	Erkek	Lise	Özel Sektör	08.05.2024	35
K28	Erkek	Lise	Özel Sektör	08.05.2024	25
K29	Erkek	Lise	Özel Sektör	09.05.2024	33
K30	Erkek	Ön Lisans	Kamu Sektör	10.05.2024	35

1.6. Verilerin Analizi

Nitel araştırmaların esnek ve bağlamsal bir doğası vardır. Nitel araştırmalar, belirli bir standart prosedür veya tek tip yöntemler yerine, araştırmanın yapıldığı ortam ve

katılımcıların özelliklerine göre özelleştirilmiş yaklaşımlar gerektirir. Bu durum, her araştırmanın kendine özgü bir tasarım ve analiz yöntemleri içermesi anlamına gelir. Yani, nitel araştırmalarda kullanılan yöntemler, araştırmanın hedefleri, katılımcılar ve bağlamına göre farklılık gösterebilir. Bu esneklik, araştırmanın daha derinlemesine ve bağlamsal bir anlayış sağlamasına olanak tanır, ancak aynı zamanda her araştırmanın kendi özel koşullarına ve gereksinimlerine uygun olarak tasarlanmasını gerektirir (Yıldırım & Şimşek, 2021, s. 43).

Bu çalışmada araştırma verilerinin çözümlenebilmesi için tematik analiz yöntemi kullanılmıştır. Tematik Analiz, nitel bir analiz türüdür. Sınıflamaları analiz etmek ve verilerle ilişkili temaları sunmak için kullanılır. Verileri büyük bir ayrıntıyla betimler ve çeşitli konuları yorumlamalar aracılığıyla ele alır (Boyatzis, 1998).

Tematik Analiz, yorumlamalar kullanarak keşfetmeye yönelik herhangi bir çalışma için en uygun yöntem olarak kabul edilir. Verilerin analizine sistematik bir unsur katar. Araştırmacının bir temanın sıklığının analizini bütün içerikle ilişkilendirmesine olanak tanır. Bu, doğruluk ve karmaşıklık kazandırır ve araştırmanın genel anlamını artırır. Nitel araştırma, çeşitli yönlerin ve verilerin anlaşılmasını ve toplanmasını gerektirir. Tematik Analiz, herhangi bir sorunun potansiyelini daha geniş bir şekilde anlamak için fırsat sunar (Marks & Yardley, 2004).

Tematik analizin başlangıcında, verilerdeki benzerlikler ve farklılıklar belirlenerek ortak kodlar oluşturulur ve bu kodlar ardından ortak temalar altında birleştirilir (Yıldırım & Şimşek, 2021, s. 236). Çalışmamızda veri analizi, daha önceki araştırmalarda belirtilen aşamalardan uygun olan altı aşama kullanılarak yapılmıştır (Demirkıran, 2014, s. 86). Söz konuşu aşamalar;

- ✓ Verilerin bilgisayar ortamına aktarılması
- ✓ Her sorunun altına ilgili katılımcı görüşlerinin yığılması
- ✓ Verilerin okunarak kodlanması
- ✓ Kodların belirli temalar altında birleştirilmesi
- ✓ Kodların ve temaların kontrolü
- ✓ Bulguların sunumu ve yorumlanması

Bu çalışmamızda görüşmelerden elde edilen veriler bilgisayar ortamına aktarılmış ve ardından ses kayıt cihazları tekrar dinlenerek Word belgesinde 30 sayfalık bir döküm

haline getirilmiştir. Herhangi bir hataya yer vermemek adına ses kayıtları tekrar dinlenilmiş ve elde edilen dökümler üzerinden geçilerek gerekli düzeltmeler yapılarak son şekli verilmiştir. Bir sonraki aşamada, görüşmecilerden toplanan veriler ilgili sorular altında düzenlenmiş ve görüşmecilerin konuyla ilgili ifadeleri kapsamlı bir şekilde incelenmiştir. Ardından elde edilen dökümler okunarak kodlanmış ve belirli temalar altında birleştirilmiştir. Ardından, ses kayıtları, bu kayıtların Word ortamındaki dökümleri ve temalaştırma işlemi, biri nitel araştırmalar konusunda uzmanlaşmış ve doktorasını bu alanda tamamlamış iki öğretim üyesi tarafından incelenmiş; gerekli düzenlemeler yapılarak onay alınmış ve temalar bu şekilde kesinleştirilmiştir. Son aşama olan bulgular kısmı katılımcı görüşlerinden alıntılar yapılıp yorum katılarak sunulmuştur.

1.7. Araştırmanın Geçerlik ve Güvenirliği

Geçerlilik ve güvenirlik; araştırmanın her aşamasında yani kavramsal çerçeveden verilerin toplanması ve analizine kadar önemli olduğunu ve bu faktörlerin, sonuçların güvenilirliğini ve geçerliliğini doğrudan etkilediğini gösterir. Araştırmanın genel kalitesini ve bulguların doğruluğunu garanti altına almak için kritik bir öneme sahiptir (Merriam, 2013, s. 200). Bilimsel araştırmalarda, elde edilen sonuçların inandırıcı ve güvenilir olması kritik bir öneme sahiptir. Bu, araştırmanın genel kalitesini ve bilimsel değerini belirler. Geçerlilik, araştırmanın amacına uygun olup olmadığını, güvenirlik ise sonuçların tutarlı ve tekrar edilebilir olduğunu belirtir. Özellikle nicel araştırmalarda bu kavramlar, bilimsel bulguların doğruluğunu sağlamak için temel ölçütler olarak kabul edilir. Nicel araştırmalar genellikle ayrıntılı tanımlar, yöntemler ve istatistiksel testler içerir. Bu da elde edilen sonuçların nesnel ve karşılaştırılabilir olmasını sağlar. Nitel araştırmalarda ise geçerlilik ve güvenirlik kavramlarının uygulanması daha karmaşıktır. Nitel araştırmalarda sonuçların değerlendirilmesinde daha çok araştırmacının subjektif yargıları ve bağlamsal anlayışları dikkate alınarak standartlaştırılmış yöntemlerden ziyade, niteliksel derinlik ve bağlamın önemi daha fazla ortaya koyar (Yıldırım & Şimşek, 2021, s. 269).

Güvenirlik, araştırma bulgularının tekrarlandığında aynı sonuçları verip vermemesi ile ilgilidir, bu nedenle bir çalışma yeniden yapıldığında benzer sonuçların elde edilmesi beklenir. Ancak nitel araştırmalarda güvenilirlik sorunlu olabilir, çünkü insan davranışları oldukça değişkendir. Nicel araştırmalarda güvenirlik, tek bir gerçeğin var olduğunu ve

araştırmanın tekrarının aynı sonuçları vereceğini varsayar, ayrıca değişkenler arasındaki neden-sonuç ilişkilerini ve olguları açıklayan kanunların belirlenmesine odaklanır. Nitel araştırmalar ise insan davranışlarına dair genel kanunlar oluşturmaktan ziyade, dünyadaki deneyimleri olduğu gibi tanımlayıp açıklamaya çalışır. Bu yüzden, nitel araştırmalarda yapılan çeşitli yorumlar nedeniyle, geleneksel anlamda güvenilirliği sağlayacak kesin ölçütler bulunmamaktadır (Merriam, 2013, s. 211).

Nitel araştırmalarda doğru bir anlam ya da yorum, tek bir doğruyu yansıtmayacağını belirtir ve güvenirliğin, çıkarımların iyi bir şekilde tartışılması ve farklı yorumlara yer verilmesiyle sağlanabileceğini ifade eder (Seggie & Bayyurt, 2015, s. 260).

Bu araştırmada literatür taramasına ve elde edilen kaynaklara göre çalışmanın geçerlik ve güvenirliği aşağıda maddeler halinde ifade edilebilir:

- ✓ Araştırmada Karaman ilinde ikamet eden 3 kişi ile birebir görüşme gerçekleştirilmiş ve elde edilen veriler incelenerek yöneltilen sorulara verilen yanıtların geçerliliğe uygun olduğu gözlemlenmiştir (Cresswell, 2013, s. 251).
- ✓ Araştırma denetleme yoluyla yürütülmüştür. Görüşmeler esnasında ses kaydı alınmış, elde edilen bilgiler bilgisayar ortamına aktarılarak yazılı bir döküm halinde saklanmıştır (Yıldırım & Şimşek, 2021, s. 283).
- ✓ Araştırma uzman incelemesine tabi tutularak yapılmıştır. Elde edilen veriler, bulgular ve yorumlar biri nitel araştırmalar konusunda uzmanlaşmış ve doktorasını bu alanda tamamlamış iki öğretim üyesi tarafından incelenmiş ve onay alınmıştır (Yıldırım & Şimşek, 2021, s. 279).
- ✓ Araştırmamızın dış güvenirliğini artırmak için katılımcı bilgileri ve görüşme detayları, katılımcıların isimleri gizli tutulacak şekilde paylaşılmıştır (Yıldırım & Şimşek, 2021, s. 274).
- ✓ Araştırmada kullanılan veri toplama ve veri analiz yöntemleriyle ilgili ayrıntılı açıklamalara yer verilmiştir (Yıldırım & Şimşek, 2021, s. 274).
- ✓ Araştırmada verilerin güvenilirliğini sağlamaya yönelik görüşmeler yarı yapılandırılmış görüşme tekniğiyle gerçekleştirilmiştir (Yıldırım & Şimşek, 2021, s. 270).
- ✓ Araştırmada görüşmecilerin ifadelerine doğrudan alıntı yapılarak yorum katılmadan aktarımlarda yapılmıştır (Yıldırım & Şimşek, 2021, s. 262).

1.8. Araştırmanın Sınırlılıkları

Bu çalışmanın kısıtları, sınırlı zaman ve mali kaynakların bulunması nedeniyle araştırmanın kapsamının ve alanının sınırlı kalmasıdır. Ayrıca, araştırmanın sadece Karaman il merkezinde gerçekleştirilmesinin, bulguların genelleştirilmesini zorlaştırabileceği ve farklı bölgelerdeki insanların deneyimlerini yansıtmayabileceği düşünülmektedir. Bunun yanı sıra, araştırma katılımcılarının sadece 18 yaşından büyük akıllı kimlik kartı kullanıcılarıyla sınırlı olması, genç kullanıcıların bakış açılarını ve deneyimlerini kapsam dışı bırakabilecektir. Bu kısıtlar, araştırmanın sonuçlarının yorumlanması sırasında göz önünde bulundurulmalıdır ve bulguların genel geçerliliğini etkileyebileceği düşünülmektedir.

1.9. Araştırma Sorusu ve Hipotezler

Araştırma, vatandaşların akıllı kimlik kartlarına yönelik mahremiyet algılarını ve bu kartların kullanımı sırasında kişisel verilerin korunması ve güvenlik ile ilgili düşüncelerini keşfetmeyi amaçlamaktadır.

Araştırmanın varsayımları, katılımcıların akıllı kimlik kartlarının amacı ve işlevleri hakkında temel bilgiye sahip olduğu, gizlilik bilgilerinin anlaşılır bir şekilde sunulduğu ve mahremiyetle ilgili geri bildirimde bulunabilecekleri mekanizmaların bulunduğu şeklindedir.

Hipotezler, katılımcıların mahremiyet farkındalığı, güvenlik önlemleri ve kartların mahremiyet yönleri hakkındaki algıları üzerine kurulmuştur. Bu çerçevede araştırmanın varsayımları ve hipotezleri aşağıdaki gibidir;

Temel Varsayımlar:

- ✓ Akıllı kimlik kartı kullanıcılarının kimlik kartının amacı ve işlevleri hakkında temel bir bilgiye sahip olmadığı varsayılmaktadır.
- ✓ Akıllı kimlik kartı gizliliğine ilişkin olarak kullanıcılara sunulan bilgilerin açık ve anlaşılır bir şekilde sunulmadığı varsayılmaktadır.
- ✓ Kullanıcıların akıllı kimlik kartlarının mahremiyet yönleri ile ilgili geri bildirimde bulunmaları veya soru sormaları için yetkili mekanizmaların bulunmadığı varsayılmaktadır.

Hipotezler:

- **H1:** Akıllı kimlik kartı kullanan vatandaşlar genel olarak, kişisel verilerinin kartlarda olması ve saklanmasına ilişkin mahremiyet meselelerinde yüksek düzeyde farkındalığa sahiptir.
- **H2:** Akıllı kimlik kartlarının mahremiyet yönlerine dair farkındalığı olan vatandaşların, kartlardaki kişisel verilerin güvenliğine dair endişeleri daha yüksektir.
- **H3:** Akıllı kimlik kartlarının faydaları ve sunduğu kolaylıkların kendileri açısından daha önemli olduğunu düşünen vatandaşlar, mahremiyet endişeleri olsa dahi, kartları kullanma ve benimseme düzeyleri daha fazladır.
- **H4:** Akıllı kimlik kartlarıyla ilgili yasal düzenlemelere yüksek düzeyde güven duymayan vatandaşların, kartların mahremiyet yönlerine dair algılarının olumlu olma olasılığı daha düşüktür.

Bu araştırmada, akıllı kimlik kartlarına yönelik çeşitli hipotezler aracılığıyla vatandaşların mahremiyet ve güvenlik algıları incelenmiştir. Genel olarak araştırma ile ilgili geliştirilen hipotezler, katılımcıların akıllı kimlik kartları ile ilgili farkındalık düzeylerini, güvenlik endişelerini, kullanım ve benimseme düzeylerini ve yasal düzenlemelere güvenlerini anlamayı amaçlamaktadır.

2. BÖLÜM: AKILLI KİMLİK KARTLARI KAVRAMSAL ÇERÇEVE

2.1. Akıllı Kart Teknolojilerine Giriş

Roland Moréno, 1974 yılında Fransa'da, Jürgen Dethloff ve Kunitaka Arimura ise 1969 ve 1970 yıllarında Almanya ve Japonya'da gerçekleştirdikleri çalışmalarla, akıllı kart teknolojisinin öncüleri kabul edilmektedir (Ceyhan vd., 2018, s. 746; Özbey, 2006, s. 1). Bu kartlar, çeşitli fonksiyonları tek bir çipte birleştirerek birden fazla fiziksel kartın ihtiyacını ortadan kaldırmakta (Ceyhan vd., 2018) ve kullanıcılara çeşitli avantajlar sunmaktadır (Özbey, 2006).

Akıllı kartlar, kredi kartı büyüklüğünde, içinde işlemci, RAM (Random Access Memory-Rastgele Erişim Belleği) ve ROM (Read-only Memory-Sadece Okunabilir Bellek) belleği gibi komponentleri barındıran entegre devrelerle donatılmıştır. Manyetik şeritler, barkodlar ve temassız radyo frekans vericileri gibi farklı teknolojilerle zenginleştirilmiş bu kartlar, güvenlik ve mahremiyetin ön planda olduğu giriş kontrolü, elektronik ticaret ve kimlik doğrulama gibi pek çok alanda kullanılmaktadır (Abd Elwahab vd., 2009, s. 514; Özbey, 2006).

2.2. Akıllı Kartların Kullanım Alanları

Akıllı kartlar günümüzde giderek yaygınlaşmakta ve teknoloji sayesinde bilgisayarlar, el bilgisayarları, cep telefonları gibi her türlü cihaza kart okuyucuları entegre edilmektedir. Hizmet sağlayıcıları, yüksek güvenlikli anahtar unsurlar olarak kullanarak, akıllı kartları yeni hizmetler geliştirilebilecek bir alan (e-ticaret, vatandaş yönetimi ve diğer hizmetler gibi) olarak görmektedir (Abrial vd., 2001, s. 1101). Bu uygulama alanları arasında ödeme sistemleri (banka kartları ve kredi kartları gibi), kimlik doğrulama (pasaport ve akıllı kimlik kartları gibi), erişim kontrolü (kapı girişleri ve ofisler gibi), toplu taşıma (otobüs, metro ve tren gibi), akıllı bina sistemleri (örneğin akıllı evlerdeki erişim kontrolü gibi) ve lojistik gibi alanlar öne çıkmaktadır (Djalal, 2019, s. 8). Akıllı kart uygulaması, nüfus, sağlık, pasaport, ehliyet, trafik, güvenlik, maliye gibi çeşitli alanlardaki bilgiler tek bir kart üzerinde toplanmasını sağlayarak, kamunun hızlı, verimli ve maliyet açısından etkin bir şekilde korunmasını sağlamaktadır (Öktem ve Aydın, 2005, s. 273).

Örneklerle akıllı kartların kullanım alanlarına ilişkin daha detaylı bilgi vermek gerekirse, Güney Kore'nin Seul Şehri'nde 2004 yılında uygulanan otomatik ücret toplama sistemleri, manuel ücret toplama yöntemlerine göre daha etkili ve maliyet tasarrufu sağlayan bir alternatif olarak kabul edilmiştir. Bu sistem, mesafeye dayalı, entegre bir ücret toplama ve hesaplama sistemi olarak tasarlanmıştır. Akıllı kart tabanlı bu toplu taşıma ücreti programı, her yolculuğun biniş ve iniş zamanları ile konumları gibi detaylı bilgiler sağlayarak, toplu taşıma kullanımı hakkında ayrıntılı veri toplamaktadır (Jang, 2010, s. 142).

Telekomünikasyon sektörü, akıllı kartların kullanıldığı alanlardan biridir. Cep telefonu aboneleri, akıllı kart teknolojisini SIM (Subscriber Identity Module-Abone Kimlik Modülü) kart olarak kullanmaktadır. Özellikle telekomünikasyon sektöründe 1980'lerin sonunda ve 1990'ların başında ortaya çıkan SIM kartlar, zamanla ödeme sistemleri, erişim kontrolü ve sağlık sektörü gibi daha geniş bir kullanım alanına yayılmıştır (Djalal, 2019, s. 9).

Akıllı kartlar, lojistik sektöründe de kullanım potansiyeline sahiptir. Örneğin, Chen ve ekibi (2007), tanker taşımacılığını yönetmek için bir akıllı kart uygulaması geliştirmişlerdir. Bir başka örnek çalışma, Taherdoost (2017)'nin çalışmasına göre, üniversite ortamında, erişim kontrolünde kullanılabilecek, kişisel güvenlik özelliklerine sahip, birden fazla işlevi yerine getirebilen çoklu uygulamalı ve güncellenebilir akıllı kartlar bulunmaktadır.

Aynı zamanda çoklu uygulamalı akıllı kartlar kimlik başvuruları, seçim başvuruları, pasaport başvuruları, sürücü belgesi başvuruları ve sağlık hizmeti başvuruları gibi uygulamalardan oluşabilmektedir (Abd Elwahab vd., 2009, s. 514). Ayrıca, günümüz teknolojisinde uygulama alanı olarak yer bulan ve temas gerektirmeyen akıllı kartlar da önemli bir rol oynamaktadır. Temasın olmaması, bakım maliyetlerini azaltmanın yanı sıra kullanım kolaylığı sağlayacak ve güvenilirliği artırarak son kullanıcı memnuniyetini artıracaktır (Abrial vd., 2001, s. 1101).

2.3. Akıllı Kimlik Kartlarının Tanımı ve Özellikleri

Kimlik kartları, vatandaşlık durumunu belgeleyen ve kamu yönetimi tarafından kişileri birbirinden ayırt etmekte kullanılan önemli araçlardır. Türkiye'de kimlik kartlarına ilk

kez 1927 yılında başvurulmuş, ancak çok nadir de olsa aynı bilgilerin farklı bireylerin kartlarında yer alması gibi durumlar yaşanmıştır. Bu sorunu çözmek amacıyla, 2000 yılında her vatandaşa özgü 11 haneli Türkiye Cumhuriyeti (T.C.) Kimlik Numarası sistemi devreye alınmıştır. Ancak bu sistem bile sahtecilik, dolandırıcılık ve terörle mücadelede yetersiz kalmış, kimlik kartlarının güvenliğini artırmak için yenilikler yapılması gerekliliği ortaya çıkmıştır.

Bu ihtiyaç doğrultusunda, 2007 yılında Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) tarafından geliştirilen akıllı kimlik kartları projesi hayata geçirilmiş, ilk testler Bolu ilinde yapılmıştır (Karaarslan vd., 2010, s. 5). Türkiye'de 2016 yılında başlayan akıllı kimlik kartı başvuruları, ilk etapta pilot bölge olarak seçilen Kırıkkale'de dağıtımla hayata geçirilmiştir (Ceyhan vd., 2018, s. 746). Kırıkkale ve bağlı ilçelerinde yaklaşık 40.000 vatandaşa kimlik kartı dağıtılmıştır. Projenin genişletilmesi amacıyla, ikinci aşamada Rize, Artvin, Trabzon, Erzincan ve Erzurum illeriyle başlayıp, daha sonra Adıyaman, Aksaray, Burdur, Uşak ve Yalova'da dağıtım gerçekleştirilmiştir. 2017 yılı itibarıyla bu uygulama tüm Türkiye çapında yaygınlaştırılmıştır (NVGM, 2024c). Bu projenin amacı, üç yıl içerisinde akıllı kimlik kartlarının tüm ülkeye yayılmasını sağlamaktır. Kartlar hem seyahat belgesi hem de elektronik imza amacıyla kullanılabilir niteliktedir (Ceyhan vd., 2018).

Akıllı kimlik kartları, devletin yetkili organları tarafından verilen, vatandaşın kimliğini kamu ve özel sektörde tanımlayan araçlardır (TÜBİTAK-UEKAE, 2006). TÜBİTAK tarafından geliştirilen çipli kimlik kartları, Akıllı Kart İşletim Sistemi (AKİS) sayesinde taklit ve sahteciliğe karşı yüksek güvenlik sunmaktadır. Kartlarda parmak, damar ve avuç içi izleri gibi biyometrik veriler kullanılmaktadır ve 1 Gigabyte (GB) depolama kapasitesine sahiptir (Ceyhan vd., 2018).

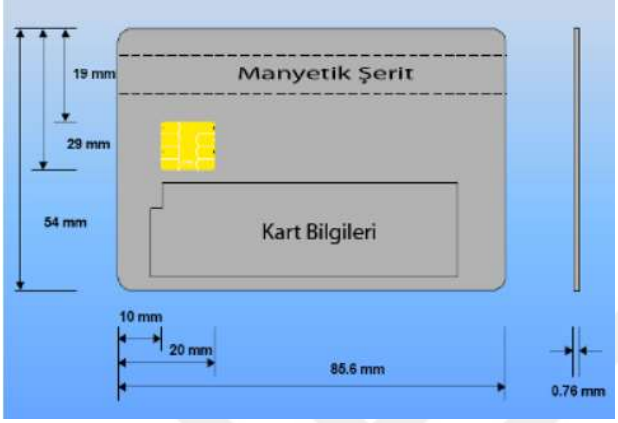
2.4. Akıllı Kimlik Kartı Tipleri

ISO 7810 standardında üç farklı kart tipi tanımlanmıştır. Bunlar; ID-1, ID-2 ve ID-3 kimlik kartlarıdır. Bu standart, kartların boyutları, imal malzemesi, kişisel bilgi alanları ve dayanabileceği ısı aralıkları gibi sabit bilgileri belirlemektedir. ID-1 kartlar genellikle bankacılık, ehliyet ve kimlik kartı gibi alanlarda kullanılırken, ID-2 kartlar birçok ülkede kimlik kartı olarak kullanılmakta ve ID-1'den biraz daha büyük boyutlara sahiptir. ID-3

kartlar ise pasaport ve uluslararası geçişlerde kullanılan vize kartlarıdır ve en büyük boyuta sahip kimlik kartlarıdır (Şanslı, 2007, ss. 3-5).

Şekil 1'de ID-1 kart görünümü verilmiştir.

Şekil 1. ID-1 Kart Görünümü



Kaynak: Şanslı, 2007, s. 4

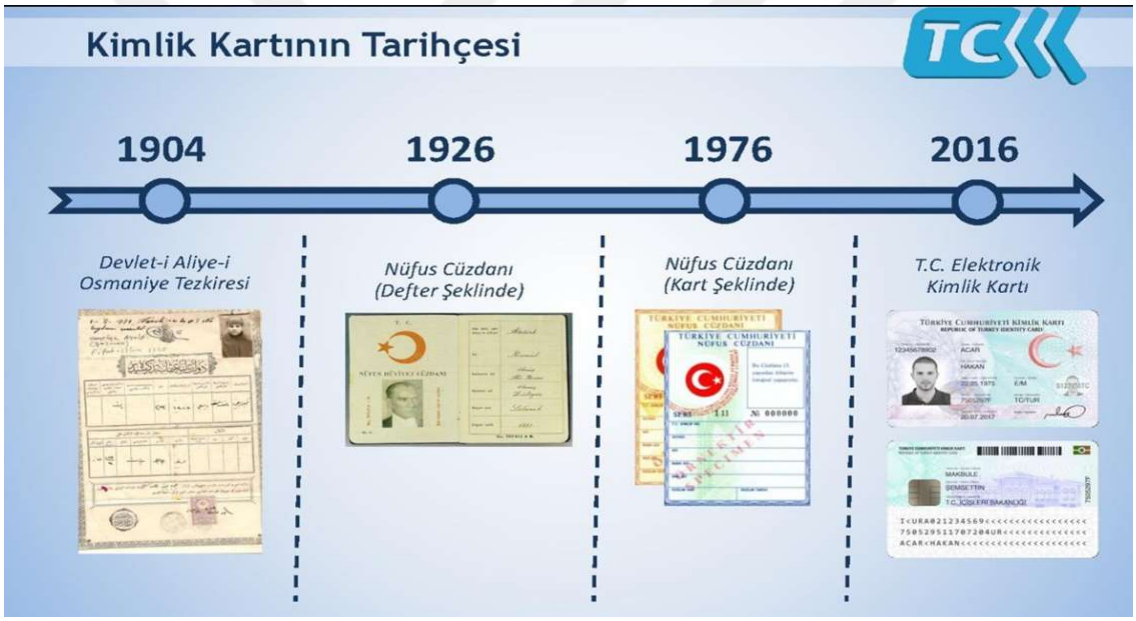
2.5. Akıllı Kimlik Kartlarının Tarihçesi ve Evrimi

Akıllı kartların tarihsel gelişimi, kronolojik bir sıralama ile ifade edildiğinde, aşağıdaki gibi özetlenebilir (Djalal, 2019, ss. 7-8):

- ✓ 1968: Alman mucitler tarafından ilk ICC (Entegre Devreli Kart) patenti alınması.
- ✓ 1970: Japonya, ardından 1974'te Fransa'da akıllı kart geliştirilmesi.
- ✓ 1979: Bankacılık sektörü için akıllı kartların ilk kez kullanılması.
- ✓ 1984: Fransa, çip entegreli ilk bankacılık kartını piyasaya sürmesi.
- ✓ 1995: İlk SIM kartların piyasaya sürülmesi.
- ✓ 1997: Almanya'da, sigorta bilgilerini içeren 70 milyon akıllı kartın dağıtılması.
- ✓ 1999: Finlandiya tarafından ilk ulusal eID kartının tanıtılması.
- ✓ 1999: Taşımacılık alanında ilk akıllı kartların kullanılması.
- ✓ 2001: Amerika Birleşik Devletleri Savunma Bakanlığı'nın, fiziksel erişim kontrolü ve güvenli kimlik doğrulaması için Askeri CAC kimlik bilgilerini ilk kez dağıtması.
- ✓ 2005: Norveç'in ICAO (International Civil Aviation Organisation-Uluslararası Sivil Havacılık Örgütü) standartlarına uygun ilk elektronik pasaportu uygulaması.

