İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BANKA KREDİ KARTI SÜREÇLERİNDE KİŞİSEL VERİLERİN BÜYÜK VERİ YÖNTEMLERİ İLE GİZLİLİĞİNİN KORUNMASI

YÜKSEK LİSANS TEZİ

Mahbub Dilan Koyuncu Kaya

Bilişim Uygulamaları Anabilim Dalı
Bilgi Güvenliği Mühendisliği ve Kriptografi

ŞUBAT 2024

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BANKA KREDİ KARTI SÜREÇLERİNDE KİŞİSEL VERİLERİN BÜYÜK VERİ YÖNTEMLERİ İLE GİZLİLİĞİNİN KORUNMASI

YÜKSEK LİSANS TEZİ

Mahbub Dilan KOYUNCU KAYA
(707211006)

Bilişim Uygulamaları Anabilim Dalı
Bilgi Güvenliği Mühendisliği ve Kriptografi

Tez Danışmanı: Prof. Dr. Enver ÖZDEMİR

ŞUBAT 2024

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

PRIVACY AND USE OF BIG DATA IN BANK CREDIT CARD PROCESSES

M.Sc.THESIS

Mahbub Dilan KOYUNCU KAYA
(707211006)

Applied Informatics Department
Cyber Security Engineering and Crptography

Thesis Advisor: Prof. Dr. Enver ÖZDEMİR

FEBRUARY 2024

İTÜ, Lisansüstü Eğitim Enstitüsü'nün 707211006 numaralı Yüksek Lisans Öğrencisi Mahbub Dilan KOYUNCU KAYA, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "BANKA KREDİ KARTI SÜREÇLERİNDE KİŞİSEL VERİLERİN BÜYÜK VERİ YÖNTEMLERİ İLE GİZLİLİĞİNİN KORUNMASI" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Prof. Dr. Enver ÖZDEMİR** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Prof. Dr. Enver ÖZDEMİR** İstanbul Teknik Üniversitesi	.....
	Doç. Dr. Ergün YARANERİ İstanbul Teknik Üniversitesi	.....
	Dr. Öğr. Üyesi Neslihan Ayşen OZBAY Ankara Bilim Üniversitesi	.....

Teslim Tarihi : 05 Ocak 2024
Savunma Tarihi : 02 Şubat 2024

Eşim İlhan KAYA ve Banka Emekçilerine,

ÖNSÖZ

Araştırmamıza konu fikrin ilham kaynağı olan değerli hocam Prof. Dr. Enver ÖZDEMİR öncülüğünde başladığımız çalışmamız için beni her koşulda destekleyen Bilgisayar Mühendisi İlhan KAYA'ya, bankacılık sektörünün değerli emekçilerine ve yüksek lisans süresince desteklerini esirgemeyen Vakıfbank Teftiş Kurulu'na ayrı ayrı teşekkürü borç bilirim.

Şubat 2024

Mahbub Dilan KOYUNCU KAYA
Vakıfbank Baş Müfettişi

İÇİNDEKİLER

Sayfa

KISALTMALAR

KVKK : Kişisel Verileri Koruma Kanunu
BKM : Bankalararası Kart Merkezi
EDI : Elektronik Veri Değişimi
GDPR : General Data Protection Regulation
POS : Point of Sales
KKB : Kredi Kayıt Bürosu
BDDK : Bankacılık Denetleme ve Düzenleme Kurulu
LKS : Limit Kontrol Sistemi
PSD : Payment Service Direction
SCA : Strong Customer Authentication
CFPB : Tüketici Mali Koruma Bürosu
SSL : Secure Socket Layer
TLS : Transport Layer Security

ŞEKİL LİSTESİ

Sayfa

BANKA KREDİ KARTI SÜREÇLERİNDE KİŞİSEL VERİLERİN BÜYÜK VERİ YÖNTEMLERİ İLE GİZLİLİĞİNİN KORUNMASI

ÖZET

Alışveriş kavramı tarihin ilk çağlarından beri insanoğlunun hayatının merkezinde yer almış, yerleşik hayata geçilerek medenileşme süreçlerine ön ayak olmuş, esasında şu anki medeniyetlerin oluşmasında büyük bir katkısı olan kavramlardan biri olarak karşımıza çıkmıştır. Alışveriş kavramı teknolojinin hızla gelişmesi ile fiziki dünyadan sanal dünyaya taşınmış, e-ticaret, alışveriş siteleri, kripto paralar, kredi kartları