Akıllı kimlik kartları, akıllı kartların bir alt grubunu oluşturur. Teknolojinin gelişimiyle paralel olarak bu kartlar da sürekli olarak gelişmektedir ve gün geçtikçe akıllı kimlik kartlarının geliştirilmesi üzerine yeni bilimsel araştırmalar yapılmaktadır. Örneğin Djalal (2019) yaptığı çalışmada tüm vatandaşların kimlik kart işlemlerinin akıllı kart sistemi üzerinden yapılabileceği bir öneri getirmiştir. Bu sistemde vatandaşlar akıllı kimlik kartlarını kullanarak resmi işlemlerini gerçekleştirecekler ve akıllı kimlik kartlarını, kimlik kartları, sürücü belgeleri, ulaşım kartları ve sağlık hizmetleri gibi farklı alanlarda kullanabileceklerdir. Ayrıca, gümrük ve vergi ödemeleri gibi işlemleri de akıllı kimlik kartları üzerinden yapılabilecektir. Aynı zamanda kamu çalışanı ise personel kontrolü ve maaş ödemelerini kendi akıllı kimlik kartı ile yapabileceklerdir (Djalal, 2019, s. 18).

Şekil 2. Türkiye'de Akıllı Kimlik Kartlarının Kronologik Olarak Gelişimi



Kaynak: Nüfus ve Vatandaşlık Genel Müdürlüğü (2024)

Şekil 2, Türkiye'deki akıllı kimlik kartlarının gelişimini kronolojik olarak sunmaktadır. Osmanlı Devleti döneminde "Devleti Aliyye-i Osmaniyye Tezkiresi" adıyla ilk kez kullanılmaya başlanan kimlik belgesi, zaman içerisinde önce defter şeklinde, ardından kart şeklinde ve günümüzde ise elektronik kimlik kartı olarak son formunu almıştır.

2.5.1. Global Perspektifte Akıllı Kimlik Uygulamaları

Günümüzde birçok ülkede teknoloji ve dijitalleşme süreci ilerledikçe, akıllı kimlik uygulamaları da giderek önem kazanmaktadır. Farklı ülkelerin benimsediği yöntemler ve

uygulamalarda büyük çeşitlilik görülmektedir. Bu çerçevede Estonya, Singapur, Hindistan, İsveç ve Norveç gibi ülkelerde kimlik uygulamaları öne çıkmaktadır.

- **Estonya:**

Estonya bağımsızlığını kazandıktan sonra teknoloji odaklı bir devlet inşa etmiş ve e-devlet uygulamalarıyla öne çıkmıştır. Dünyadaki seçim süreçlerini internete taşıyan ilk ülke olan Estonya, 2014 yılında e-vatandaşlık uygulamasını başlatmıştır. Bu uygulama, Estonya'nın ulusal bir marka haline gelmesini sağlamış ve diğer ülkelerle paylaşılmak üzere geliştirilmeye devam etmektedir. Estonya, e-vatandaşlara kendi e-devlet sistemi ve Avrupa Birliği ağını kullanma fırsatı da sunmaktadır. E-vatandaşlık sisteminin daha iyi bir şekilde desteklenmesi için, politika, yasal ve kurumsal çerçevesini oluşturan e-Estonya projesi hayata geçirilmiştir. E-vatandaşlığın ve e-Estonya'nın temel yapı taşı, "isikukood" adı verilen Estonya Kişisel Kimlik Kodundan oluşmaktadır (Koç, 2021, s. 2259).

- **Singapur:**

Singapur'da Kimlik Kartı (IC), daimi kayıt sahipleri için zorunlu bir belgedir ve 15 yaşına gelindiğinde (16 yaş günü öncesinde) kayıt yaptırmaları gerekmektedir. Kayıt süreci, çevrimiçi başvuru ve biyometrik kayıt içermektedir. Devlet okullarına devam eden bireyler için biyometrik kayıtlar, kaydedilen bir günde okullarda yapılırken, devlet okuluna gitmeyen veya okula kayıt gününü kaçıran bireyler için biyometrik kayıt için ICA Binasında randevu alınması gerekmektedir. Kimlik kartı bilgileri için düzenli belgeler sağlanması gerekmektedir. Bunlar arasında vaftiz veya dini sertifika, kişilerin rızasıyla isim değişiklikleri için tapu anketi ve son üç ay içinde çekilmiş yeni vesikalık, dijital, renkli fotoğraflar yer almaktadır (ICA, 2024).

- **Hindistan:**

Aadhaar, 2009 yılında uygulamaya konulan, Hindistan'da en güvenilir kimlik belgesi olarak kabul edilmektedir. Bu belge, dünya genelinde her altı kişiden birinin sahip olduğu, 12 haneli benzersiz kimlik numarası sunarak, Hindistan'daki sakinlere önemli fırsatlar sunmaktadır. Bu kimlik numarası, insanlara artan bir güven ve güvenlik duygusu vererek yaşam ve iş yapmayı kolaylaştırmaktadır. Bir banka hesabı ile

ilişkilendirildiğinde bireyin finansal adresi haline gelen Aadhaar, kullanıcılarının gelecekte yatırım yapmasını kolaylaştırmaktadır. Aadhaar sayesinde, aracılar olmadan sınırsız kaynaklarla hizmetlerin, halkın ve sübvansiyonların hedef kitleye yönlendirilmesi sağlanmaktadır. Ayrıca hükümete Hindistan'ın nüfusu hakkında net bir görüş de sunmaktadır (UIDAI, 2024).

- **İsveç:**

İsveç Ulusal Kimlik Kartı, İsveç bölgesine verilen zorunlu olmayan bir biyometrik kimlik belgesidir. İsveç Polisi tarafından verilen bu kart, ülkenin iki resmi kimlik belgesinden biri olup, diğer İsveç pasaportudur. Yalnızca İsveç vatandaşlarına verilmekte ve vatandaşlığı belirtmektedir. Plastik ve kayıtlı şekilli olan kimlik kartı, yaklaşık 86x54 milimetre uzunluğundadır ve sol tarafta altın kaplamalı bir kontak çipi, sağ tarafta ise taşıyıcının fotoğrafı bulunmaktadır. Kartın üst kısmında İsveç adı üç dilde (İsveççe, İngilizce ve Fransızca) yazılıdır ve altında kartın adı yine aynı üç dilde yer alır. Kart, bir biyometrik pasaport sembolü ve sahibinin İsveç uyruğu ve ülke koduyla birlikte sağda yer alan bilgileriyle tamamlanır. Ayrıca kart, sonraki bir anda elektronik kimlik kartı olarak işlev gösteren hazır bir kontak çipi ve arka tarafın sağ alt kısmında temassız bir RFID çipi ile donatılmıştır. Kart, sahibinin fotoğrafıyla birlikte verilmektedir (wikipedia, 2024a). Ayrıca, BankID İsveç, İsveç'teki bankaların kullandığı bir dijital kimlik hizmetidir. Bu hizmet, kullanıcıların kimliklerini sürdürmek ve dijital imzayı göstermek için kullanılır. Uzaktan dijital imza uygulamaları AB eIDAS Yönetmeliği'ne uyumlu geliştirilmiş elektronik imza sağlar. BankID İsveç, Intesi Group tarafından sunulmakta ve kullanıcıların BankID kimlik bilgileriyle doğrulanan kimliklerine göre dijital sertifika sağlamaktadır (BankID, 2023).

- **Norveç:**

Norveç'te 30 Kasım 2020'den beri verilen Norveç Kimlik Kartı, zorunlu olmayan bir biyometrik kimlik belgesidir ve genellikle ulusal kimlik kartı olarak adlandırılmaktadır. Bu kart iki türdedir. Seyahat haklarına sahip olanlar, Avrupa Ekonomik Alanı ve İsviçre'de hem kimlik hem de seyahat belgesi olarak da kullanılabiliyorken, seyahat hakkı olmayanlar sadece kimlik tespiti için geçerlidir. Norveç Polis Teşkilatı tarafından verilen bu kartlar, Norveç bölgesine özeldir ve Avrupa Serbest Ticaret Birliği ve Avrupa

Ekonomik Alanı içinde seyahat özgürlüğünü kolaylaştıran bir belgedir. İskandinav ülkeleri arasındaki seyahatlerde ise İskandinav Pasaport Birliği sayesinde herhangi bir kimlik belgesine gerek yoktur. Kartın çipi, ICAO 9303 uyumluluğu ve tüm zorunlu veri gruplarını içermektedir. Kart sahibinin fotoğrafı renkli, 446x580 piksel ve JPEG 2000 formatındadır (wikipedia, 2024b).

2.5.2. Türkiye Özelinde Uygulama: Türkiye Cumhuriyeti Kimlik Kartı

T.C. Kimlik Numarası, 11 basamaktan oluşan bir tanımlayıcı numaradır. Bu numaranın son iki basamağı, bir doğrulama sayısını temsil etmektedir. Doğrulama sayısı, ilk dokuz basamak kullanılarak belirli bir algoritma ile hesaplanmaktadır. Bu algoritma, T.C. Kimlik Numarası geçerliliğini kontrol etmek için kullanılmakta ve sadece belirli bir numaranın, verilen bir T.C. Kimlik Numarası olup olmadığına dair bilgi sağlamaktadır. Bu algoritma, diğer kamu kurumlarıyla da paylaşılmakta ve T.C. Kimlik Numarası doğruluğunu kontrol etmelerine olanak tanımaktadır (NVGM, 2024c).

2000 yılında vatandaşlara verilmek üzere bir T.C. Kimlik Numarası havuzu oluşturulmuş ve bu havuzda kaydedilen T.C. Kimlik Numarası ilçe, cilt, aile sıra numarası ve birey sıra numarasına göre sıralanmıştır. Bu şekilde, bir kişinin T.C. Kimlik Numarasından akrabası olan başka bir kişinin kimlik bilgilerini elde etmek mümkün değildir. T.C. Kimlik Numarası, bir kişiye yalnızca bir kez verilmekte ve daha sonra değiştirilememektedir. T.C. Kimlik Numarası, ilçe nüfus müdürlükleri ve http://tckimlik.nvi.gov.tr adresinden öğrenilebilmektedir (NVGM, 2024c).

Kimlik kartlarının özellikleri aşağıdaki gibi sıralanabilir (NVGM, 2024c):

- ✓ Yeni sistemde kimlik kartları tek renktir.
- ✓ Geçerlilik süresi 10 yıldır.
- ✓ Polikarbon materyalden oluşmaktadır.
- ✓ TÜBİTAK tarafından geliştirilen milli işletim sistemi kullanılmıştır.
- ✓ Kimlik kartının üzerinde temaslı ve temassız çip yer almaktadır.
- ✓ Kimlik kartı vize muafiyeti olan ülkelere yapılacak seyahatlerde pasaport yerine seyahat belgesi olarak kullanılabilmektedir.
- ✓ Kart üzerindeki temaslı yongada elektronik imza özelliği bulunmaktadır.
- ✓ Yonga içerisinde saklanan verilerin kopyası alınamaz ve değiştirilemez.

- ✓ Fotoğraf ve kişisel bilgiler özel yöntemlerle karta basılmaktadır.
- ✓ Karttaki bilgiler sadece yetki tanımlanan uygulamalar tarafından kullanılabilmektedir.
- ✓ Kart bilgilerinin ve biyometrik verilerin güvenliğinin sağlanması için en yüksek düzeyde güvenlik tedbirleri alınmıştır.
- ✓ Biyometrik veri olarak parmak izi, parmak damar izi ve el ayası damar izi alınmıştır.

Şekil 3. Türkiye Cumhuriyeti Kimlik Kartı Görseli Ön ve Arka Yüz

Şekil 3, 14 Mart 2016'dan itibaren dağıtılmaya başlanan Türkiye Cumhuriyeti Kimlik Kartının ön ve arka yüzlerine ait örnekleri göstermektedir.

Türkiye'de T.C. Kimlik Kartı başvurusu, randevulu veya randevusuz olarak nüfus müdürlükleri veya dış temsilciliklere yapılmaktadır. Randevu almak için Alo199, https://randevu.nvi.gov.tr/ veya e-devlet sistemi kullanılabilmektedir.

Kimlik kartı, doğum, değiştirme, kayıp, yeniden kayıt ve vatandaşlığın kazanılması nedenleriyle düzenlenmektedir. On beş yaşını tamamlayanlar T.C. Kimlik Kartı için şahsen başvurmalıdır. On beş yaşını tamamlamayanlar için veli, vasi, kayyum veya resmi vekil başvuru yapabilmektedir.

Koruma altındaki on beş yaşını tamamlamayan çocukların başvuruları ilgili kuruluş yetkililerince yapılabilmektedir. Akıl hastalığı veya zayıflığı nedeniyle kısıtlananların başvuruları veli, vasi veya kayyum tarafından yapılmaktadır. Türk vatandaşlığı kazanımında biyometrik fotoğraf, pasaport benzeri belge ve vatandaşlığı gösteren resmi belge istenmektedir (NVGM, 2024c).

2.6. Akıllı Kimlik Kartı İçeriği ve Sistemin Yapısı

Akıllı kimlik kartlarında bulunan bilgiler, kartın güvenli bölgesinde saklanarak kontrolsüz erişime karşı korunmaktadır. Kart okuyucudan veri veya kart sahibinin parmak izi alınmadan kişiyle ilgili herhangi bir bilgiye ulaşılamaz. Bu kartlar, kişinin Merkezi Nüfus İdaresi Sistemi (MERNİS) kimlik bilgileri, ikametgah bilgileri, fotoğrafı, ıslak imzası, parmak izi bilgileri, biyometrik verileri, T.C. Kimlik Numarası, sosyal güvenlik, vergi, ehliyet, pasaport numaraları gibi kişisel referans numaralarını içerebilmektedir. Ayrıca, acil klinik bilgiler de kart içinde tutulabilmekte ve kart güvenlik bilgileri olarak kart şifresi, PIN numarası, değiştirme nedeni ve tarihi gibi bilgiler yer almaktadır (TÜBİTAK-UEKAE, 2006).

2.6.1. MERNİS

Merkezi Nüfus İdaresi Sistemi (MERNİS), kağıt ortamındaki nüfus kayıtlarını elektronik ortama aktararak merkezi bir veri tabanında tutmayı sağlamaktadır. Bir başka ifade ile vatandaşın özlük bilgilerinin yer aldığı veri tabanı uygulamasıdır. Bu proje ile nüfus kayıtları merkezi bir veri tabanında tutulmaya başlanmış, her vatandaşa T.C. kimlik numarası verilmiştir. Kimlik numarasıyla kişinin yaşamı boyunca yapılan işlemler takip edilmektedir. 81 il ile 973 ilçe nüfus müdürlüğü arasında çevrimiçi bağlantı kurulmaktadır. Bu sistem nüfus istatistiklerinin sağlıklı bir şekilde elde edilmesini sağlamakta ve kişilerin bulundukları yerin nüfus müdürlüğünden anında hizmet almaları sağlanmış olmaktadır (NVGM, 2024b).

2.6.2. Kart Yönetim Sistemleri

Farklı ihtiyaçlara daha uygun çözümler sunan kart yönetim sistemlerinin, kimlik kartı, sürücü belgesi, pasaport vb. uygulamalar ile entegrasyonu söz konusu olup belgelerin süreç döngüsünü yöneten uygulamadır. Örneğin, bir sürücü belgesi için gereken bilgiler ve süreçler ile bir pasaport için gerekenler farklı olabilmektedir. kart yönetim sistemleri, bu farklılıkları dikkate alarak belge türlerine özgü iş akışlarını ve güvenlik kontrollerini yönetmektedir (TÜBİTAK-UEKAE, 2006). Başka bir ifade ile kart yönetim sistemleri, çeşitli belgelerin yönetiminde büyük bir rol oynamakta ve bu belgelerin süreçlerini optimize ederken güvenlik ve verimliliği artırmaktadır. Bu sistemler, kullanıcıların farklı ihtiyaçlarına uygun çözümler sunarak, belgelerin doğru ve güvenli bir şekilde yönetilmesini sağlamaktadır.

2.6.3. Elektronik Kimlik Doğrulama Sistemi

Yeni nesil kimlik kartı özellikleri kullanılarak geliştirilen Elektronik Kimlik Doğrulama Sistemi (EKDS), kimliklerin doğrulanmasını sağlamaktadır. Bir başka ifade ile EKDS, kimlik kartının yetkili kurum tarafından verildiği, kişinin kartın sahibi olduğu, doğrulama sırasında kişinin bulunduğu yer ve doğrulama işleminin detaylarını kaydederek kişinin doğruluğunu sağlamaktadır. Bu sistem sayesinde kimlik sahteciliğinin önüne geçilmekte ve doğrulama yetersizliklerinden kaynaklanan usulsüzlük ve mali kayıplar önlenmektedir. Kurumların sunduğu elektronik hizmetlerin kalitesi artmakta, iş süreçleri hızlanmakta ve bürokrasi azalmaktadır. EKDS kullanılan kurumlarda kimlik doğrulaması kolay ve güvenli bir şekilde yapılmaktadır. Hem hizmet alan kişi hem de hizmet veren kurum kimlik doğrulamasından emin olmaktadır (NVGM, 2024a).

Kartı kullanan kişi ile kart sahibinin aynı kişiler olup olmadığını tespit etmek amacıyla PIN (Personal Identification Number- Kişisel Tanımlama Numarası), fotoğraf, biyometrik veri ve sertifika bilgisi gibi yöntemler kullanılmaktadır. Pin, T.C. Kimlik numarasının gizli olarak saklandığı ve 6 rakamdan oluşan bir şifredir. Kişi, kimlik doğrulama sırasında bu şifreyi girer ve doğrulama işlemi yapılır. T.C. Kimlik üzerine kaydedilmiş biyometrik fotoğraf ile kişinin görüntüsünün karşılaştırılması ile yapılan doğrulama fotoğraf doğrulamasıdır. Biyometrik veri, T.C. Kimlik kartı sahibinden alınan parmak izinin, kişinin parmak iziyle eşleştirilmesi sonucunda yapılan doğrulamadır. Sertifika bilgisi ise T.C. Kimlik Kartı üzerinde tutulan sertifikaların kimlik doğrulama sırasında doğrulanmasıdır.

2.6.4. Emniyet Trafik Kontrol Sistemi

Akıllı ulaşım sistemleri kapsamında, karayollarında güvenli seyahat sağlamak için trafik akışını kontrol eden ve yönlendiren trafik kontrol sistemleri kullanılmaktadır. Bu sistemler, değişken mesaj işaretleri, değişken trafik işaretleri, trafik lambaları, yüksek araç detektörleri ve araç varlık sensörlerini içermektedir. Bu bileşenler, tünel kontrol merkezinde bulunan SCADA (Supervisory Control And Data Acquisition-Gözetim Kontrol ve Veri Toplama) sistemiyle birlikte entegre bir şekilde çalışmaktadır. Trafik kontrol sistemi, önceden belirlenmiş senaryolara göre otomatik olarak çalışabilmekte veya kontrol merkezi operatörünün talimatlarına göre işleyebilmektedir (Savronik, 2024).

Akıllı ulaşım sistemleri olarak adlandırılan gelişmiş yüksek teknoloji uygulamalarından faydalanılarak, kentlerde meydana gelen anlık trafik akışının gerçek zamanlı olarak izlendiği ve kontrol edilebildiği trafik kontrol sistemlerinin bir parçası olan sinyalizasyon, 19. yüzyılın sonundan itibaren ulaşım alanına giren araçlardan biridir. Dünya ölçeğinde yaygın olarak 1960 sonrasında kentsel alanlarda sinyal lambalarının kullanıldığı bilinmektedir. Yaya butonu, yaya talebinin algılanmasını sağlayarak, yaya geçişine izin veren, geçiş talebi olmadığında ise kavşaktaki yaya fazını atlayarak araç trafiğinin sürekli akışını sağlayan, sinyal direği üzerine yerleştirilmiş düğmedir. Geri sayım cihazı, hem araç ve hem de yayalar için çevrim süresi içerisinde yeşil ve kırmızı sinyal sürelerinin geri sayımını gösteren 2 ve 3 dijitli cihazlardır. Kavşak gözlem kamerası, sinyalize kavşaklara yakın konumlanmış kameralardır. Bu sayede trafiğin durumu gözlenmekte, kavşaklardaki trafik yoğunluğuna göre sinyal sürelerinde anlık değişiklik yapılmaktadır (İBB, 2024).

Emniyet trafik kontrol sistemi, klasik yöntemlerle yapılan trafik kontrol sistemini ortadan kaldırarak, akıllı kimlik kartlarına yüklenen bilgilerle zamansal tasarruf sağlayan bir sistem olarak geliştirilmiştir. Eski sistemde sürücülerin bir dizi kağıt belgeyi yanlarında taşımaları gerekmiş ve trafik kontrolleri sırasında bu durum zaman kaybına neden olmuştur. Ancak yeni sistem, akıllı kart üzerine yüklenen bilgilerle bu süreci daha hızlı ve maliyet açısından daha verimli hale getirmektedir. Akıllı kimlik kartları sayesinde sürücülerin belgelerini taşıma zorunluluğu ortadan kalkmaktadır. Ayrıca vergi, ceza gibi bilgiler elektronik ortamda kontrol edilebilmektedir. Başka bir ifade ile akıllı kartlı sürücü belgesi sayesinde sürücünün bilgilerine hızlıca erişim sağlanmaktadır. Bu kart ile sürücünün önceki trafik suçlarına ulaşılabilmekte, ayrıca ruhsatın yerine akıllı kart kullanılarak araç ile ilgili bilgilere erişmek ve işlem yapmak daha hızlı ve güvenli hale gelmektedir. Bu sayede, aracın çalıntı olup olmadığı, muayene süresinin dolup dolmadığı, üzerinde herhangi bir tehdit olup olmadığı gibi bilgilerin kontrolü de kolaylaşmaktadır (Şanslı, 2007, s. 29).

2.6.5. Sağlık Bilgi Sistemi

Sağlık bilgi sistemi, hastalarla ilgili geniş kapsamlı bilgileri içeren bir tıbbi kayıt sistemidir. Hastaların kişisel bilgilerinden sağlık problemlerine, ilaç kullanımından sağlık sigortası bilgilerine kadar detaylı bilgileri içermektedir. Doktorlar, bu sistem sayesinde

hastaların elektronik tıbbi kayıtlarını tutabilmekte ve hızlı bir şekilde tıbbi müdahalelerde bulunabilmektedir. Kamu ve özel sağlık kurumları arasında veri uyumsuzluğunu ortadan kaldırmak için akıllı kimlik kartı uygulaması kullanılarak vatandaşın tıbbi müdahale durumunda kimlik ve sağlık bilgilerine erişim sağlanmakta ve bu durum da vatandaşların işlemlerini kolaylaştırmaktadır (TÜBİTAK-UEKAE, 2006).

Günümüzde birçok ülkede sağlık sistemlerinde akıllı kimlik kartları kullanılmaktadır. Bu kartlar sayesinde sağlık personeli, kişilerin sağlık bilgilerine anında erişim sağlamaktadır. Kartlar içinde kişinin özlük bilgileri, geçirdiği hastalıklar, tedavileri, kullandığı ilaçlar ve alerjik tepkiler gibi bilgiler bulunmaktadır. Bu veriler değerlendirilerek hastanın daha etkili ve hızlı bir şekilde iyileşmesini sağlamak için tedavi yöntemleri geliştirilebilmektedir (Şanslı, 2007, s. 29).

2.6.6. Nakit Akış Sistemi

Nakit akış sistemi, vatandaşın nakit işlemleri ve müşterisi olduğu banka hesaplarına ilişkin verilerin saklandığı sistemdir. Günümüzde nakit ödemeler genellikle bankalar tarafından verilen bankamatik veya kredi kartlarıyla yapılmaktadır. Bu kartlar, POS (Point Of Sale) cihazlarıyla kullanılarak ödeme işlemleri gerçekleştirilmektedir. Kartlar, kişinin kimliğinin yerini almakta ve merkez veri tabanından bağlı olduğu hesaptan ödeme yapılmaktadır. Ancak manyetik şeritli kartların kopyalanabilir olması ve zayıf güvenlik önlemleri nedeniyle sahtecilik ve kart kullanımı sorunları ortaya çıkmaktadır. Şanslı, (2007) çalışmasında tasarladığı sistemde, tek bir akıllı kimlik kartı ile bireylere, banka hesaplarının tutulduğu bir veri tabanı havuzu oluşturulmakta ve kişilerin hesaplarına ait kayıtlar burada tutulmaktadır. Tek kart uygulaması ile akıllı kimlik katlarının nakit akış sisteminde kullanımının mümkün olabileceği düşünülmektedir.

2.7. NFC (Near Field Communication-Yakın Alan İletişimi) ve Akıllı Kimlik Kartları

NFC, iki elektronik cihazın kısa mesafede güvenli bir şekilde iletişim kurmasını sağlayan bir kablosuz teknolojidir. Bu teknoloji, radyo frekansları kullanarak 13.56 MHz frekansında ve düşük bant genişliğinde (en fazla 424 Kbit/s) veri iletişimi sağlamaktadır. NFC'nin kısa mesafede çalışması, güvenlik açısından avantaj sağlamaktadır (Özdenizci vd., 2016, s. 1).

2011 ve 2012 yıllarında NFC'nin yaygınlaşması hedeflenmiştir. Bugün bu hedefin büyük ölçüde gerçekleştiği, mobil cihazlarda ve akıllı kimlik kartlarında yaygın olarak kullanıldığı görülmektedir (Yılmaz vd., 2014, s. 595).

NFC teknolojisi son yıllarda hızla gelişen bir alandır. Bu teknoloji, ödeme sistemlerinde, akıllı kimlik kartlarında, akıllı telefonlarda, akıllı ev cihazlarında ve daha birçok alanda kullanılmaktadır. Ayrıca, NFC teknolojisi QR kodlarına benzer şekilde, etiketlerin ve nesnelerin etrafına yerleştirilen NFC etiketleriyle de kullanılabilmektedir. (SecroMix, 2024).

Şekil 4. NFC Teknolojisi Kullanım Alanları

Kaynak: SecroMix,2014

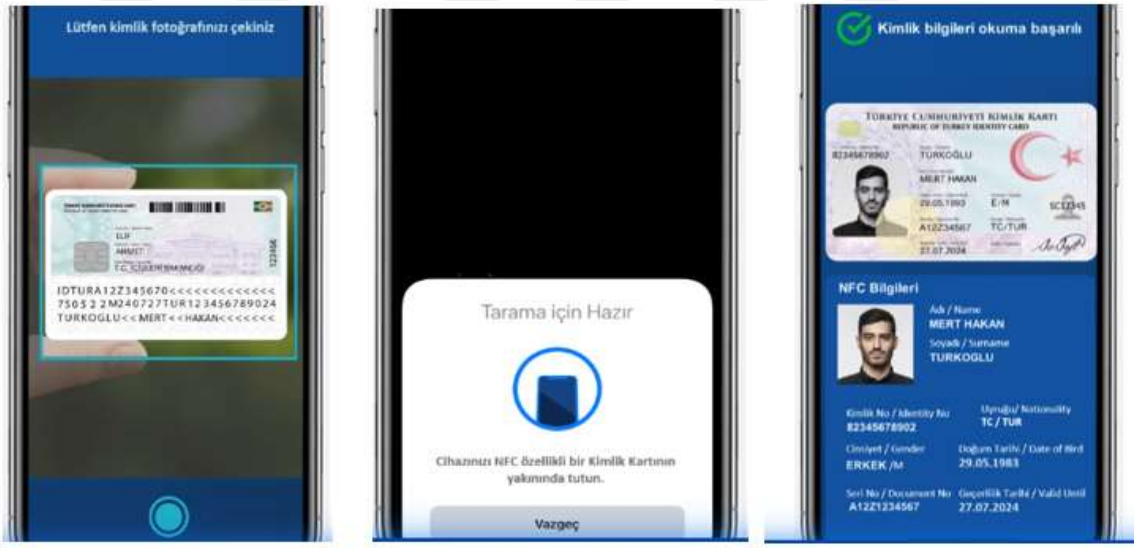
Şekil 4'te, NFC teknolojisinin çeşitli kullanım alanları görselleştirilmiştir. Bu görsele göre, NFC'nin kullanım alanları arasında kimlik doğrulama (identification), biletleme (ticketing), bağlılık ve üyelik programları (loyalty and membership), nakitsiz ödeme (cashless payment), toplu taşıma (transit), güvenli bilgisayar oturumu açma (secure PC log-on), fiziksel erişim kontrolü (physical access) ve zaman ve katılım takibi (time and attendance) yer almaktadır.

NFC ve akıllı kimlik kartlarının bazı kolaylıkları şunlardır:

- ✓ NFC özellikli akıllı telefonlar ile yeni çipli T.C. Kimlik Kartınızı okutarak bankaların dijital kanallarını kullanabilirsiniz.

- ✓ NFC özellikli bir mobil cihaz ve akıllı kimlik kartı kullanarak, LinkedIn gibi sosyal medya platformlarında QR kodunu taratarak profilinizi doğrulayabilirsiniz. Bu işlem pasaportla da yapılabilmektedir.
- ✓ NFC özellikli bir cihaz ve yeni çipli kimlik kartınız varsa, telefon numaranızı kimlik kartınızla doğrulayabilirsiniz. Bu, telefon numaranızın size ait olduğunu doğrulamanın güvenli bir yoludur. Başka bir ifade ile kimlik belgesinin üzerindeki çipteki veriler, kimliği veren ülkenin yetkilileri tarafından dijital olarak imzalanmakta ve kopyalanmaya karşı korunmaktadır. NFC teknolojisi ile kimlik belgesinin çipindeki verilere hızlıca erişilerek kimlik doğrulaması yapılabilmektedir (SCSoft, 2024).

Şekil 5. NFC ile Akıllı Kimlik Kartı Doğrulama İşlemi



Kaynak: SCSoft, 2024

Şekil 5'te NFC ile akıllı kimlik kartı doğrulama işlemi gösterilmiştir. Bu görsel, kimlik doğrulama sürecini gösteren üç aşamayı içermektedir:

- ✓ **İlk Aşama: Kimlik Fotoğrafının Çekilmesi:**

Görselin sol tarafında, kullanıcıdan kimlik kartının fotoğrafını çekmesi istenmektedir. Kimlik kartı bir akıllı telefon kamerası ile taranmaktadır.

- ✓ **İkinci Aşama: NFC Tarama Hazırlığı:**

Orta kısımda, cihazın NFC özellikli olduğu belirtilmiş ve kullanıcının kimlik kartını cihazın yakınına tutması istenmiştir. Bu aşama, NFC teknolojisi kullanarak kimlik kartındaki bilgilerin taranması için hazırlık yapıldığını göstermektedir.

- ✓ **Üçüncü Aşama: Kimlik Bilgilerinin Okunması:**

Sağ tarafında ise, NFC taramasının başarılı bir şekilde tamamlandığı ve kimlik kartındaki bilgilerin okunarak ekrana yansıtıldığı görülmektedir. Kimlik sahibinin fotoğrafı, adı, soyadı, kimlik numarası, uyruğu, cinsiyeti, doğum tarihi ve kimlik kartının geçerlilik tarihi gibi detaylar görüntülenmektedir.

Bu süreç, kimlik doğrulamanın güvenli ve hızlı bir şekilde yapılmasını sağlamaktadır. Özellikle NFC teknolojisinin kullanılması, kimlik bilgilerinin doğruluğunu artırmakta ve manuel giriş hatalarını minimize etmektedir. Bu tür bir doğrulama, güvenli oturum açma, fiziksel erişim kontrolü gibi çeşitli uygulamalarda kullanılabilir.

2.8. Akıllı Kimlik Kartlarının Avantajları ve Potansiyel Riskleri

Teknolojik ilerlemeler, beraberinde yeni risk unsurlarını da getirmektedir. Akıllı kimlik kartlarının getirdiği olumlu etkilerin yanı sıra, bazı olumsuz etkiler de bulunmaktadır. Akıllı kimlik kartları da teknolojik gelişmelerin bir sonucudur ve birçok avantaj sunar. Örneğin, kimlik doğrulama süreçlerini kolaylaştırır, güvenliği artırır ve çeşitli hizmetlere erişimi kolaylaştırır. Ancak, bu teknolojik yeniliklerin beraberinde getirdiği riskler de vardır. Özellikle, kişisel verilerin kötü niyetli kişilerin eline geçme riski gibi güvenlik endişeleri söz konusudur (Alkhurayyif, 2013, s. 44).

2.8.1. Akıllı Kimlik Kartlarının Avantajları

Akıllı kimlik kartlarının kullanımı, suçla ve terör eylemleriyle mücadelede, yasadışı göçle mücadelede ve kamu hizmetlerine erişimin artmasında önemli avantajlar sunmaktadır. Ayrıca, bilgilerin tek bir kartta toplanması gibi birçok faydayı içermektedir. Bu avantajlar aşağıda başlıklar halinde sıralanmıştır (Alkhurayyif, 2013, s. 44):

- ✓ **Suçla ve Terör Eylemleriyle İlgili Mücadele:**

Akıllı kimlik kartlarının kullanımıyla kimlik hırsızlığının önüne geçilebilecektir. Bu durum, terörist eylemlerin tespitinde yardımcı olmanın yanı sıra elektronik para suçlarının aklanmasını engellemede de avantaj sağlayacaktır.

- ✓ **Yasadışı Göçle Mücadele:**

Tüm vatandaşlar için kimlik kartlarının zorunlu hale getirilmesi durumunda, yasadışı göçmenlerin tespiti kolaylaşacak ve aynı zamanda yasa dışı çalışanların belirlenmesine de olumlu katkı sağlanacaktır.

- ✓ **Kamu Hizmetlerine Erişimin Arttırılması:**

Kişisel bilgilerin tek bir merkezde toplanması, kamu hizmetlerinin sunumunu kolaylaştıracaktır. Bu durum, kırtasiye masraflarının azalmasına ve zamandan tasarruf sağlanmasına olanak tanıyacaktır.

- ✓ **Bilgileri Tek Bir Kartta Toplama:**

Kişisel bilgileri içeren akıllı kimlik kartları, kimlik numarası, doğum yeri, doğum tarihi, cinsiyet, kan grubu, kimlik veriliş tarihi, anne-baba adı, meslek gibi bilgileri içerir. Bu bilgiler, kartın içerisinde bulunan çip üzerinde saklanır. Ayrıca, akıllı kimlik kartları parmak izi, iris ölçümü ve tıbbi veriler gibi bilgileri de kaydedebilir ve merkezi veri tabanına bağlanabilir.

- ✓ **Daha Fazla Kolaylık Sunma:**

Akıllı kimlik kartına sahip olanlar, Körfez Arap Ülkeleri İş Birliği Konseyi (KİK) ülkelerine seyahat etmek için pasaportlarını yanlarında bulundurma zorunluluğu olmadan seyahat edebilirler. Ayrıca, sürücü belgelerini taşıma gereği olmadan, ehliyetin alındığı tarih, nerede alındığı ve hangi sınıf ehliyete sahip olduğu gibi bilgilere akıllı kimlik kartı üzerinden erişilebilir.

- ✓ **Güvenli ve Sağlıklı Oy Kullanımı:**

Akıllı kimlik kartı uygulamasının bir diğer avantajı, genel ve yerel seçimlerde seçmen listesinin oluşturulması ve oy kullanımında güvenli ve sağlıklı bir ortam sağlamasıdır. Kişiler, önceden seçmen olarak kayıtlı olmasalar bile, daha sonra oy kullanmaya karar verdiklerinde ikamet ettikleri il ve ilçelerde oy kullanabileceklerdir. Seçim bölgelerinde oy kullanması gereken kişilerin ikamet adreslerini Seçim Kurulu'na güncelleme konusunda ihmal etmeleri sıkça gözlemlenmektedir. Elektronik kimlik sistemi sayesinde, mükerrer oy kullanımı veya oy kullanmamanın önüne geçilecektir.

2.8.2. Akıllı Kimlik Kartlarının Potansiyel Riskleri (Dezavantajları)

Akıllı kimlik kartlarının getirdiği avantajların yanı sıra, metin yönetiminin yüksek maliyeti, gizlilik ihlali riski, dolandırıcıların ve hackerlerin kimlik bilgilerini ele geçirme tehdidi, özgürlüğün kısıtlanması, kişi denetiminin artması ve olası suiistimaller gibi çeşitli potansiyel riskler de bulunmaktadır. Bu dezavantajlar aşağıda başlıklar halinde sıralanmıştır (Alkhurayyif, 2013, s. 45):

- ✓ **Metin Yönetiminin Maliyetli Olması:**

Akıllı kimlik kartlarının oluşturulması ve yönetimiyle ilgili kurumların yüksek maliyetlerle karşılaştığı gözlemlenmektedir. Kartların oluşturulması, dağıtımı, personel sayısı, güvenlik anahtarlarının üretimi gibi unsurların yanı sıra, sistemdeki biyolojik verilerin güncellenmesi gerekliliği gibi faktörler, yönetim maliyetlerini artırmaktadır. Ayrıca, evlilik, askerlik, adli sicil gibi kişisel bilgilerin güncellenmesi gerektiği durumlarda kartların güncellenmesi gerekmekte, bu da ek maliyetlere neden olmaktadır.

- ✓ **Gizlilik İhlali:**

Vatandaşın tüm bilgilerinin tek bir merkezde toplanması, doğal olarak bazı risklerin ortaya çıkmasına neden olur. Bu bilgilere erişim yetkisi olan herkesin, vatandaşın hassas verilerine erişebilme riski mevcuttur. Bu durum, bireylerin hak ve özgürlüklerinin ve mahremiyetinin ihlal edilmesine yol açabilir.

- ✓ **Dolandırıcıların ve Hackerlerin Kimlik Bilgilerini Ele Geçirme Tehdidi:**

Güvenlik önlemlerini artırıcı şifreleme yöntemleriyle benzersiz bir kimlik kartı üretimi hedeflenmiş olsa da bu bilgilerin tek bir merkezde toplanması ve tüm bilgilerin sisteme kaydedilmesi, dolandırıcıların ve hackerlerin kişisel bilgilere daha kolay erişmesini sağlayabilir.

- ✓ **Özgürlüğün Kısıtlanması, Kişi Denetiminin Artması ve Olası Suiistimaller:**

Vatandaşın kötüye kullanım riskiyle karşı karşıya olması durumu, devlet tarafından verilen yetkilerle görevini yerine getiren çalışanların, vatandaşları tehdit etme ve kişisel çıkar sağlama olasılığını artırabilir.

Özetle akıllı kartlar birçok alanda kullanılmaktadır. Finans alanında, bankacılık sistemlerinde yaygın olarak kullanılmaktadır. Telekomünikasyon alanında, cep telefonlarında SIM kartlar olarak kullanılmaktadır. Sağlık alanında, sağlık bilgilerine erişim için kullanılmaktadır. Ulaşım alanında toplu taşıma sistemlerinde ücretlendirme ve kontrol için kullanılmaktadır. Kimlik alanında, nüfus, ehliyet, sağlık kartları gibi kimliklerin yerine kullanılmaktadır. Trafik alanında, sürücü belgeleriyle ilgili bilgilere anında erişim sağlamakta ve işlem yapmayı hızlandırmaktadır (Şanslı, 2007, s. 30)

3. BÖLÜM: MAHREMİYET VE GÜVENLİK BAĞLAMINDA AKILLI KİMLİK KARTLARI

3.1. Mahremiyetin Tanımı ve Toplumsal Önemi

Mahrem kelimesi, Arapça "haram" kelimesinden gelmekte ve yasaklanan, kutsal, tabu gibi anlamları içermektedir. Aynı kökten türemiş olan mahremiyet kavramı ise TDK sözlüğünde "gizlilik" olarak tanımlanmış ve samimiyeti, kişinin evlenemeyeceği kişileri ve herkese açık olmayan şeyleri ifade etmektedir (Vardi, 2015, s. 54).

Mahremiyet, sosyal bilimlerde yakınlık ve özel hayatı ifade etmekte ve bireyin başkalarıyla paylaşmak istemediği, koruduğu her şeyi kapsamaktadır. Bireyler özel hayatlarında, başkalarının yargısından uzak, kendilerini serbestçe ifade edebilmektedir. İnsan ruhu, başkalarının bakışlarından uzak, özgürce var olabileceği alanlara ihtiyaç duymaktadır. Tam bir açıklık ise ruhsal tükenişe yol açabilmektedir (Aslan-Turan, 2022, ss. 846-847). Başka bir ifade ile görünür olmak, mahremiyetin ihlal edilmesine yol açmaktadır. Modern hukukta mahremiyet,

"Mahremiyet, genel olarak, kişilerin yalnız başına kalabildikleri, istedikleri gibi düşünüp davranabildikleri, başkalarıyla hangi yer, zaman ve koşullarda ne ölçüde ilişki ve iletişim kuracaklarına bizzat kendilerinin karar verebildikleri bir alan ve bu alan üzerinde sahip olunan hakkı ifade eder. Bununla birlikte, insanın günlük yaşantısının çok önemli bir parçasını oluşturan mahremiyet hakkı, başkalarını tamamen dışlamak veya onlarla olan ilişkiyi tümüyle kesmek anlamına gelmez. Sadece bir kimsenin, kendi hayatını başkalarıyla ne ölçüde paylaşacağını belirleme hakkına sahip olduğunu ifade eder."(Yüksel, 2003, s. 182)

Mahremiyetin tehdit altında olduğu üç temel kaynak vardır: kendini açıklama, merak ve gözetleme (Yüksel, 2003, s. 185). Mahremiyet ihlali, kişinin kendi mahremiyetini ihlal etmesiyle ortaya çıkmaktadır. Merak, bilgi akışında önemli bir rol oynamaktadır ve özellikle aile ve komşuluk gibi ilişkilerde yaygındır. Merak, karşısındaki kişinin özel hayatını inceleme, gözlemleme ve mahrem bilgilere erişme isteği olarak ortaya çıkmaktadır. Gözetim ise bir kişinin başka birinin mevcut düzen ve kurallara uyumunu izleme sürecidir (Akçadağ, 2024, ss. 91-92).

Yeni nesil teknolojik ürünlerden akıllı kimlik kartlarındaki mahremiyet kartta saklanan bilgilerin gizliliğini içermek ve kart kullanıcıları için büyük önem taşımaktadır.

3.2. Mahremiyetin Tarihsel Gelişimi ve Kökenleri

Özel yaşam olarak da tanımlayabileceğimiz mahremiyet, aslında tarih boyunca var olan ancak modernleşme süreci ile özellikle bireyin ve özel yaşamın tanımlanmasıyla birlikte yeni bir anlam kazanan bir olgudur. Modernleşme, sosyal hareketlilik, iş bölümü ve uzmanlaşma gibi süreçlerle birlikte mahremiyet, toplumda daha önemli bir konuma gelmiş ve zamanla hukuki olarak da tanınmış ve düzenlenen bir hak haline dönüşmüştür (Yüksel, 2003, s. 182).

Mahremiyet kavramının tarihsel gelişimi incelendiği vakit tarih öncesi çağlarda mitler, söylenceler ve masallar ile günümüz kadar ulaşan bilgiler mevcuttur. Özellikle ilkel kabilelerde totem anlayışı mahremiyet ile ilişkilidir. Bu bölümde mahremiyetin kavramının gelişimi, kültürel yaklaşımlar ve sosyal normlar ve mahremiyet alt başlıklarında ele alınmıştır.

- ✓ **Kültürel Yaklaşımlar:**

Farklı kültürlerde mahremiyetin nasıl algılandığı ve değerlendirildiği konusu kültürel yaklaşımlar alt başlığının ana odak noktasını oluşturmaktadır. Mahremiyet kavramı ilkel toplumlarda ensest ilişkileri engelleyen bir kavram olarak karşımıza çıkmaktadır. İlkel kabilelerde totem anlayışı, aynı totem grubuna mensup olanlar arasında evlilik ve cinsel ilişkinin yasak olduğunu belirtmektedir. Totem grubunun toplantılarında erkekler ve kadınlar ayrı kamplarda bulunurdu. Kadınlar erkeklerin kampına giremezdi. Ölüm durumunda ise, kişinin saçları hemen kesilir ve cenaze uzak bir yere gömülür, bu sırada kadınlar ve ergin olmayan gençler bu törene katılamazlardı. Ensest kavramında akrabalık önemlidir ve egzogami, kendi klan grubu dışından evlenmeyi ifade etmektedir. İlkel toplumlarda aynı toteme sahip olanlar akraba olarak kabul edilirken, günümüzde kan bağıyla birbirlerine bağlı olanlar akraba olarak tanımlanmaktadır. Ensest yasağı ve egzogami (bireyin kendi klan grubu dışından biriyle evlenmesi) ilişkilidir. Egzogaminin başlangıcında kız kaçırma gibi uygulamalar önemli rol oynamış ve bu durum da egzogamiyi ve ensest yasağını şekillendirmiştir (Kartopu & Dağcı, 2015, s. 145).

- ✓ **Sosyal Normlar ve Mahremiyet:**

Sosyal normlar ve mahremiyet konusu oldukça geniş kapsamlı bir konudur. Bu konudaki toplumsal ve küresel normlar küresel mahremiyet normları ve ilkeler başlığında etraflıca

açıklanmıştır. Sosyal normlar ve mahremiyet konusu iletişim ve mahremiyet ile teknoloji ve mahremiyet konularını da kapsayan bir konudur.

3.3. Küresel Mahremiyet Normları ve İlkeleri

Küresel mahremiyet normları ve ilkeleri bölümü, Avrupa Birliği'nde (AB) yapılan düzenleme Genel Veri Koruma Yönetmeliği, Birleşmiş Miletler Mahremiyet İlkeleri ve diğer küresel anlaşmalar ve ilkeler alt başlığında incelenmiştir.

3.3.1. GDPR'nin İncelenmesi ve Etkileri

General Data Protection Regulation (GDPR-Genel Veri Koruma Yönetmeliği), 27 Nisan 2016 tarihinde yayımlanan, AB'de kişisel verilerin işlenmesi ve bu verilerin korunmasıyla ilgili bir düzenlemedir. Temel amacı, AB vatandaşlarının kişisel verilerinin işlenmesi sırasında daha yüksek bir koruma seviyesi sağlamaktır. Genel hükümler, prensipler, veri sahibinin hakları, denetleyici ve işlemci, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması, bağımsız denetim otoriteleri, iş birliği ve tutarlılık, çözümler, sorumluluklar ve cezalar, belirli işleme durumlarına ilişkin hükümler, devredilen tasarruflar ve uygulama tasarrufları ve nihai hükümlerin yer aldığı 11 bölüm ve 99 maddeden oluşmaktadır (GDPR, 2024).

GDPR'de, kişisel verilerin işlenmesi, temel bir hak olarak kabul edilmektedir. Avrupa Birliği Temel Haklar Bildirgesi'nin 8. maddesi ve Avrupa Birliği İşleyişine İlişkin Antlaşma'nın 16. maddesi, herkesin kişisel verilerinin korunma hakkına sahip olduğunu belirtmektedir. Kişisel verilerin işlenmesiyle ilgili prensipler ve kurallar, herkesin temel hak ve özgürlüklerini, özellikle kişisel verilerinin korunma hakkına saygı göstermelidir (GDPR, 2024).

3.3.2. Birleşmiş Milletler Mahremiyet İlkeleri

The United Nations (UN-Birleşmiş Milletler-BM), 1945 yılında kurulan ve şu anda 193 Üye Devleti içeren uluslararası bir kuruluştur. BM'nin çalışmaları, kuruluş şartnamesinde belirtilen amaçlar ve ilkeler doğrultusunda yönlendirilmektedir. BM'nin organları Genel Kurul, Güvenlik Konseyi, Ekonomik ve Sosyal Konsey, Vesayet Konseyi ve Uluslararası Adalet Mahkemesi ve BM Sekreteryasıdır (T.C. Dış İşleri Bakanlığı, 2024).

Genel Kurul, BM'nin ana müzakere, politika oluşturma ve temsil organıdır. BM'nin 193 Üye Devletinin tamamı Genel Kurul'da temsil edilmekte ve bu durum Genel Kurul'u, evrensel temsile sahip tek BM organı yapmaktadır. Her yıl, Eylül ayında, BM'nin tam üyeleri, birçok devlet başkanının katılıp konuşma yaptığı yıllık Genel Kurul oturumu ve genel tartışmalar için New York'taki Genel Kurul Salonu'nda toplanmaktadır. Barış ve güvenlik, yeni üyelerin kabulü ve bütçe konuları gibi önemli sorunlara ilişkin kararlar, Genel Kurul'un üçte iki çoğunluğu ile diğer sorulara ilişkin kararlar ise basit çoğunlukla alınmaktadır. Genel Kurul her yıl bir yıllık görev süresi için bir Başkan seçmektedir (UN, 2024).

Güvenlik Konseyi, BM Şartnamesi uyarınca uluslararası barış ve güvenliğin korunmasından birincil sorumluluğa sahip olan 15 Üyesi (5 daimi ve 10 daimi olmayan üye) bulunan ve her üyenin bir oy hakkı olan konseyidir. Şartname uyarınca, tüm Üye Devletler Konsey kararlarına uymakla yükümlüdür. Güvenlik Konseyi, barışa yönelik bir tehdidin veya saldırı eyleminin varlığının belirlenmesinde öncülük yapmaktadır. Anlaşmazlığın taraflarını barışçıl yollarla çözüme çağırmakta ve düzeltme yöntemleri veya çözüm koşulları önermektedir. Bazı durumlarda Güvenlik Konseyi, uluslararası barış ve güvenliği korumak veya yeniden tesis etmek için yaptırım uygulamaya başvurabilmekte ve hatta güç kullanımına izin verebilmektedir. Güvenlik Konseyi'nin her ay dönüşümlü olarak değişen bir Başkanlığı vardır (UN, 2024).

BM Kişisel Verilerin Korunması ve Gizliliğine İlişkin İlkeler, BM Gizlilik Politikası Grubu (UNPPG) tarafından oluşturulmuş ve 2018 yılında BM sistemi tarafından kabul edilmiştir. BM sistem kuruluşları tarafından veya onlar adına, zorunlu faaliyetleri yerine getirirken "kişisel verilerin" işlenmesine ilişkin temel bir çerçeve ortaya koymaktadır. Bu ilke seti, Birleşmiş Milletler Sistem Kuruluşları veya adlarına çalışanlar tarafından zorunlu görevler sırasında işlenen kişisel veriler için bir çerçeve sunmaktadır. Amaçları arasında;

- ✓ Birleşmiş Milletler Sistemi genelinde kişisel veri koruma standartlarının uyumlu hale getirilmesi,
- ✓ Sorumlu bir veri işleme sürecinin kolaylaştırılması,
- ✓ Bireylerin insan haklarına ve temel özgürlüklerine saygı gösterilmesi

yer almaktadır. Bu ilkeler, herhangi bir biçimde işlenen ve kişisel veri içeren tüm durumlar için geçerlidir.

BM, ayrıca 28 Mayıs 2020 tarihinde COVID-19 salgınına karşı veri koruma ve gizliliğini destekleyen bir ortak açıklama da yapmıştır. Bu açıklama, kişisel verilerin kullanımını salgınla mücadelede gizliliği ve insan haklarını koruyacak şekilde yönlendirmektedir. Açıklama, dijital temas takibi gibi yöntemlerin virüsün yayılmasını izlemede ve BM'nin görevlerini uygulamada yardımcı olabileceğini belirtmektedir. Ancak bu veri işleme faaliyetlerinin kişisel ve hassas verilerin korunmasına dikkat edilerek yapılması gerektiği vurgulanmaktadır. İşlemler yasal, sınırlı, zamanlı, gerekli ve orantılı olmalıdır. Ayrıca, veri kullanımı şeffaf olmalı ve insan haklarına saygı gösterilmelidir. Bu ilkeler, sadece COVID-19 salgınıyla sınırlı değildir, gelecekte emsal teşkil edecek durumlarda veri kullanımı konusunda bir örnek teşkil edecektir (UN, 2024).

3.3.3. Diğer Küresel Anlaşmalar ve İlkeler

Mahremiyet konusunda GDPR ve BM gizlilik ilkeleri dışında, küresel ölçekte birkaç önemli anlaşma ve ilke bulunmaktadır. Bu anlaşma ilkelerden bazıları şunlardır:

- ✓ **Avrupa İnsan Hakları Sözleşmesi (ECHR):**

Avrupa Konseyi tarafından hazırlanan ve insan haklarını ve temel özgürlükleri koruyan bir anlaşmadır. ECHR'nin "Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir." olan 8. maddesi, mahremiyet hakkını korumakta ve özel yaşamın ve haberleşmenin gizliliğini güvence altına almaktadır (ECHR, 2024).

- ✓ **Amerikan İnsan Hakları Sistemi:**

Amerika Kıtası'nda, Amerikan Devletleri Örgütü (Organization of American States-OAS) bünyesinde Amerikan İnsan Hakları Komisyonu ve Amerikan İnsan Hakları Mahkemesi gibi kurumlar aracılığıyla insan hakları ve mahremiyet konularında çeşitli

anlaşma ve ilkeler bulunmaktadır. Özellikle, Amerikan İnsan Hakları Sözleşmesi, kişisel sorumluluklar başlığı altında her insanın ailesine, toplumuna ve insanlığa karşı sorumluluğunu vurgulamaktadır. Sözleşme, haklar ve ödevlerin diğerlerinin haklarıyla sınırlı olduğunu belirtmekte ve toplamda 82 maddeden oluşmaktadır. Medeni ve siyasi hakları içeren sözleşme ikili devlet ilişkileri yerine insan haklarının tarafsız bir hukuki rejim altında korunmasını amaçlamaktadır (Aslan, 2016, s. 268).

- ✓ **Ekonomik ve Sosyal Konsey (ECOSOC) Kararları:**

ECOSOC, BM bünyesinde ekonomik, sosyal ve kültürel konularla ilgilenen bir organdır. ECOSOC'un alınan kararlarında, mahremiyet hakkı gibi konulara da değinilmektedir (UN, 2024).

3.4. Akıllı Kimlik Kartları ve Mahremiyet İlişkisi

Dijital devrim ve teknolojinin gelişimi, mahremiyet kavramının biçim ve algılanışını değiştirmiştir. Daha önceleri bedensel gizlilik ile ilişkilendirilen mahremiyet kavramı günümüzde internet gizliliği ve kişisel verilerin korunması olarak algılanmaya başlanmıştır. Kişisel yetkiye erişim ve bu verilerin dağılımının kullanılması, modern dünyanın önemli bir sorunu haline gelmiştir (Eroğlu, 2018, s. 131).

Geçmişten günümüze sanayi devrimleri ve teknolojinin gelişimi incelendiği vakit buhar teknolojisinin üretimde kullanılması ile başlayan Endüstri 1.0 sanayi devrimini, elektriğin icadı ile buharlı makinelerin yerini elektrikli makinelerin alması ile Endüstri 2.0 sanayi devrimi almış ve sonrasında ve 1950'lere gelindiği vakit Alan M. Turing tarafından devrim yaratan bir araştırma sorusu ortaya atılmıştır. "Can machine thinks? (Makineler düşünebilir mi?) Bu süreçten sonra Endüstri 3.0 ya da bilgisayar çağı olarak adlandırılan süreç başlamış ve bu süreci 2011 Almanya Hannover Fuarı'nda lansmanı yapılan Endüstri 4.0 sanayi devrimi takip etmiştir. Dördüncü sanayi devriminden sonra 2016 yılında Japonya'da "5. Bilim ve Teknoloji Temel Planı" olarak resmen önerilen ve Toplum 5.0 ya da Cobot (kolaboratif robot) Teknolojisi olarak tanımlanan Endüstri 5.0 sürecinin ise diğer bütün sanayi ve teknolojik gelişmelerden ayırt edici tarafı mahremiyet ve güvenlik konuları olmuştur. Beşinci Sanayi Devrimi olarak görülen bu dönem, toplumla teknolojiyi entegre etme amacı nedeniyle Endüstri 5.0 yerine "T5.0" olarak adlandırılmıştır (Çalış Duman, 2022, s. 313). T5.0, Endüstri 4.0 dan sonra 5. aşamada

başlatılan insan merkezli yeni toplum vizyonudur. Başka bir ifade ile T5.0 olarak adlandırılan bu süreç aslında, siber-fiziksel sistemler aracılığı ile insan güvenliği ve refahı için sürdürülebilir bir toplum yaratmayı amaçlamaktadır. Akıllı teknolojilerin en büyük sorunlarından birisi de güvenlik ve mahremiyet konularıdır. Bu perspektiften güvenlik bir zorunluluk olmakla birlikte, cobot pazarına girmenin de temelini oluşturmaktadır.

Günümüz dijital devrimleri arasında sayılan akıllı kimlik kartlarının, teknolojinin ilerlemesiyle birlikte, kullanımı genişlemiş; ancak bu durum, mahremiyet ihlalleri ve güvenlik sorunlarına ilişkin endişeleri de beraberinde getirmiştir. Akıllı kimlik kartları ve mahremiyet ilişkisine dair literatür incelemesi, kullanıcı merkezli kimlik yönetimi sistemlerinin mahremiyeti nasıl etkilediğine ve bu alandaki zorluklara odaklanmaktadır. Literatürdeki çeşitli araştırmalar, akıllı kimlik kartlarının mahremiyet ve güvenlik boyutlarını ele alarak, olası riskler ve bu risklerle başa çıkma yöntemlerini araştırmıştır.

Bu perspektiften bakıldığında, Hiltz ve arkadaşlarının (2003) yaptığı çalışma, akıllı kimlik kartlarına ilişkin mahremiyet endişelerini ve güvenlik zorluklarını ortaya koymaktadır. Yapılan analizler, izleme teknolojilerinin mahremiyet üzerindeki potansiyel etkilerine odaklanırken, karşı çözüm önerileri geliştirmeyi sağlamaktadır. Çalışmalarında, akıllı kimlik kartlarının tasarımında mahremiyeti koruyucu ve güvenlik açıklarını azaltıcı yöntemlerin yollarını vurgulamaktadır. Juang ve arkadaşları (2008), akıllı kimlik kartları aracılığıyla, güçlü ve etkili bir kullanıcı kimliği sunma sistemi önermektedirler. Bu sistem, mahremiyetin korunması, düşük maliyet ve yüksek güvenlik gibi özelliklere dikkat çekmektedir. Bu çalışma, akıllı kimlik kartlarının güvenlik ve mahremiyet odaklı bir yaklaşımla nasıl iyileştirilebileceğine ilişkin önemli bilgiler sunmaktadır.

Lim ve arkadaşlarının (2009) çalışmasında, internet kullanıcılarının mahremiyet kaygıları ve ulusal kimlik kartlarına olan tutumları incelenmektedir. E-devlet uygulamaları ve finansal gözetim gibi konuların mahremiyet denetimi üzerindeki etkileri incelenmiştir. Bulgular, kullanıcıların mahremiyet konusunda ciddi endişelere sahip olduğunu ve bu endişelerin teknolojik çözümlerle giderilmesinin mümkün olduğunu göstermektedir. Mutlugün ve Adalıer (2009) ise, Türkiye'de e-devlet projeleri kapsamında yeni bir akıllı kimlik kartı sistemini ele almaktadır. Bu sistem, biyometrik veriler ve kriptografik güvenlik özelliklerine dikkat çekmektedir. Çalışma, bu tür bir sistemin vatandaşlık

oranlarının nasıl bir mahremiyet ve güvenlik düzeyini sağlayabileceğini tartışmaktadır. Ceyhan ve arkadaşlarının (2018) yaptığı çalışma, akıllı kimlik kartı güvenlik açıklarına, olası saldırı türlerine ve bu saldırılara karşı alınabilecek önlemlere odaklanmaktadır. Bu çalışma, akıllı kimlik kartlarına yönelik güvenlik zafiyetlerini ve bu zafiyetlerin nasıl giderilebileceğini incelemektedir.

Clauβ ve arkadaşları (2005), kullanıcı mahremiyetini korumaya yönelik araştırmaları ve mekanizmaları ele alırken, Fan ve Lin (2009), biyometrik verileri koruyarak mahremiyeti maksimize etmeyi amaçlayan üç faktörlü kimlik doğrulama şemalarını önermektedir. Yeow ve arkadaşları (2012), akıllı ulusal kimlik kartlarının (SNIC-Smart National Identity Cards) kullanımıyla ilişkili güvenlik ve ergonomi sorunlarını tartışırken, Alkhurayyif (2013), 11 Eylül sonrası güvenlik endişelerinin arttığı ve kimlik kartlarına olan ihtiyacın yeniden değerlendirildiği bir dünyada mahremiyet ve özgürlük kaybı konularına dikkat çekmektedir. Kuada ve arkadaşları (2017) ise, ulusal kimlik sistemlerinin gizlilik endişeleri üzerine bir inceleme yaparak, bu sistemlerin tasarımında gizliliği artırıcı özelliklerin önemini vurgulamaktadır. Singh ve arkadaşları (2018) akıllı kart teknolojisinin güvenilirliğini ve erişim kontrolü gibi işlevlerini ele alarak, bu teknolojinin kimlik yönetiminde nasıl bir çözüm sunabileceğini tartışmaktadır.

Bu literatür genel olarak, akıllı kimlik kartlarının ve kimlik yönetimi sistemlerinin, kullanıcı mahremiyetini korurken aynı zamanda güvenlik ve erişim kontrolü gibi önemli ihtiyaçları nasıl karşılayabileceğine dair bir çerçeve sunmaktadır. Bir başka ifade ile literatürdeki bu çalışmalar, akıllı kimlik kartlarının mahremiyet ve güvenlik boyutlarına geniş bir perspektiften bakmaktadır.

Mahremiyet ihlalleri ve güvenlik politikaları, bu teknolojinin yaygınlaşmasıyla birlikte önemli konular haline gelmiş; araştırmacılar ise bu sorunlara yönelik çözüm önerileri getirmişlerdir.

3.5. Akıllı Kimlik Kartlarının Mahremiyet Perspektifinden Hukuki Analizi

Mahremiyet hakkını ve özel yaşamı hukuki olarak ele alabilmek için, kişilik hakkı, kişisel hak ve özgürlükler gibi terimlerin açıklanması önem taşımaktadır (Yüksel, 2003, s. 187).

"Kişi" kelimesi Latince "persona" kelimesinden ve bu kelime de Roma aktörlerinin sahnede kullandıkları "maskeden" gelmektedir. Modern hukuk sistemlerinde "kişilik hakkı" ve "insan hakları" kavramları, Magna Carta, Virginia Haklar Bildirgesi ve Fransız İnsan ve Vatandaş Hakları Bildirgesi gibi önemli hukuki metinlerde yer alarak insanların doğuştan sahip olduğu haklar ve hürriyetler olarak tanımlanmıştır (Akkurt, 2017, s. 343).

Kişilik hakkı, kişinin kendisiyle ilgili kişisel değerleri üzerinde sahip olduğu mutlak hak olarak ifade edilmektedir. Bu kişisel değerler, insan olmanın yanı sıra toplum içindeki yaşamdan kaynaklanan değerler de içermektedir. Bu değerler arasında hayat, beden bütünlüğü, sağlık, ad, şeref, haysiyet, mesleki ve ekonomik değerler ile vicdan, özgürlük, özel hayat, aile bütünlüğü, kişisel veriler gibi duygusal değerler sayılabilir. Kişisel değerlerin kapsamı geniştir ve kanun koyucu tarafından kesin sınırlarla belirlenmemiştir (Akkurt, 2017). Başlangıçta kişilik hakları olarak değerlendirilen mahremiyet hakkı zaman içerisinde özel bir hak hâline gelmiş ve günümüzde yasalarda ve uluslar arası sözleşmelerde tanınan bir niteliğe kavuşmuştur (Yüksel, 2003, s. 210).

Mahremiyet olarak ifade edebileceğimiz özel yaşam ya da kişilik hakları yasalarca korunan bir hak haline gelmiştir. Örneğin, İnsan Hakları Evrensel Bildirisi'nin 12'nci maddesinde

"Hiç kimse, özel yaşamı, ailesi, konutu ya da yazışması konularında keyfi müdahaleye, onuruna ve adına karşı saldırıya uğrayamaz. Herkesin, bu müdahale ve saldırılara karşı yasa ile korunmaya hakkı vardır."

Yine Avrupa İnsan Hakları Sözleşmesi'nin 8'inci maddesinde

"Herkes özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir." denilmiştir. T.C. Anayasası 17'nci maddesinde

"Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir." ve 20'nci maddesinde ise;

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir." denilmiştir. Bu yasal dayanaklar mahremiyetin ve dolayısı ile kişi haklarının ve özel yaşamın korunmasına yönelik olan hukuki altyapıyı oluşturmaktadır.

3.5.1. Kişisel Verilerin Korunması Bağlamında Akıllı Kimlik Kartları

Kişisel verilerin korunması hakkında ilk olarak 1970 yılında Almanya'nın Hessen eyaletinde bir veri koruma yasası kabul edilmiştir ve bu alandaki ilk resmi kurum olan Veri Güvenlik Ofisi kurulmuştur. Bu tarihten sonra Avrupa Birliği'ne üye ülkeler ve Amerika Birleşik Devletleri (ABD) başta olmak üzere dünya genelinde birçok veri koruma kanunu yürürlüğe girmiştir. Her ülke farklı içerik ve uygulamalarla bu kanunları şekillendirmiştir. Örneğin, Almanya hem federal hem de eyalet bazında çeşitli kanunlar uygulamakta iken 1974'te ABD, kişisel bilgilere erişim ve kontrol hakkını savunan bir kanunu kabul etmiştir. Fransa, Kanada gibi ülkeler de 1970'lerde kendi veri koruma yasalarını çıkarmıştır. Uluslararası düzeyde, 1981'de Avrupa Konseyi kişisel verilerin korunması için bir sözleşme imzalamış ve 1980'de OECD, kişisel verilerin korunmasına yönelik rehber ilkeler yayınlamıştır. Bu çabalar, kişisel verilerin daha etkin şekilde korunmasını amaçlamaktadır (Yüksel-Civelek, 2011, s. 10).

Türkiye'de ise 24 Mart 2016 tarihinde kabul edilen ve 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı "Kişisel Verilerin Korunması Kanunu (KVKK)", kişisel verilerin korunmasını ve bu verileri işleyen kişi ve kuruluşların uyacağı kuralları belirlemektedir. Bu kanun, özel hayatın gizliliğini korumayı amaçlamakta ve kişisel verileri işleyen bireylerin ve kuruluşların hem haklarını hem de sorumluluklarını düzenlemektedir.

Kanunun maddelerinde öne çıkan konular şunlardır (KVKK, 2016):

- ✓ **Aydınlatma Yükümlülüğü:**

Kişisel veriler toplandığı zaman, verileri toplayan kişi ya da kuruluş, veri sahibine verilerin kim tarafından ve hangi amaçla kullanılacağını, nasıl toplandığını ve hukuki sebeplerini açıklamak zorundadır.

- ✓ **Kişisel Haklar:**

Kişiler, kendi verilerinin işlenip işlenmediğini öğrenebilir. İşlenen veriler hakkında bilgi talep edebilir. Verilerin nasıl ve neden işlendiğini, doğru kullanılıp kullanılmadığını sorgulayabilir. Verilerin yurt içi veya dışına aktarıldığı yerleri öğrenebilir. Yanlış veya eksik verilerin düzeltilmesini talep edebilir. Belirli şartlar altında verilerin silinmesini isteyebilir. Veriler üzerinde yapılan işlemlerin ilgili diğer taraflara bildirilmesini

sağlayabilir. Yalnızca otomatik sistemlerle yapılan analizlere itiraz edebilir. Verilerin usulsüz kullanılması sonucu zarara uğradığında tazminat talep edebilir.

- ✓ **Veri Güvenliği Yükümlülüğü:**

Veri sorumluları, verilerin usulsüz kullanımını önlemek için gerekli tüm önlemleri almalı. Veriler başka bir kişi veya kuruluş tarafından işleniyorsa, gerekli güvenlik önlemlerinin alınmasından ortaklaşa sorumludurlar. Kişisel verilerin izinsiz elde edilmesi durumunda, bu durum ilgili kişilere ve gerekli makamlara bildirilmelidir.

Bu yasayla birlikte, kişisel verilerin korunması daha sistematik bir hale getirilmiş olup, veri işleyen kurumlar ve bireyler için belirli standartlar ve yükümlülükler getirilmiştir. Bu kanun çerçevesinde akıllı kimlik kartı üreticilerine de belirli standartlar ve yükümlükler getirilmiş olup, kart hamilleri de kanunda sayılan kişisel haklara sahiptir.

3.5.2. Mahremiyet İhlalleri ve Hukuki Sonuçları

Mahremiyet ihlalleri genellikle bireylerin özgürlüğü, şeref, haysiyet, özel hayat ve haberleşme gizliliği gibi kişisel değerlerine yöneliktir ve bu tür ihlaller hem hukuki hem de cezai sorumluluklara yol açabilmektedir. Kişilik hakkının korunmasında yasama ve yargı organları ile servis sağlayıcılar ve denetim organlarının sorumlulukları olmasına rağmen, en büyük sorumluluk bireylerdedir (Akkurt, 2017, s. 365).

6698 sayılı KVKK çerçevesinde işlenen mahremiyet ihlalleri ve suçlara ilişkin yaptırımlar 5237 sayılı Türk Ceza Kanunu'nun (TCK) 135'ten 140'a kadar olan maddeleri ile belirlenmiştir. Bu kanuna göre:

a) Eğer birisi Kanunun 10'uncu maddesinde belirtilen bilgilendirme yükümlülüğü yerine getirilmezse, 5.000 TL'den 100.000 TL'ye kadar para cezası,
b) Veri güvenliği ile ilgili 12'nci maddedeki yükümlülükleri yerine getirmeyenlere 15.000 TL'den 1.000.000 TL'ye kadar para cezası,
c) Kişisel Verileri Koruma Kurulu'nun 15'inci maddesine göre verdiği kararları uygulamayanlara 25.000 TL'den 1.000.000 TL'ye kadar para cezası,
d) 16'ncı maddedeki Veri Sorumluları Siciline kayıt ve bildirim yükümlülüklerine uymayanlar için de 20.000 TL'den 1.000.000 TL'ye kadar para cezası uygulanabilmektedir.

Bu cezalar hem bireyler hem de özel şirketler için geçerlidir. Kamu kurumları ve kuruluşlarındaki benzer ihlallerde, ilgili personel hakkında disiplin işlemi yapılmakta ve sonuçlar Kişisel Verileri Koruma Kurulu'na bildirilmektedir.

Kişisel Verileri Koruma Kurumu, bu görevleri yerine getirmek üzere kurulmuştur ve bağımsız bir kamu kuruluşudur. Kurum, Cumhurbaşkanı tarafından atanan bir bakan ile ilişkilendirilmiştir. Merkezi Ankara'dadır ve Kurul, kurumun karar organıdır.

Kurumun görevleri kanunda şu şekildedir:

a) Uygulamaları ve mevzuattaki değişiklikleri izlemek, değerlendirmeler yapmak ve önerilerde bulunmak.
b) Gerekli olduğunda kamu kurumları, sivil toplum kuruluşları ve üniversitelerle iş birliği yapmak.
c) Kişisel verilerle ilgili uluslararası gelişmeleri takip etmek ve bu konularda uluslararası kuruluşlarla iş birliği yapmak.
d) Her yıl faaliyet raporunu Cumhurbaşkanlığına ve Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonu'na sunmak.
e) Kanunlarla verilen diğer görevleri yerine getirmek.

3.5.3. Karşılaştırmalı Hukukta Akıllı Kimlik Kartları ve Mahremiyet

Son yıllarda birçok ülkede kişisel verilerin korunması için düzenlemeler yapılmaktadır. Bu düzenlemeler bazı ülkelerde kamu ve özel sektörü kapsarken, bazıları sadece belirli sektörlere odaklanmaktadır. Veri koruma konusunda düzenlemeler yapan bazı ülkelerin mevcut durumu özetlenmiştir.

ABD, AB ile uyumlu bir veri koruma yaklaşımını benimserken, Almanya, Kıta Avrupası hukukuna dahil olup dünyada ilk veri koruma düzenlemesini yapan ülke olarak bu konuda öne çıkmaktadır. İngiltere ise, Anglo-Sakson hukukunu temsil etmesine rağmen, son yıllarda yaşanan önemli veri kayıplarının ardından AB hukukuna yakınsayan veri koruma politikaları geliştirmiştir (Yüksel-Civelek, 2011, s. 80).

3.5.3.1. ABD

ABD'de, veri koruma konusu, sosyal güvenlik numaralarının yaygın kullanımı ve veri bankalarının artmasıyla önem kazanmıştır. ABD, veri koruma yasalarında birleşik bir

yaklaşımdan ziyade, sektöre özel düzenlemeler tercih etmektedir. Örneğin, ülke OECD'nin 1981 tarihli rehber ilkelerine imza atmış olmasına rağmen, bu kuralları tam olarak iç hukukuna uygulamamıştır (Yüksel-Civelek, 2011, s. 81).

ABD'nin veri koruma yasaları, AB yasalarıyla kıyaslandığında daha esnek olduğu için iki bölge arasında anlaşmazlıklar yaşanmaktadır. AB, kişisel verilerin korunmasını temel bir hak olarak görürken, ABD bu konuya daha çok tüketici hakları açısından yaklaşmaktadır (Yüksel-Civelek, 2011).

11 Eylül saldırılarından sonra ABD, terörle mücadele amacıyla ülkeye giriş çıkışları daha kontrollü hale getirmek için yolcu isimleri kaydı gibi tedbirler almıştır. Bu kapsamda, bazı AB ülkeleri ile yapılan anlaşmalarla, ABD'ye seyahat eden AB vatandaşlarının kişisel verileri ABD makamlarına iletilmektedir. Bu veriler, bazı kişilerin ABD'ye girişlerinin reddedilmesine neden olabilecek şekilde 15 yıl süreyle saklanabilmektedir (Yüksel-Civelek, 2011).

Sonuç olarak, ABD'nin veri koruma yaklaşımı ve terörle mücadele çerçevesinde aldığı tedbirler hem AB ile ilişkilerde hem de kendi içinde çeşitli tartışmalara yol açmıştır.

3.5.3.2. Almanya

Almanya, dünyada ilk veri koruma yasasını 1970 yılında Hessen eyaletinde çıkarmıştır. Ancak, ülkedeki genel veri koruma yasalarının oluşturulması ve uygulanması zaman almış ve sonunda 2001'de tamamlanabilmiştir. Almanya'da federal düzeyde bir Veri Koruma Yasası bulunmakla birlikte, her eyaletin kendi düzenlemeleri ve uygulamaları da mevcuttur. Ayrıca, Federal Veri Koruma Komiseri dışında, Berlin ve Bavyera gibi eyaletlerde de veri koruma ile ilgili kurumlar bulunmaktadır. Alman Anayasa Mahkemesi, kişisel verilerin korunması konusunda önemli kararlar almıştır. Bu kararlar, kişisel verilerin temel haklar olarak korunması gerektiğini ve bu hakların sadece kamu yararı veya yasal gerekliliklerle ihlal edilebileceğini vurgulamaktadır (Yüksel-Civelek, 2011, s. 87).

3.5.3.3. İngiltere

İngiltere'de veri koruma yasaları, 1984'te ilk kez uygulamaya konulmuştur. Ancak bu yasada bireylerin mahremiyet haklarına ilişkin net hükümler olmadığı için 1998'de

çıkarılan yeni bir yasa ile kişisel verilerin korunması daha önemli hale getirilmiştir. Bu yasa ile, kişisel verilerin nasıl işleneceği ve kullanılabileceği belirlenmiş ve özellikli verilerin kullanımı için daha sıkı kurallar getirilmiştir.

Bu yasaya göre, veri kontrolörleri yedi temel ilkeye uymak zorundadır:

1. Adil ve hukuka uygun işleme
2. Belirlenmiş amaçlar için işleme
3. Amaca uygun, orantılı ve ilgili verileri tutma
4. Gereğinden fazla süre saklamama
5. Kişi haklarına zarar vermeyecek şekilde kullanma
6. Güvenli ortamlarda tutma
7. Yeterli koruma düzeyinin olmadığı ülkelere transfer etmeme.

İngiltere'de veri koruma konusunda Adalet Bakanlığı'nın himayesinde Bilgi Komiseri Ofisi görev yapmaktadır. Komiser, verilerin korunmasını desteklerken, vatandaşlara bilgi verme, eğitimler düzenleme ve hak ihlallerini inceleme gibi görevleri yerine getirmektedir (Yüksel-Civelek, 2011, s. 88)

3.6. Akıllı Kimlik Kartları ve Güvenlik

Akıllı kimlik kartları, taşınabilirlik ve yüksek güvenlik sağlayarak önemli avantajlar sunmaktadır. Kişisel kimlik bilgileri güvenli bir şekilde kartta saklanmakta ve kopyalanamamaktadır. Diğer kredi kartları gibi kartların manyetik şeritleri kopyalanabilirken, akıllı kimlik kartları bu riski ortadan kaldırmaktadır (Şanslı, 2007, s. 22).

Mahremiyet artırıcı teknolojiler, mahremiyet kanunlarının uygulanmasına yardımcı olmayı ve kişisel verilerin toplanması ile ilgili riskleri azaltmayı amaçlamaktadır. Bu teknolojiler, kullanıcılara çevrimiçi ortamda verilerinin kontrolünü sağlamakta, izleme teknolojilerini filtreleme, veri şifreleme gibi yöntemlerle verilerin güvenliğini artırmaktadır (Yüksel-Civelek, 2011, s. 51). Bu çerçevede, akıllı kimlik kartları da mahremiyet artırıcı teknolojilerin bir örneğidir. Çünkü kişisel bilgilerin güvenli bir şekilde depolanmasını sağlamakta ve kopyalanmalarını önlemektedir. Böylece kullanıcıların mahremiyeti korunmuş olmaktadır.

3.6.1. Sistemin Güvenlik Özellikleri

Akıllı kartlar, modern şifreleme tekniklerini barındırarak birçok güvenlik prosedürünü destekleyecek kapasitededir. Bu kartlar, özellikle Özel ve Genel Anahtarın bir arada kullanıldığı asimetrik şifreleme yani Genel Anahtar Altyapısı Şifrelemesini aktif olarak kullanmaktadır (Djalal, 2019, s. 7). Buna rağmen, kartlara yüklenen yazılımlar sebebiyle güvenlik açıkları ortaya çıkabilmekte, bu da verilerin bozulması veya çalınması gibi risklere neden olabilmektedir (Ceyhan vd., 2018, s. 746).

Haziran 1998'de Kocher ve ekibi, akıllı kart mikroişlemcilerine yönelik bir saldırı tespit etmiştir. Bu saldırı türünde, bir akıllı kartın güç tüketimi izlenerek, kartın içinde bulunan kriptografik algoritmanın gizli anahtarının çıkarılabileceği ortaya çıkmıştır. Akıllı kart teknolojilerindeki bu güvenlik açıkları, sürekli olarak yeni ve daha güvenilir güvenlik önlemlerinin geliştirilmesine yol açmıştır (Messerges vd., 2002, s. 541).

DPA (Differential Power Analysis-Farklılık Güç Analizi), akıllı kartlar, RFID (Radio Frequency Identification- Radyo Frekansı Tanımlama) cihazları ve diğer güvenlik önlemlerindeki zayıf noktaları belirlemede kullanılan bir kriptoanaliz yöntemidir. Günümüzde bu yöntemi engellemek amacıyla bilimsel çalışmalar yapılmakta ve çeşitli yöntemler sunulmaktadır. Bu araştırmaların sonuçları, belirtilen yöntemlerin mükemmel güvenlik sağladığını göstermiştir (Tiri ve Verbauwhede, 2003, ss. 135-136). Akıllı kimlik kartları, akıllı kartların bir alt kümesi olarak kabul edilmekte ve bu güvenlik önlemlerinden faydalanmaktadır.

- ✓ **Erişim Kontrol Mekanizmaları**

Kişiye tahsis edilen kimlik kartları sadece o kişiye özel veriler içermektedir. Akıllı kimlik kartı hamili şifre bilgilerini kanıtladığında hizmet verici tarafından ilgili kişinin bilgilerine erişilebilir. Bu özellik sayesinde başkasının kimlik kartıyla hizmet gördürmenin önüne de geçilmiş olunacaktır.

- ✓ **Kimlik Doğrulama Yöntemleri (Benzersiz Tanımlama)**

Bu özellik sayesinde veri tabanında kayıtlı bilgilerin taranmasını etki alanı doğrulama tanımlayıcılarını kullanarak önler. Böylelikle kişiye ait veriler yanlış beyan edilemez.

- ✓ **Veri Erişim Kontrolü (Seçici Açıklama)**

Hizmet gördürme esnasında kişiye ait bilgilerle alakalı yalnızca belirli bilgilere erişilebilir. Örneğin, bankacılık işlemlerinde kişinin adres teyidi yapılmak istendiğinde kart okuyucunun sadece adres okuyucu bilgilerini alması gerekir. Yine kişi hastane işlemlerinde kart okuyucu kişinin sadece sağlıkla ilgili verilerini sunması gerekir.

- ✓ **Güvenlik Modları ve Fonksiyonlar (Yalnızca Doğrulama Modu)**

Bu uygulama ile kimlik kartındaki veriler daha güvenli hale getirilir. Kimlik kartındaki verilerle zıt olarak çalışan ve kartın yalnızca belirli bir veri aralığında seçilen alanların eşleşmesine izin veren sorgulama motoru bulunmaktadır. Örneğin kişinin doğum tarihi bilgilerini vermek yerine 15 yaşından büyük ya da küçük olduğu sorgusuna evet ya da hayır cevabı şeklinde yanıt oluşturur.

- ✓ **Biyometrik Güvenlik Özellikleri**

Bu uygulama kimlik kartlarının kaybolması ya da çalınması durumunda oluşacak risklerin azaltılması için getirilmiştir. Veri tabanında saklanan, kişinin biyometrik verilerine erişebilen biyometrik şablonlar sayesinde yüksek düzeyde koruma sağlar.

- ✓ **Kullanıcı Deneyimi ve Kullanılabilirlik**

Kişiye ait bütün bilgilerin merkezde toplanması verilere kolay ulaşılabilmesi akıllı kimlik kartlarının daha fazla kullanılabilir olmasına olanak sağlamıştır.

Akıllı kimlik kartları kişi hakkında parmak izi, retina taramaları gibi biyometrik verilerde dahil olmak üzere bilgileri depolayan ve bunlara erişen bir mikroçip içeren kartlardır. Vatandaştan uçağa binerken veya güvenlik güçleri tarafından durdurulup kimlik kontrolü yapılırken karttaki bilgiler kişi ile karşılaştırıldığında, örneğin karta kaydedilmiş parmak iziyle canlı parmak izi taraması karşılaştırıldığında doğrulama gerçekleşir. Bir eşleşme varsa, taramanın yerini ve zamanını kaydetmek ve dosyaya kart sahibi hakkında şüphe uyandıran herhangi bir şey olup olmadığını belirlemek için kart veri tabanına bağlanır. Böylelikle kimlik kartı güvenlik kontrolleri tamamlanmış ve kısa zamanda doğru verilerle kişi bilgilerine ulaşılarak iş süreçlerin tamamlanma süreside kısaltılmış olmaktadır (Hiltz vd., 2003).

3.6.2. Akıllı Kimlik Kartlarında Güvenlik İle İlgili Endişeler

Akıllı kartlardaki güvenlik açıklarından kaynaklanan sorunlar genellikle yargıya taşınmaktadır. Bu sorun, tüm vatandaşlara ait bilgilerin tek bir merkezi biyometrik veri tabanında tutulmasından kaynaklanmaktadır (Ceyhan vd., 2018, s. 747).

Akıllı kimlik kartlarında güvenlik ile ilgili endişeler kimlik kartının kaybedilmesi, çalınması, yetkisiz erişim riski, veri sızıntısı tehlikesi ve kartın fiziksel olarak kopyalanması ve sahtecilik durumlarında ortaya çıkmaktadır.

3.6.2.1. Kart Kaybı ve Çalınması Durumu

Türkiye Cumhuriyeti Kimlik Kartı Yönetmeliğinin 19'uncu Maddesi'nde belirtilen hükme göre, kimlik kartı sahipleri kartlarını kaybettiklerinde bu durumu yurt içinde çağrı merkezine veya nüfus müdürlüklerine, yurt dışında ise en yakın dış temsilciliğe bildirmek zorundadır. Kayıp kart bildirimi e-devlet kapısı üzerinden veya yurt içinde Alo 199 numaralı çağrı merkezini arayarak yapılabilmektedir. Ardından, yurt içinde nüfus müdürlüklerine veya yurt dışında dış temsilciliklere başvurularak yeni kimlik kartı talep edilmelidir. Bu bildirimlerin veya başvuruların sonucunda kayıp kimlik kartı geçersiz hale gelmektedir (NVGM, 2024c).

Bu hükümden anlaşıldığı üzere kartın kaybolması ve çalınması durumunda kart hamilinin yeni kart başvurusunda bulunması ve kartın geçersiz hale getirilmesini talep etmesi gerekmektedir.

3.6.2.2. Yetkisiz Erişim Riskleri

Akıllı kimlik kartlarında bulunan biyometrik verilerin özel uygulamalarda kullanılması, hukuki açıdan potansiyel bir sorun oluşturabilmektedir. Kimlik kontrolünü gerçekleştiren kişi sayısının artmasıyla, yetkisiz kişilerin vatandaşların kimlik kartı kullanımını izlemesi ve ifşa etmesi gibi durumlar kişisel verilerin gizliliğini ihlal edebilecektir. Bu durum hem hukuki hem de etik sorunlara yol açabilecektir. Çünkü bir kez kişinin verilerine erişim hakkı kazanan biri, kişi hakkında detaylı bilgilere ulaşabilecek ve bu durum kişi için sorun oluşturabilecektir. Ancak, zorunlu durumlarda böyle bir seçim yapılması gerektiğinde, kullanıcıya karar verme fırsatı verilmesinin daha uygun olacağı düşünülmektedir (Ceyhan vd., 2018, s. 750; TÜBİTAK-UEKAE, 2006).

3.6.2.3. Veri Sızıntısı Tehlikesi

Veri sızıntıları teknolojik ürünlerde önemli bir güvenlik açığı oluşturmaktadır. Bu güvenlik açığına neden olan şirketler yüksek tazminat ödemek durumunda kalmaktadır. Örneğin, Facebook, dünyanın en popüler sosyal medya platformlarından biri olarak bilinmektedir ve 2018 yılında kullanıcı verilerini İngiliz şirket Cambridge Analytica'ya satmasıyla dünya çapında büyük bir veri ihlali skandalına neden olmuştur. Son olarak, Meta adı altında faaliyet gösteren şirket, kullanıcıların kişisel bilgilerine izinsiz erişim sağlandığı iddiasıyla açılan toplu davanın sona erdirilmesi için 725 milyon dolarlık bir anlaşma yapmayı kabul etmiştir (Ensonhaber, 2022b).

Amerika merkezli bir mikro çip üreticisi firma Advanced Micro Devices (AMD), büyük bir veri sızıntısıyla karşı karşıya kalmış ve şirket içindeki önemli bilgileri siber saldırganlara kaptırmıştır. Şirket, bazı gruplara 450 GB veri sızıntısı olduğu haberlerini aldıklarını ve olayı araştırdıklarını açıklamıştır (Ensonhaber, 2022a).

Başka bir örnek vermek gerekirse bir bilgisayar korsanı, Şanghay polis veri tabanında depolanan 1 milyar Çin vatandaşının kişisel bilgilerini çaldığını iddia etmiştir. Korsan, Breach Forums'ta 23 terabayttan fazla veriyi 10 Bitcoin karşılığında satmayı teklif etmiştir. Çin'de 2016 yılında Alibaba'nın kurucusu Jack Ma da dahil olmak üzere önde gelen Çinli kişiler hakkındaki özel bilgilerin Twitter'da yayınlanması üzerine yetkililer harekete geçmiş ve veri sızıntısının önlenmesi amaçlı yeni yasalar çıkarılmıştır (Türkiye, 2022).

Hassas veriler, sağlık, finans, bankacılık gibi birçok alanda kullanılan ve korunması gereken verilerdir. Bu veriler, iş gizliliği, veri gizliliği, hukuki yükümlülükler gibi konularda önem arz etmektedir. Örneğin, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası, Gramm–Leach–Bliley Yasası, BASEL II ve Sarbanes-Oxley Yasası gibi yasalar ve standartlar bu verilerin güvenliğini sağlamaya yöneliktir. Bu nedenle, bu verilerin sızıntılara karşı korunması gereklidir. Bu verilerin kanuni olmayan yollarla başkaları tarafından ele geçirilmesine veri sızıntısı veya ihlali denilmektedir (Paşaoğlu vd., 2019, s. 81). Bir başka ifade ile veri sızıntısı, bilgi güvenliği alanında bilgilerin istenmeyen şekilde ifşa edilmesini ifade etmektedir. Bu sorunu azaltmak için kullanılan veri kaybı önleme sistemleri, belirli kurallarla verilerin izinsiz ifşa edilmesini engellemektedir. Bu

sistemler, verilerin içeriğini ve bağlamını analiz etmekte, farklı durumlardaki verileri çeşitli önleyici eylemlerle korumaktadır. Geleneksel güvenlik kontrollerinden farklı olarak, bu sistemler daha proaktiftir ve verilerin içeriğine odaklanmaktadır. İçerik tabanlı veri sızıntısı önleme sistemleri (Data Leak Prevention Systems-DLPS), düzenli ifadeler, veri parmak izleri ve istatistiksel analiz gibi yöntemlerle çalışmaktadır. Ancak bu sistemlerin bazı zorlukları vardır, örneğin yüksek yanlış pozitif oranlar ve veri parmak izlerinin değişime açık olması gibi. Bu nedenle, DLPS'lerin veri sızıntısıyla mücadelede önemli bir rolü vardır ancak kesin çözüm değildir (Alneyadi vd., 2016). Akıllı kimlik kartları ile ilgili veri sızıntısını önlemek amaçlı bilimsel çalışmalar yapılmakta ve yeni önlemler geliştirilmektedir.

3.6.2.4. Kartın Fiziksel Kopyalanması ve Sahtecilik

Akıllı kartlar, içerdikleri mikroçipler sayesinde bilgilerin kopyalanmasını önlemektedir. Manyetik şeritli kredi kartlarında olduğu gibi, akıllı kimlik kartı bilgilerinin kopyalanması mümkün değildir (Şanslı, 2007, s. 22). Bir başka ifade ile akıllı kartlar veya çip kartlar, kredi kartları gibi manyetik şeritler yerine entegre bir mikroçip kullanmaktadır. Bu mikroçipler, kart üzerindeki bilgileri korumak ve güvenliği artırmak için tasarlanmıştır. Kredi kartlarındaki manyetik şeritler, üzerlerindeki bilgilerin basitçe kopyalanmasına olanak tanırken, akıllı kartlardaki mikroçipler, daha karmaşık bir yapıya sahiptir ve kopyalanmaları mümkün değildir. Ayrıca, birçok akıllı kart, kullanıcı tarafından bir pin ile korunmaktadır. Kart sahibi pini girmezse, çipin içindeki bilgilere erişmek mümkün olmamaktadır.

Bu özellikler, akıllı kimlik kartlarının kopyalanmasını önlemektedir. Dolayısıyla güvenlik seviyesini artırmaktadır.

4. BÖLÜM: BULGULAR

Veri toplama sürecinde, araştırmacılar tarafından özel olarak geliştirilen ve literatür taraması sonucunda oluşturulan yarı yapılandırılmış görüşme formu kullanılmıştır. Görüşme formu, katılımcılara yöneltilen açık uçlu sorulardan oluşmaktadır. 2024 yılında Karaman il merkezinde yaşayan 30 yetişkin bireyle yüz yüze yapılan görüşmeler, katılımcıların akıllı kimlik kartlarıyla ilgili mahremiyet ve güvenlik konularındaki görüşlerini derinlemesine anlamak amacıyla yapılan 15 soruluk mülakatlar şeklinde gerçekleştirilmiştir.

Kişisel bilgilere ilişkin güvenlik ve gizlilik nedeniyle katılımcılar K1, K2, K3,... K30 olarak kodlanmıştır. Aşağıda katılımcıların açık uçlu sorulara verdikleri yanıtlar özetlenmiş ve öne çıkan konular vurgulanmıştır.

4.1. Demografik Bilgiler

Mülakat görüşmelerine katılan yetişkin 30 bireyin demografik bilgilerine ilişkin bilgilere Tablo 2'de yer verilmiştir.

Tablo 2. Katılımcıların Demografik Bilgileri

Katılımcıların Demografik Özellikleri	**f**	**(%)**
Cinsiyet		
1 Kadın	15	50,0
2 Erkek	15	50,0
Toplam	**30**	**100**
Medeni Durum		
1 Evli	6	20,0
2 Bekar	24	80,0
Toplam	**30**	**100**
Çalışma Şekliniz		
1 Özel Sektör	20	66,7
2 Kamu Sektörü	7	23,3
3 Çalışmıyorum-Emekli	3	10,0
Toplam	**30**	**100**
Yaş		
18-25	5	16,7
26-33	5	16,7
34-41	4	13,3

42 ve üzeri	16	53,3
Toplam	**30**	**100**
Eğitim Durumu		
İlköğretim	3	10,0
Lise	10	33,3
Ön Lisans	2	6,7
Lisans	12	40,0
Yüksek Lisans	2	6,7
Doktora	1	3,3
Toplam	**30**	**100**
Mesleki Kıdem Bilgisi		
1-5 Yıl	8	26,7
6-10 Yıl	4	13,3
11-15 Yıl	4	13,3
16-20 Yıl	2	6,7
21-25 Yıl	4	13,3
26 ve üzeri	8	26,7
Toplam	**30**	**100**

Tablo 2'ye göre katılımcıların demografik özelliklerini değerlendirdiğimizde, çalışmaya katılan 30 kişinin cinsiyet dağılımının eşit bir şekilde dağıldığı gözükmektedir (%50 kadın, %50 erkek). Medeni durumları incelendiğinde, katılımcıların %80'i bekar, %20'si ise evlidir. Çalışma şekline göre çoğunluk (%66,7) özel sektörde çalışmaktadır, bunu %23,3 ile kamu sektörü takip etmektedir. Çalışmayan veya emekli olan katılımcıların oranı %10 olarak tespit edilmiştir.

Yaş dağılımı incelendiğinde, katılımcıların çoğunluğu (%53,3) 42 yaş ve üzerinde olduğu görülmektedir. Diğer yaş grupları ise %16,7 ile 18-25 ve 26-33 yaş aralıklarında, %13,3 ile 34-41 yaş aralığındadır.

Eğitim durumlarına göre, katılımcıların %40'ı lisans, %33,3'ü lise mezunu ve %10'u ilköğretim düzeyinde eğitim almıştır. Ön lisans ve yüksek lisans mezunlarının oranı ise sırasıyla %6,7'dir.

Mesleki kıdemlerine göre katılımcıların %26,7'si (8 kişi) 1-5 yıl ve %26,7'si (8 kişi) 26 yıl ve üzeri kıdeme sahiptir. Bu gruplar en büyük iki kategoriyi oluşturmaktadır. Orta kıdemde yer alan katılımcılar, 6-10 yıl, 11-15 yıl ve 21-25 yıl kategorilerinde eşit sayıda olup, her biri %13,3'lük (4 kişi) bir orana sahiptir. En az katılımcıya sahip kıdem grubu ise %6,7 (2 kişi) ile 16-20 yıl kıdemdeki çalışanlardır. Bu dağılım, çalışmaya katılanların

mesleki kıdem açısından geniş bir yelpazeye yayıldığını ve farklı deneyim seviyelerini temsil ettiğini göstermektedir

Bu demografik veriler, çalışmanın çeşitli yaş gruplarından ve eğitim düzeylerinden katılımcılarla yapıldığını göstermektedir. Ayrıca, çalışma katılımcılarının çoğunluğunun özel sektörde çalışan, bekar ve 42 yaş üzerindeki bireylerden oluştuğunu ortaya koymaktadır.

Tablo 2'de yer alan demografik bilgilerin, akıllı kimlik kartlarının güvenlik, mahremiyet ve kullanılabilirlik gibi konularında politika yapıcılar ve ilgili kurumlar için yol gösterici olabileceği düşünülmektedir. Ayrıca bu demografik özelliklerin, bu kartların tasarımı, dağıtımı ve kullanımı üzerinde nasıl bir etkiye sahip olabileceğini anlamak, daha etkili çözümler geliştirmek için önemli bir adım olduğunu vurgulamak gerekir.

4.2. Katılımcı Yanıtları

Tablo 3'te katılımcı görüşlerinin araştırma hipotezleri bağlamında detay bir değerlendirmesi yer almaktadır. Katılımcılar ile yapılan mülakat görüşme notları ise aşağıda özetlenmiştir

Tablo 3. Katılımcı Görüşlerine İlişkin Tablo

Katılımcılar	**Mahremiyet Düzeyi Farkındalığı**	**Mahremiyet ve Güvenlik İlişkisi**	**Kullanım ve Mahremiyet Endişeleri İlişkisi**	**Yasal Düzenlemelere Güvenilirlik ve Mahremiyet Algısı İlişkisi**
K1	Kişisel verilerin korunması konusundaki farkındalığının yetersiz olduğunu belirtmiştir.	Kişisel verilerin korunması konusunda yeterince bilinçli olmadığını ve mevcut güvenlik önlemlerini yetersiz bulduğunu belirtmiştir.	Bu teknolojiyi nadiren kullandığını ve mevcut akıllı kimlik kartları sisteminin zaaflar içerdiğine inandığını belirtmiştir.	Resmi bilgilendirmelerin ve güvenlik önlemlerinin yetersiz olduğunu düşündüğünden yasal düzenlemelere olan güveninin düşük olduğunu belirtmiştir.
K2	Kişisel verilerin korunması konusunda endişeler taşımakta ve daha güçlü şifreleme tekniklerinin kullanılmasını önermektedir. Bu durum, yüksek düzeyde farkındalık	Güvenlik önlemlerini yetersiz bulmakta ve kişisel verilerin korunması konusunda endişeler taşımaktadır.	Kartların güvenliği ve mahremiyeti konusundaki endişeleri, kartları kullanma ve benimseme konusunda olumsuz bir etki yaratmaktadır.	Daha sıkı denetimlerin yapılması gerektiğini ve mevcut güvenlik önlemlerini yetersiz bulduğunu ifade etmiştir. Bu bulgu, yasal düzenlemelere güvenin düşük olduğunu göstermektedir.

	gösterdiğini ifade etmektedir.			
K3	Kişisel verilerin korunması ve izinsiz erişimden kaygılı olduğunu belirtmiş ve mevcut güvenlik önlemlerinin yetersiz olduğunu ifade etmiştir. Bu bulgu, yüksek düzeyde farkındalık göstermektedir.	Kişisel verilerin korunması konusunda endişeleri olduğunu ve mevcut güvenlik önlemlerini yetersiz bulduğunu belirtmiştir. Bu bulgu, kişisel verilerin güvenliğine dair endişelerin yüksek olduğunu göstermektedir.	Akıllı kimlik kartlarına dair ciddi endişeler taşıdığını belirtmiş ve mevcut güvenlik önlemlerini yetersiz bulduğunu ifade etmiştir. Bu bulgu, kartları kullanma ve benimseme düzeyinin düşük olduğunu göstermektedir.	Resmi kurumlar tarafından yeterli bilgilendirme yapılmadığını ve daha sıkı güvenlik önlemlerinin alınması gerektiğini belirtmiştir. Bu bulgu, yasal düzenlemelere güvenin düşük olduğunu göstermektedir.
K4	Kişisel bilgilerin korunmasında yeterli güvenlik önlemlerinin alınmadığını düşünmekte ve kişisel verilere yetkisiz erişim konusunda ciddi kaygılar taşımaktadır. Bu bulgu, yüksek düzeyde farkındalık göstermektedir.	Kişisel verilerin korunmasında yeterli güvenlik önlemlerinin alınmadığını ve ciddi kaygılar taşıdığını belirtmiştir. Bu bulgu, kişisel verilerin güvenliğine dair endişelerin yüksek olduğunu göstermektedir.	Akıllı kimlik kartlarının güvenlik önlemlerinin yetersiz olduğunu düşündüğü için mahremiyet endişeleri taşıdığını belirtmiş, ancak kartların günlük yaşamda çok sık kullanıldığına da vurgu yapmıştır. Bu durumda katılımcı, endişelerine rağmen kartları kullanmak zorunda kalmaktadır.	Resmi bilgilendirme eksikliği ve şeffaflık konusunda eleştirilerde bulunmuştur. Bu bulgu, yasal düzenlemelere güvenin düşük olduğunu göstermektedir.
K5	Kişisel verilerin korunması konusunda bilinçli olduğunu ve güvenlik önlemlerini yeterli bulduğunu belirtmiştir. Bu bulgu, yüksek düzeyde farkındalık göstermektedir	Kişisel verilerin korunması konusunda bilinçli olduğunu ve güvenlik önlemlerini yeterli bulduğunu ifade etmiştir. Bu bulgu, kişisel verilerin güvenliğine dair endişelerin düşük olduğunu göstermektedir.	Akıllı kimlik kartlarının pratikliğini ve zaman tasarrufunu vurgulayarak, kartı kullanma ve benimseme düzeyinin yüksek olduğunu belirtmiştir. Mahremiyet endişeleri olmasına rağmen, kartın sunduğu faydaların kendisi için daha önemli olduğunu ifade etmiştir	Resmi bilgilendirmenin yetersiz olduğunu belirtmiş, ancak genel olarak akıllı kimlik kartlarının güvenilir olduğunu düşündüğünü ifade etmiştir. Bu bulgu, yasal düzenlemelere güvenin kısmen yüksek olduğunu ve bu nedenle mahremiyet algısının olumlu olduğunu göstermektedir.

K6	Kişisel verilerin korunması konusunda bilgi sahibi olmadığını ve güvenlik önlemlerinin yetersiz olduğunu düşündüğünü belirtmiştir. Bu bulgu, düşük düzeyde farkındalık göstermektedir.	Güvenlik önlemlerinin yetersiz olduğunu ve ciddi güvenlik endişeleri taşıdığını ifade etmiştir. Bu bulgu, kişisel verilerin güvenliğine dair endişelerin yüksek olduğunu göstermektedir.	Günlük hayatta akıllı kimlik kartlarını sıklıkla kullanmadığını, ancak resmi işlemler gerektiğinde kullandığını belirtmiştir. Bu bulgu, mahremiyet endişeleri nedeniyle kullanma ve benimseme düzeyinin düşük olduğunu göstermektedir.	Resmi bilgilendirme yapılmadığını ve güvenlik önlemlerinin yetersiz olduğunu belirtmiştir. Bu bulgu, yasal düzenlemelere güvenin düşük olduğunu göstermektedir.
K7	Kişisel verilerin güvende olmadığını düşündüğünü belirtmiştir. Bu bulgu, kişisel verilerin korunmasına ilişkin farkındalığın yüksek olduğunu göstermektedir.	Çip sisteminin güvenlik açığı olduğundan ve bilgi sızıntısına yol açabileceğinden endişe duymaktadır. Bu bulgu, kişisel verilerin güvenliğine dair endişelerin yüksek olduğunu göstermektedir.	Akıllı kimlik kartlarının eski versiyonlarının daha güvenli olduğunu düşünmekte ve mevcut çip sistemine güvenmediği için kartı kullanma ve benimseme düzeyinin düşük olduğunu belirtmektedir	Resmi bilgilendirme yapılmadığını ve güvenlik açığı olduğuna inandığını belirtmiştir. Bu bulgu, yasal düzenlemelere güvenin düşük olduğunu göstermektedir.
K8	Kişisel verilerinin güvende olmadığını düşünmekte ve çip sisteminin güvenli olmadığını belirtmektedir. Bu bulgu, mahremiyet meselelerinde farkındalığın yüksek olduğunu göstermektedir.	Çip sisteminin güvenli olmadığını ve kişisel verilerin çalınması veya kaybolması durumunda ciddi güvenlik sorunları yaşanabileceğini belirtmektedir. Bu bulgu, kişisel verilerin güvenliğine dair endişelerin yüksek olduğunu göstermektedir.	Kimlik kartını hastane gibi belirli işlemler için kullandığını ancak genel kullanımda sınırlı olduğunu ifade etmiştir. Bu bulgu, mahremiyet endişeleri nedeniyle kartın kullanım ve benimseme düzeyinin düşük olduğunu göstermektedir.	Herhangi bir resmi bilgilendirme yapılmadığını ve güvenlik önlemlerinin yetersiz olduğunu belirtmiştir. Bu bulgu, yasal düzenlemelere güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.
K9	Kişisel verilerinin güvende olmadığını ve mahremiyetle ilgili endişeleri olduğunu belirtmiştir. Bu bulgu, mahremiyet meselelerinde farkındalığın yüksek olduğunu göstermektedir	Kişisel verilerin güvende olmadığını ve güvenlik önlemlerinin yetersiz olduğunu düşündüğünü belirtmiştir. Bu bulgu, kişisel verilerin güvenliğine dair endişelerin yüksek olduğunu göstermektedir	Kimlik kartlarını genellikle resmi işlemler için kullanmakta ve genel olarak güvenlik önlemlerinin yetersiz olduğunu düşünmektedir. Mahremiyet endişeleri yüksek olduğundan, kullanım ve benimseme düzeyinin daha düşük olduğu anlaşılmaktadır.	Herhangi bir resmi bilgilendirme yapılmadığını belirtmiş ve kişisel verilerin güvende olmadığını ifade etmiştir. Bu bulgu, yasal düzenlemelere güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.

K10	Kişisel verilerin korunması konusunda bilinçli olmadığını ve güvenlik önlemlerini yetersiz bulduğunu belirtmiştir. Bu bulgu, düşük düzeyde farkındalığa işaret etmektedir.	Kişisel verilerin güvende olmadığını ve güvenlik önlemlerinin yetersiz olduğunu düşünmektedir. Bu bulgu, güvenlik endişelerinin yüksek olduğunu göstermektedir	Ehliyet bilgilerini taşıdığı için kimlik kartını sıkça kullandığını ancak kişisel verilerin güvenliği konusunda endişeleri olduğunu belirtmiştir. Bu durumda, kullanım ve benimseme düzeyi yüksektir.	Herhangi bir resmi bilgilendirme olmadığını ve güvenlik önlemlerinin arttırılması gerektiğini düşünmektedir. Bu bulgu, yasal düzenlemelere güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.
K11	Kişisel verilerinin korunması konusunda bilinçli olmadığını ve güvenlik önlemlerini yetersiz bulduğunu belirtmiştir. Bu bulgu, düşük düzeyde farkındalık göstermektedir.	Kişisel verilerinin güvende olmadığını ve izinsiz erişim riski bulunduğunu düşündüğü için güvenlik endişeleri yüksektir.	Akıllı kimlik kartlarının işlevselliğini ve kolaylığını vurgulamış ancak güvenlik endişeleri taşıdığını belirtmiştir.	Resmi bir bilgilendirme olmadığını ve güvenlik önlemlerinin artırılması gerektiğini ifade etmiştir. Bu bulgu, yasal düzenlemelere güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.
K12	Kişisel verilerinin korunması konusunda bilinçli olmadığını ve bu konuda bilgilendirme yapılmadığını belirtmiştir. Bu bulgu, düşük düzeyde farkındalık göstermektedir.	Güvenlik önlemlerini yetersiz bulduğunu ve kartın kaybolması durumunda ciddi sorunlar yaşanabileceğini vurgulamıştır. Bu durum, yüksek düzeyde güvenlik endişelerine işaret etmektedir.	Kimlik kartını sadece resmi ve banka işlemlerinde kullanmak dışında gerekli görmediğini belirtmiştir. Bu, kartın kullanımı ve benimsenmesiyle ilgili düşük bir düzeyi göstermektedir	Kimlik fotokopisinin her kurum tarafından istenmesinin endişe verici olduğunu vurgulamış ve resmi bir bilgilendirme olmadığını belirtmiştir. Bu bulgu, yasal düzenlemelere güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.
K13	Kişisel verilerinin korunması konusunda bilinçli olmadığını ve yeterli bilgilendirme yapılmadığını belirtmiştir. Bu bulgu, düşük düzeyde farkındalık göstermektedir.	Güvenlik önlemlerini yetersiz bulduğunu ve kartın kaybolması veya çalınması durumunda ciddi sorunlar yaşanabileceğini düşündüğünü ifade etmiştir. Bu bulgu, yüksek düzeyde güvenlik endişelerine işaret etmektedir.	Kimlik kartını genellikle resmi ve banka işlemlerinde kullandığını ancak gerekli olmadığı durumlar için kullanmadığını belirtmiştir. Bu bulgu, düşük bir benimsenme düzeyini göstermektedir.	Türkiye'nin akıllı kimlik kartları konusunda hazır olmadığını düşündüğünü ve daha güvenli bir sistemin olması gerektiğini ifade etmiştir. Bu bulgu, yasal düzenlemelere olan güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.

K14	Kişisel verilerinin korunması konusunda bilinçli olmadığını ve yeterli bilgilendirme yapılmadığını belirtmiştir. Bu bulgu, düşük düzeyde farkındalık göstermektedir	Güvenlik önlemlerini yetersiz bulduğunu ve kartın kaybolması veya çalınması durumunda ciddi sorunlar yaşanabileceğini düşündüğünü ifade etmiştir. Bu bulgu, yüksek düzeyde güvenlik endişelerine işaret etmektedir	Kartı, genellikle resmi dairelerde ve bankalarda kullanmakta ancak geçerlilik tarihini yük olarak gördüğünü belirtmiştir. Bu bulgu, düşük bir benimsenme düzeyini göstermektedir	Kart okuyucu sistemlerinin faaliyete geçirilmesi, şifreleme yöntemlerinin kullanılması ve kart sahibinin onayıyla erişim sağlanması gerektiğini belirtmiştir. Bu bulgu, yasal düzenlemelere olan güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.
K15	Kişisel verilerinin korunması konusunda bilinçli olmadığını ve herhangi bir bilgilendirme yapılmadığını belirtmiştir. Bu bulgu, düşük düzeyde farkındalık göstermektedir.	Güvenlik önlemlerini etkisiz bulduğunu ve kartının kaybolması veya çalınması durumunda ciddi sorunlar yaşanabileceğini düşündüğünü ifade etmiştir. Bu bulgu, yüksek düzeyde güvenlik endişelerine işaret etmektedir.	Kartı, günlük yaşamında sıkça kullanmasa da resmi dairelerde ve bankalarda kullandığını belirtmiştir. Bu bulgu, orta düzeyde bir benimsenme düzeyini göstermektedir.	Mahremiyetle ilgili endişelerin azaltılması için bilgilendirme kampanyaları yapılması gerektiğini ifade etmiştir. Bu bulgu, yasal düzenlemelere olan güvenin düşük ve mahremiyet algısının olumsuz olduğunu gösterir.
K16	Mahremiyetin korunması konusunda endişeleri olduğunu ve mevcut güvenlik önlemlerinin etkisiz olduğunu belirtmiştir. Bu bulgu, yüksek düzeyde farkındalık göstermektedir.	Güvenlik önlemlerinin etkisiz olduğunu ve kartının kaybolması veya çalınması durumunda ciddi sorunlar yaşanabileceğini düşündüğünü ifade etmiştir. Bu bulgu, yüksek düzeyde güvenlik endişelerini göstermektedir.	Kartını günlük yaşamında pek kullanmadığını ancak resmi işlemler için kullandığını belirtmiştir. Bu bulgu, orta düzeyde bir benimsenme düzeyini göstermektedir.	Mahremiyetin korunması için önceden bilgilendirme mesajları gönderilmesi ve işlemlerin onayı olmadan gerçekleştirilmemesi gerektiğini düşünmektedir. Bu bulgu, yasal düzenlemelere olan güvenin düşük ve mahremiyet algısının olumsuz olduğunu gösterir.
K17	Kişisel verilerinin korunması konusunda akıllı kimlik kartlarına güvendiğini ancak mevcut güvenlik önlemlerini tam anlamıyla etkili bulmadığını belirtmiştir. Ayrıca, işlem yapan memurların veya kurum çalışanlarının	Kartının kaybolması veya çalınması durumunda ciddi sorunlar yaşanabileceğini düşündüğünü belirtmiştir. Ayrıca, çevrimiçi kullanım sırasında ek güvenlik önlemleri alınması gerektiğini savunmuş ve mahremiyet bilgilerinin	Kartını günlük hayatta sıkça kullanmadığını ancak resmi işlemler için kullandığını belirtmiştir. Bu bulgu, orta düzeyde bir benimsenme düzeyini göstermektedir.	Resmi bilgilendirme yapılmadığını ve kişisel verilerinin güvende olmadığını düşündüğünü ifade etmiştir. Bu bulgu, yasal düzenlemelere olan güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.

	sadece işlemle ilgili bilgileri görmesini önermesi, mahremiyet farkındalığının yüksek olduğunu göstermektedir.	tehlikede olduğunu vurgulamıştır. Bu bulgu, güvenlik endişelerinin yüksek olduğunu göstermektedir		
K18	Akıllı kimlik kartlarının güvenlik ve mahremiyet endişeleri taşıdığını belirtmiş ve daha üst düzey güvenlik çalışmaları yapılması gerektiğini önermiştir. Bu bulgu, mahremiyet konusunda yüksek düzeyde farkındalık göstermektedir.	Mevcut güvenlik önlemlerini yetersiz bulduğunu ve kartların kaybolması veya çalınması durumunda ciddi sorunlar yaşanabileceğini düşündüğünü belirtmiştir. Bu bulgu, güvenlik endişelerinin yüksek olduğunu göstermektedir.	Akıllı kimlik kartlarının güvenlik ve mahremiyet zaafları içerdiğini düşündüğünü ve daha manuel sistemleri tercih ettiğini belirtmiştir. Bu bulgu, düşük bir benimsenme düzeyini göstermektedir	Resmi bilgilendirmelerin yetersiz olduğunu ve daha güçlü şifreleme ve doğrulama yöntemlerinin uygulanmasını önermiştir. Bu bulgu, yasal düzenlemelere olan güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.
K19	Kişisel verilerin yetkisiz erişime karşı korunması için daha güçlü şifreleme ve doğrulama yöntemlerinin uygulanmasını önermiş ve mahremiyet bilgilerinin tehlikede olduğunu düşündüğünü belirtmiştir. Bu bulgu, mahremiyet konusunda yüksek düzeyde farkındalık göstermektedir.	Mevcut güvenlik önlemlerinin yetersiz olduğunu düşünmekte, çip kullanımının daha etkin hale getirilmesi gerektiğini vurgulamaktadır. Güvenlik önlemlerinin yetersiz olduğunu ve kartların kaybolması veya çalınması durumunda ciddi güvenlik sorunları yaşanabileceğini düşündüğünü belirtmiştir. Bu bulgu, güvenlik endişelerinin yüksek olduğunu göstermektedir	Çipli kartların daha işlevsel hale getirilmesi için önerilerde bulunmuş, ancak güvenlik ve mahremiyet zaafları olduğunu belirtmiştir. Bu bulgu, düşük bir benimsenme düzeyini göstermektedir	Resmi bilgilendirmenin yetersiz olduğunu belirtmiş ve daha güçlü şifreleme ve doğrulama yöntemlerinin uygulanmasını önermiştir. Bu bulgu, yasal düzenlemelere olan güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.
K20	Kişisel verilerin korunması konusunda bilinçli olduğunu ifade etmiş ancak arka planda ne kadar korunduğunu bilmediğini belirtmiştir. Güvenlik önlemlerinin yetersiz olduğunu düşündüğü için, mahremiyet konusunda da farkındalığa sahip	Çift katmanlı doğrulama sistemleri gibi ek güvenlik önlemleri önermiş ancak güvenlik ve mahremiyet endişeleri taşıdığını belirtmiştir. Bu bulgu, kartların kullanımı ve benimsenmesi ile mahremiyet endişeleri arasında bir çatışma olabileceğini göstermektedir.	Çift katmanlı doğrulama sistemleri gibi ek güvenlik önlemleri önermiş ancak güvenlik ve mahremiyet endişeleri taşıdığını belirtmiştir. Bu bulgu, kartların kullanımı ve benimsenmesi ile mahremiyet endişeleri arasında bir çatışma olabileceğini göstermektedir	Resmi bilgilendirmenin yetersiz olduğunu belirtmiş ve daha güçlü şifreleme ve doğrulama yöntemlerinin kullanılması gerektiğini savunmuştur. Bu bulgu, yasal düzenlemelere olan güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.

	olduğunu söylemek mümkündür.			
K21	Kişisel verilerin korunması konusunda yeterince bilinçli olmadığını ifade etmiştir. Mevcut güvenlik önlemlerini yeterli bulsa da birçok kuruluşun altyapısında hala bu bilgilere erişilebildiğini vurgulamıştır. Bu bulgu, genel olarak mahremiyet konusunda düşük farkındalık göstermektedir.	Güvenlik önlemlerini yeterli bulsa da kişisel verilerin izinsiz erişime karşı korunmasının zayıf olduğunu düşündüğünü belirtmiştir. Bu bulgu, güvenlik ve mahremiyet arasında bir ilişki olduğunu ve mahremiyet konusunda endişeler taşıdığını göstermektedir.	Akıllı kimlik kartlarının daha aktif bir şekilde günlük hayata entegre edilmesi gerektiğini önermiştir. Bu bulgu, kartların kullanımı ve benimsenmesi ile mahremiyet endişeleri arasında bir çatışma olmadığını göstermektedir	Resmi bilgilendirmenin yetersiz olduğunu belirtmiş ve daha güçlü şifreleme ve doğrulama yöntemlerinin kullanılması gerektiğini savunmuştur. Bu bulgu, yasal düzenlemelere olan güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.
K22	Kişisel verilerini koruma konusunda bilgisi olduğunu ancak bilinçli hareket edemediğini ve verilerinin ne kadar korunduğunu bilmediğini ifade etmiştir. Mahremiyet konusunda güvenlik önlemlerini yeterli bulmakla birlikte, kimlik kartının kaybolması durumunda ciddi sorunlar yaşayabileceğini belirtmiştir. Bu bulgu, genel olarak mahremiyet konusunda düşük farkındalık göstermektedir.	Kişisel bilgilerine yetkisiz erişimi engellemek için özel önlemler almadığını ve bu konuda bilgi sahibi olmadığını belirtmiştir. Ayrıca, mevcut siber güvenlik önlemlerini yeterli bulmamaktadır. Bu bulgu, güvenlik ve mahremiyet arasında bir ilişki olduğunu ve mahremiyet konusunda endişeler taşıdığını göstermektedir.	Kimlik kartlarının kullanımını desteklemekte ancak mahremiyet endişeleri olduğunu belirtmektedir. Bu bulgu, kartların kullanımı ve benimsenmesi ile mahremiyet endişeleri arasında bir çatışma olabileceğini göstermektedir	Resmi bilgilendirmenin yetersiz olduğunu ve güvenlik ve mahremiyet endişelerini azaltmak için bilinçlendirme yapılması gerektiğini vurgulamıştır. Bu bulgu, yasal düzenlemelere olan güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.

K23	Güvenlik önlemlerinin devlet tarafından yeterli olduğunu düşünse de, kimlik kartının kaybolması veya çalınması durumunda ciddi sorunlar yaşayabileceğini ve veri sızıntılarının fazla olduğunu ifade etmiştir. Bu bulgu, genel olarak mahremiyet konusunda düşük bir farkındalık göstermektedir.	Çip kullanımının daha aktif hale getirilmesi gerektiğini ve kişisel bilgi erişimine parmak izi doğrulaması eklenmesini önermiştir. Bu bulgu, güvenlik önlemlerine yönelik bir farkındalık olduğunu göstermektedir.	Kimlik kartlarının sunduğu kolaylıkları ve trafik kontrolü gibi olumlu yönlerini vurgulamıştır. Ancak, güvenlik açıklarını ve mahremiyet endişelerini de dile getirmiştir. Bu bulgu, kartların kullanımı ve benimsenmesi ile mahremiyet endişeleri arasında bir çatışma olduğunu göstermektedir.	Resmi bilgilendirmenin yetersiz olduğunu ve güvenlik önlemlerinin artırılması gerektiğini belirtmiştir. Bu bulgu, yasal düzenlemelere olan güvenin düşük ve mahremiyet algısının olumsuz olduğunu göstermektedir.
K24	Kişisel verilerini koruma konusunda bazı önlemler aldığını belirtse de genel olarak mahremiyet konusunda endişeler taşımaktadır. Özellikle, sanal ortamda güvenliğin aşılabileceğini düşündüğünü ve veri sızıntılarının ciddi sonuçlar doğurabileceğini ifade etmiştir.	Güvenlik önlemlerinin yetersiz olduğunu ve çevrimiçi kullanım esnasında güvenlik önlemlerinin artırılması gerektiğini savunmuştur. Bu bulgu, mahremiyet konusunda güvenlik endişeleri taşıdığını göstermektedir.	Akıllı kimlik kartlarının potansiyel faydalarını görmekte ancak mevcut durumda kullanımının beklenen vermediğini düşünmektedir. Bu bulgu, kartların benimsenmesi ile mahremiyet endişeleri arasında bir çatışma olduğunu göstermektedir.	Resmi bilgilendirmenin yetersiz olduğunu ve mevcut düzenlemelerin kartların güvenliği ve mahremiyeti konusunda yetersiz olduğunu düşünmektedir.
K25	Kişisel verilerini koruma konusunda bilinçli olduğunu ve çevrimiçi paylaşımlarda dikkatli olduğunu belirtmiştir. Ancak, mevcut güvenlik önlemlerini yeterli bulmadığını ve veri sızıntıları konusunda endişeleri olduğunu ifade etmiştir.	Güvenlik önlemlerinin yetersiz olduğunu düşünmekte ve dolayısıyla mahremiyet konusunda da endişeler taşımaktadır	Akıllı kimlik kartlarının taşıma kolaylığı ve işlem hızı gibi faydalarını önemsemektedir. Güvenlik ve mahremiyet konularında da endişeleri bulunmaktadır.	Resmi bilgilendirmenin yetersiz olduğunu ve bu konuda kendi araştırma yapmadığını ifade etmiştir.
K26	Kişisel verilerini koruma konusunda bilinçli olduğunu ve mevcut güvenlik önlemlerini etkili bulmadığını belirtmiştir	Güvenlik önlemlerinin etkisiz olduğunu düşünmekte ve bu yüzden mahremiyet konusunda da endişeleri bulunmaktadır.	Akıllı kimlik kartlarının kullanışlılığını ve mobil işlemlerdeki pratikliğini vurgulamış ancak güvenlik ve	Resmi bilgilendirmenin yetersiz olduğunu ve bu konuda kendi araştırmasını yapmadığını ifade etmiştir.

			mahremiyet endişeleri olduğunu belirtmiştir.	
K27	Kişisel verilerini koruma konusunda bilinçli olduğunu ve mevcut güvenlik önlemlerini yetersiz bulduğunu belirtmiştir.	Güvenlik önlemlerinin etkisiz olduğunu düşünmekte ve bu yüzden mahremiyet konusunda da endişeleri bulunmaktadır.	Akıllı kimlik kartlarının kullanışlılığını ve mobil işlemlerdeki pratikliğini vurgulamış ancak güvenlik ve mahremiyet endişeleri olduğunu belirtmiştir.	Resmi bilgilendirmenin yetersiz olduğunu ve bu konuda yeterli bilgiye sahip olmadığını ifade etmiştir.
K28	Kişisel verilerin korunması konusunda daha fazla bilgi ve güvenlik önlemi gerektiğini düşündüğünü belirtmiştir.	Mevcut güvenlik önlemlerini yetersiz bulduğunu ve daha güçlü güvenlik önlemlerinin getirilmesi gerektiğini vurgulamıştır.	Akıllı kimlik kartlarının kullanışlılığını ve avantajlarını belirtmiş ancak güvenlik ve mahremiyet konularında da endişeleri olduğunu ifade etmiştir	Resmi bilgilendirmenin eksik olduğunu ve bu konuda kullanıcıların daha fazla bilgilendirilmesi gerektiğini belirtmiştir.
K29	Kişisel verilerinin güvende olmadığını düşündüğünü ve çevrimiçi kullanım sırasında bilgilerinin izinsiz erişime karşı korunmadığını belirtmiştir.	Çip kullanımının daha aktif hale getirilmesi gerektiğini ve ek güvenlik önlemlerinin zorunlu olması gerektiğini önermiştir.	Akıllı kimlik kartlarının kullanışlılığını ve trafik kontrolünde kullanımının avantajlarını vurgulamış, ancak güvenlik ve mahremiyet konularında endişeler taşıdığını belirtmiştir	Devletin yetkili kurumu tarafından çıkarıldığı için akıllı kimlik kartlarının güvenlik önlemlerinin yeterli olduğunu düşündüğünü belirtmiş, ancak güvenlik açıklarını ve çip kullanımının eksikliğini vurgulamıştır
K30	Kişisel verilerinin korunması konusunda yeterince bilinçli olmadığını ve nasıl önlem alabileceğini bilmediğini belirtmiştir.	Mevcut güvenlik önlemlerinin yetersiz olduğunu düşünmekte, çip kullanımının daha etkin hale getirilmesi gerektiğini vurgulamaktadır.	Akıllı kimlik kartlarının boyutunu ve kullanım kolaylığını olumlu bulmuş, ancak güvenlik ve mahremiyet konularında endişelerini dile getirmiştir	Güvenlik önlemlerinin artırılması gerektiğini ve daha etkin bilgilendirme yapılması gerektiğini önermiştir.

4.2.1. Katılımcıların Akıllı Kimlik Kartlarının Mahremiyetine Yönelik Farkındalık Algısı

1- Katılımcıların akıllı kimlik kartlarının mahremiyet konusundaki farkındalıklarını ölçebilmek için "*Akıllı kimlik kartları hakkında genel görüşleriniz nelerdir?" ve*

"*Akılı kimlik kartınızı kullanırken kişisel verilerinizi koruma konusunda ne kadar bilinçli olduğunuzu düşünüyorsunuz*?" soruları yöneltilmiştir.

"Akıllı kimlik kartları hakkında genel görüşleriniz nelerdir?"

Sorusuna verilen yanıtlar değerlendirildiğinde 30 katılımcının birbirine benzer görüşlere sahip olduğu görülmüştür. Özellikle kullanım açısından cebe sığabilecek boyutta olmasını, cinsiyetçi renklerin kalkmış olmasını olumlu bulurlarken fotoğraf kısmının soluk olmasını eleştirmişlerdir. Bu soru ile ilgili biraz daha farklı yorum yapan katılımcıların görüşleri aşağıdaki şekildedir:

"Yeni kimlik kartlarını boyut olarak başarılı buluyorum. Ayrıca cinsiyetçi renklerin kaldırılmış olması yönünden de güzel. Fotoğrafların soluk olması yönünden ise çok kötü buluyorum. Yani herkes birbirine benziyor gibi ve hapisten çıkmış gibi duruyor. İşleyiş olarak da hastane de ve trafikte geçmiş bilgilerin kart içinde saklanıyor olması güzel. Kimlik kartımı verdiğim an trafik kontrol işlemlerini yapabiliyorlar ya da hastane de geçirmiş olduğum rahatsızlıklarımı, kullandığım ilaçları, geçmişte yapılan aşılarıma bütün bilgilere ulaşabiliyorlar. Bu da işlerimi hızlı halletmemi sağlıyor." (K20, Erkek).

"Bence istenilen amaca ulaştığında iyi bir şey. Şu an için ehliyet bilgilerinin karta taşınabilir olması açısından iyi buluyorum. Onun dışında kullanım alanının genişletilmesi gerektiğini düşünüyorum. Sadece ehliyet uygulamasında yani trafik uygulamasında kalmaması gerektiği düşünüyorum." (K24, Erkek)

"Akıllı ibaresinin günlük hayatımıza bir akıllı telefon gibi kattığı çok fazla yenilik olmasa da sanırım güvenlik açısından eski kimlik kartlarımızdan daha ileri seviyede olduğunu düşünüyorum." (K21, Kadın)

"İsmen akıllı ama kullanım olarak akıllı tarafını henüz göremedik diğer kimlik kartı ile aynı standartlarda neredeyse. Kimliği doğrulayan resmi bir evrak olarak görüyorum." (K25, Kadın)

"*Akılı kimlik kartınızı kullanırken kişisel verilerinizi koruma konusunda ne kadar bilinçli olduğunuzu düşünüyorsunuz*?"

Sorusuna verilen yanıtlardan ise "bilinçli olduğunu düşünenler" ve "bilinçli olmadığını düşünenler" şeklinde iki farklı görüş ortaya çıkmaktadır. Her iki kategori için katılımcı görüşleri aşağıdaki şekildedir:

Akıllı kimlik kartlarını kullanırken kişisel verilerini koruma konusunda bilinçli olduğunu düşünenler;

"Yeterince bilinçli olduğumu düşünüyorum. Mesela hat değişikliği yaptığımda kimlik fotokopime not bırakıyorum. Sadece ilgili işlemi belirterek şerh düşüyorum. Onun haricinde internet sitesinden ya da banka uygulamalarından veri paylaşımına izin vermiyorum." (24, Erkek)

"Bilinçli olduğumu düşünüyorum fakat kişisel verilerimi koruma konusunda yeterli kontrol gücümün olmadığını düşünüyorum. Mesela bir işlemi yaptırabilmek için mecbur olarak bilgilerimi paylaşmak zorunda kalıyorum." (K18, Kadın)

"Bilinçli olduğumu düşünüyorum ama mevcut sistem kişisel verilerimi kurum ve kuruluşlarda paylaşmam için zorluyor. Genelde paylaşım yaptığım yerler resmi kurumlar olduğu için kişisel verilerimin korunduğunu düşünüyorum." (K27, Erkek)

"Bilinçli olduğumu düşünüyorum. Yeni kimlik kartlarını yeterli ve güvenilir buluyorum. Biraz daha kapsamlı olabilir ama bu haliyle bile yeterli olduğunu düşünüyorum. Eski kartla kıyasladığımda daha iyi buluyorum. Mesela eskisinde hem kullanışlılığı hem yer kaplama açısından fuzuliydi. Görüntü olarak sağlamlık olarak detay olarak üzerindeki bilgiler az ve öz yine de daha farklı bilgiler yüklenmesi gerektiğini de düşünüyorum. Banka bilgileri, özel bilgiler mesela eğitim gibi bilgilerin yer alması gerektiğini de düşünüyorum." (K5, Erkek)

"Kendimce bilinçliyim. Kendim dışındaki gelişen faktörlerden dolayı güvenmediğim birçok yönü bulunuyor. Mesela iş gördürürken kimlik bilgilerimi paylaşıyorum hatta fotokopisi bile alınıyor. Paylaştığım bilgilerimin arka planda saklanıp saklanmadığını bilmiyorum. İleride kötü bir amaç için kullanılabilir. Bu durumda kişisel verilerimi koruma konusunda sadece ilgili kurum ve kuruluşlara müracaat edebilirim" (K4, Kadın)

"Yeterince bilinçli olduğumu düşünüyorum. Yeni kimlik kartlarında parmak izi, fotoğraf ve imza örneği olduğu için bir nebzede olsa kişisel verilerimin korunduğunu düşünüyorum." (K17, Erkek)

Akıllı kimlik kartı kullanımında kişisel verilerin korunması konusunda yeterince bilinçli olmadığını düşünenler içerisinde soruya yorum katan katılımcılar ise;

"Bu konuda çok bilgi sahibi değilim açıkçası. Yeni kimlik kartları ile ilgili bilinçlendirici bilgilendirmeler yapılmadığı gibi benim de çok bir araştırmam olmadığı için bilinçli olduğumu düşünmüyorum." (K12, Kadın)

"Yeterince bilinçli olduğumu sanmıyorum. Bunun için nasıl bir önlem alabilirim ki? Sadece internet işlemlerimde bütün bilgilerimi paylaşmıyorum. Diğer resmi kurumlarda zaten kimliği fiziki olarak karşı tarafa teslim ederek işlem yaptırabiliyorum." (K30, Erkek)

"Çok bilinçli olduğumu düşünmüyorum. Sanırım teknoloji anlamında yetersiz ve bilgisiz olmam da beni bu düşünceye itiyor. Bu konuyla ilgili araştırma hiç yapmadım çünkü. Bu düşünceye iten bir diğer sebepse herkesin kullanması zorunlu olan bir kart olduğu için bir şey olmaz düşüncesi de var." (K21, Kadın)

"Bu konuda çok da bilinçli olduğumu düşünmüyorum. Ama dikkat ederim. Mesela T.C. kimlik bilgilerim istenirken ne amaçla istediklerini sorarım. (K9, Kadın)

"*Bu konuda çok da bilinçli olduğumu düşünmüyorum. Eski kimlik kartları daha iyiydi. Yeni kimlik kartında cip var robotlar bile ses kaydı alıyor ciplerde ne var hiçbir bilgim bulunmuyor. Değiştireceksiniz cezası var dedikleri için değiştirdim. Aslında cip dışında değişen bir şey yok. Maliyetten başka bir şey değil devletin kendini düşünmek için yaptığı bir uygulama olarak düşünüyorum."* (K7, Kadın)

Bu ölçütle, katılımcıların akıllı kimlik kartlarının mahremiyet konusundaki farkındalık düzeyi değerlendirilmiştir. Özellikle kişisel verilerin korunması konusundaki bilinçlilik ve bilgilendirme düzeyi üzerine odaklanılmıştır. Görüşme sonuçlarından katılımcıların büyük bir kısmının yüksek düzeyde farkındalığa sahip olduğu belirlenmiştir.

4.2.2. Akıllı Kimlik Kartlarının Mahremiyet ve Güvenlik Arasındaki İlişki

Katılımcılar, mahremiyet ve güvenlik ilişkisi ölçütü üzerinden değerlendirilmiş ve özellikle mevcut güvenlik önlemlerinin etkisi, kaybolma veya çalınma durumunda güvenlik riski ve izinsiz erişim önlemleri üzerine odaklanılmıştır.

"Akıllı kimlik kartınızın mahremiyetinizi koruma konusundaki güvenlik önlemlerini ne kadar etkili buluyorsunuz?" sorusuna verilen yanıtlar genel itibariyle benzer olup birkaç katılımcı yanıtına aşağıda yer verilmiştir.

"Kimlik kartımı kullanırken mevcut güvenlik önlemlerini yeterli bulmuyorum. Günümüz şartlarında tek tuşla bile dolandırıcılık yapılabildiği için ve çip içinde yüklü olan bilgilerimin neler olduğunu bilmediğim ve her işlemimde T.C. numaramla işlem yapmak zorunda kaldığım için güvenli bulmuyorum. İnternet üzerinden halletmem gereken işlemlerimde bile her türlü riskle karşı karşıyayım ve bununla ilgili mahkemeye bile çağrıldığım olmuştur. Bilgilerim çok kolay kopyalanabiliyor ve bilgim dışında kimlik bilgilerimle işlem yapılabiliyor." (K13, Kadın)

"Mevcut güvenlik önlemlerinin mahremiyeti koruduğunu sanmıyorum. Kötü niyetli kişiler kolaylıkla kimlik bilgilerine erişim sağlayabilir. Bu konuda veri sızıntılarının olduğunu düşünüyorum hatta yakın zamanda çevremde başına gelen bir tanıdığım bile var. E devletten ad, soyadı bilgisi girerek nüfus kayıt bilgilerinin tamamına telefon bilgine, doğum tarihi, aile nüfus kayıt örneğine kadar ulaşabiliyorlar." (K16, Kadın)

"Mevcut güvenlik önlemlerinin yeterli olmadığını düşünüyorum. Bugün sadece T.C. kimlik numaramla bile adıma şirket çok kolay bir şekilde açılabilir ya da telefon hattı çıkarılabilir. Kişiler için büyük öneme sahip işlemlerin bu kadar kolay yapılamaması gerekiyor. Bu sebepten dolayı e-devlet üzerinden sürekli adıma şirket ya da telefon hattı açılıp açılmadığını kontrol ediyorum." (K19, Erkek)

"Siber güvenlik önlemi alınmıştır muhakkak ama yeterli güvenlik önlemi alınmış olsaydı bugün dolandırıcılık işlemlerinin bu kadar çok olabileceğini sanmıyorum" (K20, Erkek)

"Yeterince güvenli bulmuyorum. İşlem yaptırdığım yetkili kurum ve kuruluş çalışanlarının iyi niyetli olup olmadığını bilmiyorum sonuçta. Kötü niyetli bir çalışan tarafından da verilerim sızdırabilir." (K25, Kadın)

"Açıkçası kimlik kartları ile ilgili yeterli güvenlik önlemi alındığını sanmıyorum. Çünkü güvenlik denilen şey arka planda sadece siber saldırı için alınan önlemler değildir. Devlet bu hususta kendisini korur. Benim de günlük işlerimi gördürmek için alabileceğim güvenlik yolunu açabilmeli. Mesela kimliğim ile işlem yapıldığında, e posta bilgilendirmesi, sms bilgilendirmesi gelebilmeli" (K30, Erkek)

Toplam 26 katılımcı akıllı kimlik kartlarının mahremiyeti koruma konusunda mevcut güvenlik önlemlerinin yeterli olmadığını belirtirken 4 katılımcı devletin yetkili kurumu tarafından çıkarıldığı için yeterince güvenlik önlemi alındığını aksi takdirde devlet için büyük bir risk unsuru oluşturabileceğini düşündüklerini belirtmişlerdir.

"Devletin yetkili kurumu tarafından çıkarıldığı için yeterli güvenlik önlemleri alındığını düşünüyorum. Aksi takdirde devletler için büyük tehdit unsuru olabilir." (K23, Erkek)

"Akıllı kimlik kartınızın kaybolması veya çalınması durumunda kişisel güvenliğiniz açısından ne derece sorun yaratacağını düşünüyorsunuz?" sorusuna verilen yanıtlarda ise 29 katılımcı ciddi problemler yaşayacağını belirtmiş özellikle yasadışı işlemler, dolandırıcılık, adına şirket kurma, cinayete kadar her türlü olayın içinde kendilerini bulabileceklerinden bahsetmiş sadece 1 tane katılımcı bu konuda herhangi bir sıkıntı yaşamayacağını belirtmiştir.

"Kimlik kartına benim bilgim ve T.C. numaram olmadan kimsenin ulaşabileceğini sanmıyorum. Kaybolması benim için sıkıntılı bir durum da değil. Zamanında kaybettim ve daha rahat bir şekilde yeni kartım elime ulaştı. Kişinin kendisine de bağlı bir durum bu kayıp bilgisini gerekli yerlere bildirmem yeterli oldu." (K5, Erkek)

"Akıllı kimlik kartlarının kullanımı sırasında kişisel verilerin izinsiz erişime karşı korunması hakkında ki düşünceniz nedir?" ve *"Akıllı kimlik kartındaki mahremiyet bilgilerinizin (dini bilgi, medeniyet durumu vb.) tehlikede olup olmadığı hakkında ne düşünüyorsunuz?"* sorularına verilen yanıtlarda katılımcılardan yalnızca K5' in mevcut güvenlik önlemlerinin etkisi, kaybolma veya çalınma durumunda güvenlik riski ve izinsiz erişim önlemlerini güvenli bulduğu diğer katılımcılar ise kimlik kartlarının kullanımı sırasında kişisel verilerin izinsiz erişime karşı korunmadığını ve mahremiyet bilgilerinin tehlikede olduğunu belirtmişlerdir.

4.2.3. Akıllı Kimlik Kartlarının Kullanımı ve Mahremiyet Endişeleri Arasındaki İlişki

Bu ölçüt ile katılımcıların akıllı kimlik kartlarının kullanım ve mahremiyet endişeleri değerlendirilmiştir. Özellikle kullanım sıklığı, izleme ve takip edilme endişeleri ile mahremiyet ihlali endişeleri üzerine odaklanılmıştır. Katılımcılara;

"Akıllı kimlik kartınızı ne sıklıkla kullanıyorsunuz?"

Sorusuna bütün katılımcılar birbirine benzer nitelikte yanıtlar vermiş olup genel olarak resmi ve özel sektörde işlemlerini yaptırırken, hastane, banka, trafik kontrolü gibi işlemlerinde kimlik kartlarını kullandıklarını belirtmişlerdir.

"Akıllı kimlik kartınızı kullanırken kişisel bilgilerinize yetkisiz erişimi engellemek için özel önlemler alıyor musunuz?"

Bu soruya katılımcıların tamamı kimlik kartlarını kullanırken kişisel bilgilere yetkisiz erişimi engellemek için özel önlem almadıklarını belirtmişlerdir.

"Kimlik kartım için alınabilecek bir önlem bulunmuyor buna en basit örneği telefon alımında verilebilirim ya da bankada sigorta işlemlerinde bile kimlik ön ve arka bilgilerini vermem gerekiyor. İstenilen bilgileri paylaşmadığım sürece işlemlerim ilerlemiyor paylaştığım zamanda da güvensiz bir ortamda risk altında hissediyorum kendimi" (K13,16, Kadın)

"Akıllı kimlik kartlarınızı kullanırken kişisel verilerinizin güvende olduğunu düşünüyor musunuz?" ve "Akıllı kimlik kartlarının izleme veya takip edilme olasılığı hakkında ne düşünüyorsunuz?" sorularına sadece K5, K8 ve K15 katılımcıları kişisel verilerinin güvende olduğunu, izleme ve takip edilme durumunun olmadığını düşündüklerini böyle bir şey yapılıyorsa da doğru bulmadıklarını belirtmişler diğer katılımcılar ise olumsuz görüş bildirmişlerdir. Birkaç katılımcı görüşüne aşağıda yer verilmiştir.

"Kimlik kartımı kullanırken kişisel verilerimin güvende olduğunu düşünmüyorum. Mesela kimlik bilgilerimi paylaştığım yetkili kuruluşlarda çalışan kişilerin iyi niyetli olup olmadığını bilmiyorum. Kurum çalışanının bile her türlü veri sızıntısını yapabileceğini düşünüyorum." (K1,6,19,20, Erkek)

"Kişisel verilerimin güvende olduğunu düşünmüyorum. Dijitalleşmeden kaynaklıda bir veri açığı bulunduğunu ya da işlemi gerçekleştiren kişilerin kötü niyetli olabileceğini de düşünüyorum. Arka planda bilgilerimi kopyalayabilirler verilerimi kötü niyetli kişilere verebilir ya da kendileri kötü niyetli bir şekilde kullanabilirler." (K2,8,16, Kadın)

"Çin de örneği var. Birçok vatandaş buna karşı çıktı özel hayatın gizliliği çok önemli. Bunu kimsenin bilmesini istemem ancak ulusal güvenliği tehdit eden bir davranış olacaksa herkesin izlenmesi olumlu ama bunun ilerisine gidilirse kötü amaçlar için kullanılacaksa buna karşıyım ve olumlu bakmıyorum."(K1, Erkek)

"Yeni kimlik kartları şu an tam olarak istenilen kullanım alanına sahip değil. Buna sahip olduğunda kesinlikle izleme ve takip edilme olacaktır. Düşünsenize gün içinde bir alışveriş merkezine girdiniz kimlik kartınızı taratıyorsunuz sonra hastaneye gittiniz aynı yani her gittiğimiz yerde kimlik kartımızı kullanmamızdaki amaç zaten izleme ve takip edilme olduğunu düşünüyorum." (K23,24,30 Erkek)

4.2.4. Akıllı Kimlik Kartlarının Yasal Düzenlemelere İlişkin Güvenilirliği ve Mahremiyet Algısı Arasındaki İlişki

Bu ölçüt ile, katılımcıların akıllı kimlik kartlarının yasal düzenlemelere duyulan güven ve mahremiyet algısı arasındaki ilişkiyi değerlendirir. Özellikle resmi bilgilendirme varlığı ve çevrimiçi kullanımda güvenlik önlemleri üzerinde odaklanılmış ve katılımcılara "*Akıllı kimlik kartı kullanımına ilişkin güvenlik ve mahremiyet konularıyla ilgili herhangi bir resmi bilgilendirme yapıldı mı?" ve "Akıllı kimlik kartlarının çevrimiçi kullanımı esnasında verilerinizin korunması için neler yapılabilir?"* soruları yöneltilmiştir.

"Kimlik kartımın çevrimiçi kullanımı esnasında şifreleme yöntemleri getirilmeli, çift katmanlı doğrulama sistemi getirilmeli, e devlet ile entegre çalışması gerekti̇ğini düşünüyorum" (K20, Erkek)

"Kimlik kartımı çevrimiçi kullanımı esnasında ara bir sistem kurularak doğrulama işlemi yapılabilir. Mesela masterpass sisteminde olduğu gibi. Bilgilerim direkt karşı tarafla paylaşılmadan arada doğrulama sistemi kurulmalı. Banka MasterCard'larındaki sistemde olduğu gibi işlemlerde sadece ödendi bilgisi veriyor başka bilgi paylaşmıyor." (K26, Erkek)

Mevcut güvenlik önlemlerinin yeterli olmadığını düşünen katılımcılar özellikle çip kullanımının daha etkin hale getirilmesi gerektiğini vurgulamaktadır. Kaybolması veya çalınması durumunda kişisel güvenliğinin ciddi şekilde tehdit altında olacaklarını düşünmekte ve özellikle finansal dolandırıcılık riskinden endişe duymaktadırlar. Kişisel bilgilerine yetkisiz erişimi engellemek için herhangi bir önlem almadıklarını ve bu konuda devletten resmi bir bilgilendirme yapılmadığını ifade etmişlerdir.

Güvenlik ve mahremiyet endişelerini azaltmak için çift doğrulama sistemi gibi ek önlemlerin getirilmesi gerektiğini önermişlerdir.

Son olarak, güvenlik önlemlerinin arttırılması gerektiğini düşünen katılımcı, daha etkin bilgilendirme, cihaz ve konum eşleştirme kontrolleri gibi tedbirlerin alınması gerektiğini düşünmektedir.

Birbirinden farklı 30 katılımcının görüşleri genel olarak değerlendirildiğinde;

Güvenlik Endişeleri

Katılımcılar, akıllı kimlik kartlarının güvenlik önlemlerini yetersiz bulmakta ve kartların çalınması veya kaybolması durumunda ciddi sorunlar yaşanabileceğinden endişe

duymaktadır. Örneğin, bir katılımcı şunları belirtmiştir: “Kartın çalınması durumunda kişisel verilerimin tehlikeye gireceğinden endişeliyim. Kartların daha güvenli şifreleme yöntemleriyle korunması gerektiğini düşünüyorum.”

Mahremiyet Endişeleri

Katılımcılar, kişisel verilerin izinsiz erişime karşı korunması gerektiğini vurgulamakta ve akıllı kimlik kartlarının mahremiyet konusunda hassas bir konu olduğunu düşünmektedir. Örneğin, bir katılımcı şunları söylemiştir: “Kartımdaki bilgilerin sadece yetkili kişilerce erişilebilir olmasını istiyorum. Daha az bilgi içeren kartlar, mahremiyetimi daha iyi koruyabilir.”

Bilgilendirme Eksikliği

Katılımcılar, resmi kurumların veya yetkililerin akıllı kimlik kartları hakkında yeterli bilgilendirme yapmadığını belirtmektedir. Bu eksik bilgilendirme, katılımcıların güvenlik ve mahremiyet konularında daha fazla endişe duymasına neden olmaktadır. Örneğin, bir katılımcı şunları ifade etmiştir: “Kartların güvenlik özellikleri hakkında daha fazla bilgiye ihtiyacımız var. Resmi kaynaklardan düzenli olarak güncel bilgiler almalıyız.”

4.3. Katılımcı Önerileri

Katılımcılar arasında yaygın olarak dile getirilen görüş, akıllı kimlik kartlarının güvenlik önlemlerinin daha etkili hale getirilmesi gerektiğidir. Birçok katılımcı, mevcut güvenlik önlemlerinin yetersiz olduğunu ve kartların kötüye kullanımını önlemek için daha gelişmiş teknolojilerin uygulanması gerektiğini ifade etmiştir. Özellikle, çift faktörlü kimlik doğrulama gibi yöntemlerin kartlara entegre edilmesi önerilmiştir. Bu, kart sahibinin kimliğinin doğrulanması için iki ayrı doğrulama adımının kullanılmasını içerir, böylece güvenlik riski önemli ölçüde azaltılmış olur. Bir katılımcı bu konuda şu öneriyi yapmıştır: “Kartlarda çift faktörlü kimlik doğrulama gibi daha güçlü güvenlik önlemleri kullanılmalı. Ayrıca, kişisel verilerin sadece belirli durumlar için paylaşılmasını sağlayacak yasal düzenlemeler getirilmeli.”

Buna ek olarak, mahremiyetin korunması hususunda daha sıkı yasal düzenlemeler talep edilmektedir. Katılımcılar, kişisel verilerin toplanması ve işlenmesi süreçlerinde daha fazla şeffaflık ve denetim gerektiğini belirtmişlerdir. Örneğin, kişisel verilerin yalnızca gerekli ve belirli durumlarda kullanılmasını sağlayacak yasal düzenlemelerin getirilmesi

gerektiği vurgulanmıştır. Bu talepler, kişisel mahremiyetin korunması ve bireylerin verilerinin izinsiz kullanılması durumlarının önüne geçilmesi amacıyla yapılmıştır.

Ayrıca, katılımcılar resmi bilgilendirme eksikliğinden de şikayet etmişlerdir. Akıllı kimlik kartlarının güvenlik ve kullanım özellikleri hakkında yeterli bilgilendirme yapılmadığına dikkat çekilmiş ve daha fazla kamuoyu bilgilendirme kampanyası talep edilmiştir. Bu tür kampanyaların, kullanıcıların kartları nasıl güvenli bir şekilde kullanacakları konusunda bilinçlenmelerine yardımcı olacağı düşünülmektedir.

Bazı katılımcılar, akıllı kimlik kartlarının günlük yaşamda pratik ve kullanışlı olduğunu belirtmişlerdir. Özellikle kartların cüzdana sığacak şekilde tasarlanmış olması ve birçok farklı işlemi kolayca gerçekleştirme imkanı sağlaması vurgulanmıştır. Bu katılımcılar, kartların taşınabilirliğinin ve kullanım kolaylığının, günlük işlerde zaman kazandırdığı ve hayatı kolaylaştırdığı konusunda olumlu geri bildirimlerde bulunmuşlardır.

Ancak, olumlu görüşler dile getirilirken bile, katılımcılar güvenlik ve mahremiyet konularına daha fazla önem verilmesi gerektiğini vurgulamışlardır. Kartların avantajlarını kabul ederken, olası güvenlik açıklarının ve kişisel veri ihlallerinin önlenmesi için sürekli olarak daha iyi çözümler aranması gerektiğine dikkat çekmişlerdir.

- ✓ **Genel Değerlendirme:**

Katılımcıların demografik bilgilerinin (eğitim, yaş, çalıştığı kurum, cinsiyet) bulgular üzerinde herhangi bir etkiye sahip olmadığı, bilgilendirme eksikliğinin olması günümüzde dolandırıcılık eylemlerinin daha da fazla yaşanıyor olması kimlik kartları için yeterli güvenlik önlemi alınmadığını düşündürmektedir.

Katılımcıların çoğunluğu, akıllı kimlik kartlarıyla ilgili güvenlik ve mahremiyet konularında ciddi endişeler taşımaktadır. Bu endişeler, daha etkili güvenlik önlemleri ve sıkı yasal düzenlemeler ile giderilmelidir. Katılımcılar, mevcut güvenlik önlemlerinin yetersiz olduğunu ve mahremiyetin korunması için daha sıkı denetim ve şeffaflık talep etmektedirler. Ayrıca, resmi bilgilendirme eksikliğinin bu endişeleri artırdığı ve kullanıcıların bilinçlendirilmesi gerektiği vurgulanmıştır. Bu bağlamda, hem kartların kullanım kolaylığı ve pratikliği açısından olumlu görüşler dile getirilmiş, hem de güvenlik ve mahremiyetin sağlanması için daha fazla önlem alınması gerektiği belirtilmiştir.

Çalışma kapsamında belirlenen hipotezlerin katılımcı görüşlerine göre tamamının kabul edildiğini söylemek mümkündür. Buna göre hipotezler akıllı kimlik kartlarının mahremiyet düzeyi farkındalığı, mahremiyet ve güvenlik ilişkisi, kullanım ve mahremiyet endişeleri ilişkisi ve yasal düzenlemelere güven ve mahremiyet algısı ilişkileri ifade edilerek Tablo 3 oluşturulmuş ve hipotezlerin kabulüne ilişkin değerlendirme yapılmıştır.

Tablo 4. Hipotezlere İlişkin Tablo

Hipotezler	**Mahremiyet Düzeyi Farkındalığı**	**Mahremiyet ve Güvenlik İlişkisi**	**Kullanım ve Mahremiyet Endişeleri İlişkisi**	**Yasal Düzenlemelere Güven ve Mahremiyet Algısı İlişkisi**
H_1: Akıllı kimlik kartı kullanan vatandaşlar genel olarak, kişisel verilerinin kartlarda olması ve saklanmasına ilişkinmahremiyet meselelerinde yüksek düzeyde farkındalığa sahiptir.	Katılımcı görüşlerine göre H_1 **kabul** edilmiştir. Buna göre akıllı kimlik kartı kullanan vatandaşların genel olarak mahremiyet konusunda yüksek düzeyde farkındalığa sahip oldukları düşünülmektedir.			
H_2: Akıllı kimlik kartlarının mahremiyet yönlerine dair farkındalığı olan vatandaşların, kartlardaki kişisel verilerin güvenliğine dair endişeleri daha yüksektir.		Katılımcı görüşlerine göre H_2 **kabul** edilmiştir. Buna göre mahremiyet konularına duyarlı olan bireylerin, kartlardaki kişisel verilerin güvenliği konusunda daha fazla endişe taşıdıkları düşünülmektedir.		

H_3: Akıllı kimlik kartlarının faydaları ve sunduğu kolaylıkların kendileri açısından daha önemli olduğunu düşünen vatandaşlar, mahremiyet endişeleri olsa dahi, kartları kullanma ve benimseme düzeyleri daha düşüktür.			Katılımcı görüşlerine göre H_3 **kabul** edilmiştir. Buna göre akıllı kimlik kartlarının sağladığı faydaların, kullanıcılar için mahremiyet endişelerinden daha önemli olduğu düşünülmektedir.	
H_4: Akıllı kimlik kartlarıyla ilgili yasal düzenlemelere yüksek düzeyde güven duymayan vatandaşların, kartların mahremiyet yönlerine dair algılarının olumlu olma olasılığı daha düşüktür.				Katılımcı görüşlerine göre H_4 **kabul** edilmiştir. Buna göre akıllıkimlik kartlarıyla ilgili yasal düzenlemelere güven duymayanların, kartların mahremiyet yönlerine daha olumsuz baktıkları düşünülmektedir.

5. BÖLÜM: SONUÇ ve DEĞERLENDİRME

Kimlik kartları, kişilerin kimliklerini kanıtlamak ve kamu yönetimi tarafından tanınmalarını sağlamak için kullanılan önemli araçlardır. Akıllı kimlik kartları, devlet tarafından verilen ve vatandaşların kimliklerini hem kamu hem de özel sektörde belirlemek için kullanılan özel kartlardır. Bu kartlar, taklit ve sahteciliği önlemek için yüksek güvenlik önlemlerine sahiptir. Parmak izi, damar izi ve avuç içi izi gibi biyometrik verileri kullanmaktadır ve 1 GB depolama kapasitesine sahiptir.

ISO 7810 standardına göre üç farklı kart tipi tanımlanmıştır: ID-1, ID-2 ve ID-3. ID-1 kartlar genellikle bankacılık, ehliyet ve kimlik kartları gibi alanlarda kullanılırken, ID-2 kartlar birçok ülkede kimlik kartı olarak kullanılır ve ID-1'den biraz daha büyük boyutlara sahiptir. ID-3 kartlar ise pasaport ve uluslararası geçişlerde kullanılan vize kartlarıdır ve en büyük boyuta sahip kimlik kartlarıdır.

Mahremiyet en sade ifade ile gizlilik olarak tanımlanmaktadır. Akıllı kimlik kartları, modern şifreleme tekniklerini kullanarak birçok güvenlik prosedürünü desteklemektedir. Özellikle, Genel Anahtar Altyapısı Şifrelemesi, bu yeni nesil teknolojik üründe aktif olarak kullanılmaktadır. Ancak, kartlara yüklenen yazılımlar nedeniyle güvenlik açıkları ortaya çıkabilmekte, bu da veri sızıntıları gibi risklere yol açabilmektedir.

Bu araştırmanın amacı, vatandaşların akıllı kimlik kartlarına yönelik mahremiyet algılarını ve bu kartların kullanımı sırasında kişisel verilerin korunması hakkındaki düşüncelerini detaylı bir şekilde incelemektir. Çalışmanın evrenini, 2024 yılında Karaman il merkezinde yaşayan ve 18 yaş üzeri 30 reşit bireyden oluşmaktadır. Veri toplama sürecinde, araştırmacılar tarafından özel olarak geliştirilen ve literatür taraması sonucunda oluşturulan yarı yapılandırılmış görüşme formu kullanılmıştır. Araştırmada toplam 15 adet açık uçlu soru bulunmaktadır.

Elde edilen veriler değerlendirildiğinde, katılımcıların demografik bilgilerinin (eğitim, yaş, çalıştığı kurum, cinsiyet) bulgular üzerinde herhangi bir etkiye sahip olmadığı, bilgilendirme eksikliğinin olması günümüzde dolandırıcılık eylemlerinin daha da fazla yaşanıyor olması kimlik kartları için yeterli güvenlik önlemi alınmadığını düşündürmektedir. Ayrıca Kimlik kontrolünü gerçekleştiren kişi sayısının artmasıyla, yetkisiz kişilerin vatandaşların kimlik kartı kullanımını izlemesi ve ifşa etmesi gibi

durumlar kişisel verilerin gizliliğini ihlal etmektedir. Bir kez kişinin verilerine erişim hakkı kazanan biri, kişi hakkında detaylı bilgilere ulaşabilecek ve bu durum kişi için sorun oluşturabilecektir.

Elde edilen bulgulara göre, katılımcıların çoğunluğu akıllı kimlik kartlarıyla ilgili güvenlik ve mahremiyet konularında ciddi endişeler taşımaktadır ve daha etkili önlemler alınmasını talep etmektedir.

Akıllı kimlik kartları, kişisel verilerin korunması ve kullanıcı güvenliğinin sağlanması açısından önemli bir araç olarak görülmektedir. Ancak, katılımcılar kartların güvenlik önlemlerini yetersiz bulmakta ve bu durumun kartların çalınması veya kaybolması gibi olaylarda ciddi sorunlara yol açabileceğinden endişe duymaktadır. Kartların çalınması durumunda kişisel bilgilerin kötüye kullanılma riski, katılımcıların güvenlikle ilgili büyük kaygılarından biridir.

Mahremiyet konusunda ise, katılımcılar kişisel verilerin izinsiz erişime karşı korunması gerektiğini vurgulamakta ve bu konuda daha sıkı güvenlik önlemleri talep etmektedir. Özellikle, kartlardaki bilgilerin sadece yetkili kişiler tarafından erişilebilir olması gerektiğini düşünen katılımcılar, daha az bilgi içeren kartların mahremiyetin korunmasına yardımcı olabileceğini düşünmektedir.

Bunun yanı sıra, katılımcılar resmi kurumların veya yetkililerin akıllı kimlik kartlarıyla ilgili yeterli bilgilendirme yapmadığını belirtmektedir. Bu bilgilendirme eksikliği, kullanıcıların güvenlik ve mahremiyet konularında daha fazla endişe duymasına neden olmakta ve kartların doğru kullanımı ve güvenliği konusunda eksiklikler yaşanmasına yol açmaktadır.

Bir diğer husus ise katılımcıların resmi kurumların yeterli bilgilendirme yapmadığı hususunda şikayetlerini dile getirmiş olmalarına rağmen kendilerinin de bu konu hakkında herhangi bir araştırma yapmayışları olmuştur. Kişilerin hayatında çok önemli yeri olan kimlik kartlarıyla ilgili yüksek düzeyde endişeler yaşanmasına rağmen herhangi bir araştırmanın yapılmaması aynı zamanda vatandaşların okuma ve araştırma düzeylerinin de düşük olduğu sonucunu vermektedir.

Özetle katılımcılar akıllı kimlik kartlarındaki güvenlik ve mahremiyet konularında ciddi endişeler taşımakta ve bu konularda daha etkili önlemler alınmasını talep etmektedir. Ayrıca, resmi bilgilendirme eksikliğinin bu endişeleri artırdığına dikkat çekmektedirler.

Bu noktada, daha şeffaf ve düzenli bilgilendirme ile güvenlik önlemlerinin güçlendirilmesi gerektiği vurgulanmaktadır.

Sonuç olarak, bu çalışma vatandaşların akıllı kimlik kartlarıyla ilgili güvenlik ve mahremiyet konularında ciddi endişeler taşıdığını göstermektedir. Bu endişelerin giderilmesi için daha etkili güvenlik önlemleri alınması, şeffaf bilgilendirme süreçlerinin sağlanması ve mahremiyetin korunması için daha sıkı yasal düzenlemelerin hayata geçirilmesi gerekmektedir. Bu önerilerin, akıllı kimlik kartlarının güvenliği ve kullanımıyla ilgili politika yapıcılar ve ilgili kurumlar tarafından dikkate alınması gerektiği düşünülmektedir.

Öneriler;

- Akıllı kimlik kartlarında kullanılan güvenlik önlemlerinin güçlendirilmesi gerekmektedir. Özellikle, biyometrik verilerin daha güvenli bir şekilde depolanması ve işlenmesi için yeni teknolojilerin ve standartların benimsenmesi önemlidir. Kartların fiziksel güvenliği için yeni nesil malzemelerin kullanılması ve çip tabanlı güvenlik sistemlerinin iyileştirilmesi gerekmektedir. Yazılım güvenliği açısından düzenli güncellemeler ve güvenlik yamaları sağlanmalıdır.
- Kişisel verilerin izinsiz erişime karşı korunması için sıkı şifreleme yöntemleri kullanılmalı ve erişim kontrolleri sıkı bir şekilde uygulanmalıdır. Kartlarda yer alan kişisel bilgilerin minimum düzeyde tutulması ve sadece gerektiğinde erişilebilir olması sağlanmalıdır. Mahremiyet politikaları ve standartları, uluslararası güvenlik normlarına uygun olarak güncellenmelidir.
- Vatandaşların akıllı kimlik kartlarının doğru ve güvenli kullanımı konusunda düzenli olarak bilgilendirilmesi sağlanmalıdır. Bu, kullanıcıların kartlarıyla ilgili bilinçli kararlar almasını sağlayacaktır. Resmi kurumlar ve yetkililer, kartların güvenliği ve kullanımıyla ilgili açık ve anlaşılır bilgi sağlamalıdır. Kullanıcıların karşılaşabileceği riskler ve alınması gereken önlemler konusunda detaylı bilgilendirme süreçleri oluşturulmalıdır.
- Akıllı kimlik kartlarının kullanımıyla ilgili olarak daha sıkı yasal düzenlemelerin hayata geçirilmesi gerekmektedir. Bu düzenlemeler, kartların güvenliği, kullanımı ve kişisel verilerin korunmasıyla ilgili net kuralları içermelidir. Veri

güvenliği ve mahremiyet konularında uluslararası standartlara uyum sağlanmalı ve uygun denetim mekanizmaları oluşturulmalıdır.

Bu önerilerin, akıllı kimlik kartlarının güvenliği ve kullanımıyla ilgili politika yapıcılar, ilgili kurumlar ve teknoloji sağlayıcıları tarafından dikkate alınması gerektiği düşünülmektedir. Bu şekilde, vatandaşların güvenliği ve mahremiyetinin korunması için daha sağlam bir temel oluşturulabilir.

Gelecekteki Çalışmalar;

Yetişkin 30 birey ile mülakat görüşmeleri gerçekleştirilerek yapılan bu çalışmanın kısıtları göz önüne alındığında gelecekte yapılacak çalışmalar aşağıdaki alanlarda derinleştirilebilir:

- ✓ **Farklı Demografik Grupların İncelenmesi:**

Bu çalışma genel olarak yetişkin ve 30 birey ile nitel yöntemle yapılan bir çalışmayı kapsamaktadır. Gelecekte, farklı yaş grupları, eğitim seviyeleri veya meslek grupları gibi farklı demografik özelliklere sahip katılımcıların görüşleri nitel ve/veya nicel araştırma teknikleri ile incelenebilir. Bu, akıllı kimlik kartlarının farklı gruplar üzerindeki etkilerini daha kapsamlı bir şekilde ortaya koyabilir.

- ✓ **Teknolojik Gelişmelerin İncelenmesi:**

Akıllı kimlik kartları teknolojisinin hızla geliştiği bir dönem yaşamaktayız. Gelecekteki çalışmalar, yeni güvenlik teknolojilerinin kartlara entegrasyonu, biyometrik verilerin kullanımı ve güvenlik açıkları konularını daha detaylı inceleyebilir.

- ✓ **Hukuki ve Düzenleyici Çalışmalar:**

Akıllı kimlik kartlarının kullanımıyla ilgili mevcut hukuki çerçeve ve düzenlemeler, gelecekteki çalışmalarda daha derinlemesine incelenebilir.

- ✓ **Kullanıcı Deneyimi:**

Gelecekteki çalışmalar, vatandaşların akıllı kimlik kartlarını günlük yaşamlarında nasıl kullandıklarını ve bu kullanımın pratikliği üzerindeki etkilerini değerlendirebilir.

- ✓ **Kültürel ve Sosyal İnceleme:**

Akıllı kimlik kartlarının kabul edilme oranları ve kullanımı, kültürel ve sosyal faktörlere de bağlı olabilmektedir. Gelecekteki çalışmalar, bu kartların farklı kültürel ve sosyal

bağlamlarda nasıl algılandığını ve kullanıldığını inceleyerek, daha kapsamlı bir tablo ortaya koyabilir.

Araştırma, katılımcıların güvenlik ve mahremiyet konusundaki endişelerini ve önerilerini ortaya koyarak, akıllı kimlik kartlarının geliştirilmesi için yol gösterici nitelikte olduğu düşünülmektedir. Bu doğrultuda, güvenlik açıklarının ve kişisel veri ihlallerinin önlenmesi için gerekli teknik ve yasal düzenlemelerin yapılması gerektiği vurgulanmıştır.

Bu çalışmanın sonuçları, kamuoyu farkındalığını artırmak ve kullanıcıların bilinçlenmesine katkıda bulunmak amacıyla düzenlenecek etkinlikler için de önemli bilgiler sağlamaktadır. Araştırmanın bulguları, akıllı kimlik kartlarının sağladığı pratik faydaların yanı sıra, güvenlik ve mahremiyet konularının kullanıcılar için ne kadar kritik olduğunu göstermiştir. Bu bağlamda, kullanıcı deneyimini iyileştirmek ve güvenlik endişelerini gidermek amacıyla daha güçlü doğrulama yöntemlerinin ve sıkı mahremiyet politikalarının uygulanması gerektiği düşünülmektedir.

Sonuç olarak, bu çalışma, akıllı kimlik kartlarının yaygınlaşan kullanımıyla birlikte ortaya çıkan güvenlik ve mahremiyet sorunlarına dikkat çekerek, hem bireylerin kişisel verilerinin korunmasını sağlamak hem de bu kartların toplum genelinde kabulünü artırmak için gerekli adımların atılması gerekliliğine vurgu yapmaktadır.

KAYNAKÇA

Abd Elwahab, A., Bahaa Eldin, A. M., Wahba, A. M., & Sheirah, M. A. (2009). A security layer for smart card applications authentication. *2009 International Conference on Computer Engineering & Systems*, 514-517. https://doi.org/10.1109/ICCES.2009.5383211

Abrial, A., Bouvier, J., Renaudin, M., Senn, P., & Vivet, P. (2001). A new contactless smart card IC using an on-chip antenna and an asynchronous microcontroller. *IEEE Journal of Solid-State Circuits*, *36*(7), 1101-1107. https://doi.org/10.1109/4.933467

Akçadağ, K. (2024). *Mahremiyetin dijital ifşası: TikTok / Digital disclosure of privacy: TikTok* [Yayımlanmamış Yüksek Lisans Tezi, Mardin Artuklu Üniversitesi, Lisansüstü Eğitim Enstitüsü, Sosyoloji Ana Bilim Dalı]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Akkurt, S. S. (2017). Kişilik Hakkının Sosyal Medya Kullanıcıları Tarafından İhlâli Hâlinde Ortaya Çıkacak Cezaî Sorumluluğa Medenî Hukuk Bağlamında Bir Bakış. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, *25*(2), Article 2. https://doi.org/10.15337/suhfd.327503

Alkhurayyif, Y. (2013). Security Concerns with National ID Cards. *International Journal of Computing Science and Information Technology*, *Vol.1*((2)), 44-48.

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. *Journal of Network and Computer Applications*, *62*, 137-152. https://doi.org/10.1016/j.jnca.2016.01.008

Aslan, V. (2016). Amerikalılar Arası İnsan Hakları Sistemi. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, *3*(2), Article 2. https://doi.org/10.21492/inuhfd.239814

Aslan-Turan, E. (2022). Dijital Teknolojilerin Mahremiyet Üzerindeki Etkileri. *Şarkiyat*, *14*(2), 834-849. https://doi.org/10.26791/sarkiat.1114557.

BankID. (2023). *BankID - Sweden*. https://helpx.adobe.com/content/help/tr/tr/document-cloud/digital-identity/bankid-sw.html

Boyatzis, R. E. (1998). *Transforming Qualitative Information*. Sage Publications, Inc. https://us.sagepub.com/en-us/nam/transforming-qualitative-information/book7714

Ceyhan, E. B., Ceyhan, İ. F., Demiryürek, E., & Bodur, R. (2018). Akıllı Kimlik Kartlarının Finansal İşlemlerde Kullanımı: Olası Güvenlik Tehditleri Ve Alınacak Önlemler. *Uluslararası Yönetim İktisat Ve İşletme Dergisi*, *14*(3), 745-760. https://doi.org/10.17130/ijmeb.2018343121

Chen, Y., Chen, W., Guo, D., & Wong, E. (2007). System Design of Smart Card Application for Tank Truck Conveying Management. *2007 International*

Workshop on Anti-Counterfeiting, Security and Identification (ASID), 398-401. https://doi.org/10.1109/IWASID.2007.373664

Chun-I Fan & Yi-Hui Lin. (2009). Provably Secure Remote Truly Three-Factor Authentication Scheme With Privacy Protection on Biometrics. *IEEE Transactions on Information Forensics and Security*, *4*(4), 933-945. https://doi.org/10.1109/TIFS.2009.2031942

Clauβ, S., Kesdogan, D., & Kölsch, T. (2005). Privacy enhancing identity management: Protection against re-identification and profiling. *Proceedings of the 2005 workshop on Digital identity management*, 84-93. https://doi.org/10.1145/1102486.1102501

Cresswell, J. W. (2013). *Qualitative inquiry & research design choosing among five approaches: C. (BÜTÜN Mesut ve DEMİR Selçuk Beşir, Çev. (Eds.))* (3. Baskı). Siyasal Kitapevi.

Cresswell, J. W. (2015). *Nitel Araştırma Yöntemleri: C. (Çev. M. Bütün ve S. B. Demir)*. Siyasal Kitapevi.

Çalış Duman, M. (2022). Toplum 5.0: İnsan Odaklı Dijital Dönüşüm. *Sosyal Siyaset Konferansları Dergisi / Journal of Social Policy Conferences*, *0*(0), 0-0. https://doi.org/10.26650/jspc.2022.82.1008072

Demirkıran, M. (2014). *Sağlık Bakanlığı'ndaki nitelikli personel devrinin nedenlerine ve önlenmesine yönelik nitel bir çalışma* [Yayımlanmamış Doktora Tezi]. Süleyman Demirel Üniversitesi, Sosyal Bilimler Enstitüsü,Sağlık Kurumları Yönetimi Ana Bilim Dalı.

Djalal, Y. I. (2019). *Çok Amaçlı Akıllı Kimlik Kartı Uygulaması Geliştirilmesi* [Yayımlanmamış Yüksek Lisans Tezi, Erciyes Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Ana Bilim Dalı]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=5C-4PmujovM679McNDhCrg&no=a5qiFrSAENQJOOQdtPwNQg

ECHR. (2024). *ECHR - Homepage of the European Court of Human Rights—ECHR - ECHR / CEDH*. ECHR. https://www.echr.coe.int

Ensonhaber. (2022a, Temmuz 8). *AMD siber saldırıya uğradı*. Ensonhaber. https://www.ensonhaber.com/teknoloji/amd-siber-saldiriya-ugradi

Ensonhaber. (2022b, Aralık 23). *Meta, veri sızıntısı davası için 725 milyon dolar ödeyecek*. Ensonhaber. https://www.ensonhaber.com/teknoloji/meta-veri-sizintisi-davasi-icin-725-milyon-dolar-odeyecek

Eroğlu, Ş. (2018). Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, *35*((2)), 130-153. https://doi.org/10.32600/huefd.439007

GDPR. (2024). *General Data Protection Regulation (GDPR)*. General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-50-gdpr/

Güler, A., Halıcıoğlu, M. B., & Taşğın, S. (2015). *Nitel Araştırma Yöntemleri* (Gözden Geçirilmiş ve Güncellenmiş 2. Baskı). Seçkin Yayıncılık. https://www.seckin.com.tr/kitap/488538757

Hiltz, S., Han, H., & Briller, V. (2003). *Public attitudes towards a national identity smart card: Privacy and security concerns*. https://doi.org/10.1109/HICSS.2003.1174312

ICA. (2024). *ICA | Register Identity Card for 15-year-olds*. ICA. https://www.ica.gov.sg/documents/ic/registration

İBB. (2024). *UYM | Sinyalizasyon*. https://uym.ibb.gov.tr/hizmetler/sinyalizasyon

Jang, W. (2010). Travel Time and Transfer Analysis Using Transit Smart Card Data. *Transportation Research Record: Journal of the Transportation Research Board*, *2144*(1), 142-149. https://doi.org/10.3141/2144-16

Juang, W.-S., Chen, S.-T., & Liaw, H.-T. (2008). Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards. *IEEE Transactions on Industrial Electronics*, *55*(6), 2551-2556. https://doi.org/10.1109/TIE.2008.921677

Karaarslan, E., Koç, S., & Akın, G. (2010). *Vatandaşlık Numarası Bazlı E-devlet Sistemlerinde Kişisel Veri Mahremiyeti Durum Saptaması*. http://acikerisim.mu.edu.tr/xmlui/handle/20.500.12809/10181

Kartopu, S., & Dağcı, A. (2015). Tarihsel Süreçte Ensest Yasakları Ve Dinî Emirler: Mahremiyetin Psiko-Antropolojik Kökenleri Üzerine Bir Değerlendirme. *Akademik Sosyal Araştırmalar Dergisi*, *3*(12), 141-160.

Kişisel Verilerin Korunması Kanunu, 6698 KVKK (2016).

Koç, H. (2021). Dijital Dünyada Yeni Vatandaşlık Konsepti: Estonya'da E-Vatandaşlık Örneği. *OPUS Uluslararası Toplum Araştırmaları Dergisi*, *17*(35), 2254-2289. https://doi.org/10.26466/opus.869773

Kuada, E., Wiafe, I., Addo, D., & Djaba, E. (2017). Privacy enhancing national identification card system. *2017 IEEE AFRICON*, 867-872. https://doi.org/10.1109/AFRCON.2017.8095596

Lim, S. S., Cho, H., & Rivera, M. (2009). Online Privacy, Government Surveillance and National ID Cards. *Commun. ACM*, *52*, 116-120. https://doi.org/10.1145/1610252.1610283

Marks, D. F., & Yardley, L. (2004). *Research Methods for Clinical and Health Psychology*. SAGE Publications, Ltd. https://doi.org/10.4135/9781849209793

Maslow, A. H. (1943). A Theory of Human Motivation. *Psychological Review*, *Vol 50*(4), 379-396.

Merriam, S. B. (2013). *Nitel araştırma: Desen ve uygulama için bir rehber: C. (S. Turan, 3. Bs.'dan Çev. (Edt.))*. Nobel Yayıncılık.

Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, *51*(5), 541-552. https://doi.org/10.1109/TC.2002.1004593

Mutlugün, M., & Adalier, O. (2009). *Turkish national electronic identity card*. 18. https://doi.org/10.1145/1626195.1626201

Neuman, W. L. (2007). *Toplumsal Araştırma Yöntemleri: Nitel ve Nicel Yaklaşımlar, (Cilt I-II): C. (S. Özge, Çev.)* (2. Baskı). https://www.siyasalkitap.com/toplumsal-arastirma-yontemleri-2-cilt-takim

NVGM. (2024a). *Elektronik Kimlik Doğrulama Sistemi (EKDS)*. https://www.nvi.gov.tr/ekds

NVGM. (2024b). *Merkezi Nüfus İdaresi Sistemi (MERNİS)*. https://www.nvi.gov.tr/mernis

NVGM, İ. İ. B. (2024c). *Yeni Kimlik Kartı Başvuruları*. https://www.nvi.gov.tr/istanbul/trkiye-cumhuriyeti-kimlik-karti-projesi

Öktem, M. K., & Aydın, M. D. (2005). Bilgi Teknolojileri Ve Türk Kamu Yönetiminde Dönüşüm. *Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *23*(2), Article 2.

Özbey, R. S. (2006). *Akıllı Kart Teknolojileri*. Ulusal Elektronik İmza Sempozyumu, Ankara.

Özdenizci, B., Ok, K., Aydın, M. N., & Coşkun, V. (2016). Yakın Alan İletişimi Teknolojisi. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, *4*(1), Article 1.

Padem, H., Göksu, A., & Konaklı, Z. (2012). *Araştırma Yöntemleri. SPSS Uygulamalı*. International Burch University.

Paşaoğlu, C., Güler, H., & Jafari, M. (2019). Ağ Tabanlı Veri Sızıntısı Tespiti Ve Önlenmesi Üzerine Bir İnceleme. *Uluslararası Yönetim BiliGim Sistemleri ve Bilgisayar Bilimleri Dergisi*, *3*(2), 79-92.

Patton, M. Q. (2018). *Nitel Araştırma ve Değerlendirme Yöntemleri: C. (Çev. M. Bütün, S. B. Demir)* (2. Baskı). Pegem Akademi.

Savronik. (2024). *Trafik Kontrol Sistemleri*. Savronik. https://www.savronik.com.tr/cozumlerimiz/akilli-ulasim-sistemleri/trafik-kontrol-sistemleri/

SCSoft. (2024). NFC İle Kimlik Doğrulama. *SCSoft Bilişim Teknolojileri*. https://www.scsoft.com.tr/urun/nfc-dogrulama/

SecroMix. (2024). *NFC Nedir? Neden NFC'ye Yatırım Yapmalısınız? – SecroMix*. https://secromix.com/blog/nfc-nedir-neden-nfcye-yatirim-yapmali/

Seggie, F. N., & Bayyurt, Y. (2015). *Nitel Araştırma Yöntem,Teknik,Analiz ve Yaklaşımları*. Anı Yayıncılık.

Singh, P. K., Kumar, N., & Gupta, B. K. (2018). Smart Card ID: An Evolving and Viable Technology. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *9*(3), Article 3. https://doi.org/10.14569/IJACSA.2018.090318

Şanslı, A. (2007). *Akıllı Kimlik Kartı Uygulaması* [Yayımlanmamış Yüksek Lisans Tezi]. T.C. Sakarya Üniversitesi, Fen Bilimleri Fakültesi, Bilgisayar ve Bilişim Mühendisliği Enstitüsü,.

Taherdoost, H. (2017). Appraising the Smart Card Technology Adoption; Case of Application in University Environment. *Procedia Engineering*, *181*, 1049-1057. https://doi.org/10.1016/j.proeng.2017.02.506

T.C. DışişleriBakanlığı. (2024). *Birleşmiş Milletler Teşkilatı ve Türkiye*. https://www.mfa.gov.tr/birlesmis-milletler-teskilati-ve-turkiye.tr.mfa

Teeluckdharry, G. D. (2022). *Saying NO To Biometrics*. https://www.academia.edu/84175063/Saying_NO_To_Biometrics

Tiri, K., & Verbauwhede, I. (2003). *Securing encryption algorithms against DPA at the logic level: Next generation smart card technology*. 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2003), COLOGNE, GERMANY.

TÜBİTAK-UEKAE. (2006). *E-dönüşüm Türkiye Projesi 2005 Eylem Planı 6. Eylem Maddesi "Akıllı kartların kamuda kullanımı" Konusunda Ön Çalışma Raporu.*

Türkiye. (2022, Temmuz 5). *Tarihe geçecek veri ihlali: 1 milyar Çinlinin kişisel bilgileri ele geçirildi*. Türkiye Gazetesi. https://arsiv.turkiyegazetesi.com.tr/teknoloji/tarihe-gececek-veri-ihlali-1-milyar-cinlinin-kisisel-bilgileri-ele-gecirildi-881031

UIDAI. (2024). *Https://uidai.gov.in/en/*. Unique Identification Authority of India | Government of India. https://uidai.gov.in/en/

UN. (2024). *The United Nations*. United Nations; United Nations. https://www.un.org/en/about-us

Vardi, R. (2015). Sanal Mahremiyet. *Toplum Bilimleri Dergisi*, *Ocak-Haziran*(9(17)), 53-73.

wikipedia. (2024a). National identity card (Sweden). İçinde *Wikipedia*. https://en.wikipedia.org/w/index.php?title=National_identity_card_(Sweden)&oldid=1211779330

wikipedia, a. (2024b). Norwegian identity card. İçinde *Vikipedi*. https://en.wikipedia.org/w/index.php?title=Norwegian_identity_card&oldid=1217614594

Yeow, P., Yuen, Y., & Loo, wee hong. (2012). Ergonomics issues in national identity card for homeland security. *Applied ergonomics*, *44*. https://doi.org/10.1016/j.apergo.2012.04.017

Yıldırım, A. (1999). Nitel Araştırma Yöntemlerinin Temel Özellikleri ve Eğitim Araştırmalarındaki Yeri ve Önemi. *Eğitim ve Bilim*, *23*(112). https://eb.ted.org.tr/index.php/EB/article/view/5326

Yıldırım, A., & Şimşek, H. (2021). *Nitel Araştırma Yöntemleri* (12. Baskı). Seçkin Yayıncılık. https://www.seckin.com.tr/kitap/176755156

Yıldız, S. (2007). Kimlik ve Ulusal Kimlik Kavramlarının Toplumsal Niteliği. *Millî Folklor*, *19*, 9-16.

Yılmaz, G., Müngen, A., Önün, F., & Çınar, A. (2014). *NFC Tabanlı Akıllı Alışveriş Sistemi*. https://ab.org.tr/ab14/kitap/yilmaz_mungen_ab14.pdf

Yüksel, M. (2003). Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi. *Ankara Üniversitesi SBF Dergisi*, *58*(1), 182-213.

Yüksel-Civelek, D. (2011). *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi* [Uzmanlık Tezi]. T.C. Başbakanlık Devlet Planlama Teşkilatı Müşteşarlığı.

EK

EK 1. Yarı Yapılandırılmış Görüşme Formu

Değerli Katılımcı,

Bu görüşmenin temel amacı, akıllı kimlik kartlarına yönelik bireysel güvenlik ve mahremiyet algılarının tespit edilmesidir.

Katılımınız tamamen gönüllülük esasına dayanmaktadır. Bu araştırmada toplanacak olan veriler, yalnızca akademik ve bilimsel amaçlar için değerlendirilecektir. Bu çerçevede, bilgilerinizin gizliliği esastır ve kesinlikle korunacaktır. Bu nedenle, yanıtlarınızda isim ve kimlik bilgilerinizi belirtmenize gerek yoktur. Araştırmanın güvenilirliği ve doğruluğu açısından, sorulan sorulara samimi ve doğru yanıtlar vermeniz büyük önem arz etmektedir.

Katılımınız ve içten yanıtlarınız için şimdiden teşekkür eder, bu bilimsel çalışmanın önemli bir parçası olduğunuzu belirtmek isteriz.

A) DEMOGRAFİK BİLGİLER FORMU

1	**Cinsiyetiniz**	( ) Kadın	( ) Erkek	
2	**Yaşınız**	( ) 18-25	( ) 26-33	
		( ) 34- 41	( ) 42 ve üstü	
3	**Mesleki Kıdem Süreniz**	( ) 1-5 yıl	( ) 6-10 yıl	( ) 11-15 yıl
		( ) 16-20 yıl	( ) 21-25 yıl	( ) 25 yıl ve üzeri
4	**Eğitim Durumunuz**	( ) İlköğretim	( ) Lise	( ) Ön lisans
		( ) Lisans	( ) Yüksek Lisans	( ) Doktora
5	**Medeni Durumunuz**	( ) Bekar	( ) Evli	
6	**Çalıştığınız Kurum**	( ) Özel Sektör	( ) Kamu	( ) Çalışmıyor

B) AKILLI KİMLİK KARTLARI İLE İLGİLİ GÜVENLİK VE MAHREMİYET GÖRÜŞLERİNİN İNCELENMESİNE YÖNELİK YARI YAPILANDIRILMIŞ GÖRÜŞME SORULARI

1. Akıllı kimlik kartları hakkında genel görüşleriniz nelerdir?
Yanıtınız

2. Akıllı kimlik kartınızı ne sıklıkla kullanıyorsunuz?
Yanıtınız

3. Akıllı kimlik kartınızı kullanırken kişisel verilerinizi koruma konusunda ne kadar bilinçli olduğunuzu düşünüyorsunuz?
Yanıtınız

4. Akıllı kimlik kartınızın mahremiyetinizi koruma konusundaki güvenlik önlemlerini ne kadar etkili buluyorsunuz?
Yanıtınız

5. Akıllı kimlik kartınızın kaybolması veya çalınması durumunda kişisel güvenliğiniz açısından ne derece sorun yaratacağını düşünüyorsunuz?
Yanıtınız

6. Akıllı kimlik kartınızı kullanırken kişisel bilgilerinize yetkisiz erişimi engellemek için özel önlemler alıyor musunuz?
Yanıtınız

7. Akıllı kimlik kartı kullanımına ilişkin güvenlik ve mahremiyet konularıyla ilgili herhangi bir resmi bilgilendirme yapıldı mı?
Yanıtınız

8. Akıllı kimlik kartlarının mahremiyetle ilgili olan endişeleri azaltmak için ne tür önlemler alınabilir?
Yanıtınız

9. Akıllı kimlik kartlarınız kullanırken kişisel verilerinizin güvende olduğunu düşünüyor musunuz?
Yanıtınız

10. Akıllı kimlik kartlarının kullanımı sırasında kişisel verilerin izinsiz erişime karşı korunması hakkındaki düşünceniz nedir?
Yanıtınız

11. Akıllı kimlik kartlarının çevrimiçi kullanımı esnasında verinizin korunması için neler yapılabilir?
Yanıtınız

12. Akıllı kimlik kartlarının izleme veya takip edilme olasılığı hakkında ne düşünüyorsunuz?
Yanıtınız

13. Akıllı kimlik kartı mahremiyet bilgilerinizin (dini bilgi, medeniyet durumu, vb.) tehlikede olup olmadığı hakkında ne düşünüyorsunuz?
Yanıtınız

14. Akıllı kimlik kartlarındaki bilgilerinizin özel hayattaki mahremiyetinizi ihlal edip etmeyeceği hakkında ne düşünüyorsunuz?
Yanıtınız

15. Akıllı kimlik kartları ile ilgili bunların dışında eklemek istediğiniz görüş ve önerileriniz nelerdir?
Yanıtınız

ÖZGEÇMİŞ

Ad Soyad: Nesibe Mahur ŞAHİN	
Eğitim Bilgileri	
Lisans	
Üniversite	Kahramanmaraş Sütçü İmam Üniversitesi
Fakülte	İktisadi ve İdari Bilimler Fakültesi
Bölümü	Kamu Yönetimi
Makale ve Bildiriler	
1.Yıldırım, A. & Şahin, N.M. (2024, Mayıs 11-12). Akıllı Kimlik Kartlarının Güvenlik ve Mahremiyet Açısından İncelenmesi: Karaman İli Örneği, *Uluslararası Sosyal Bilimlerde Yeni Ufuklar Kongresi (INCOHIS 2024 SPRING)*	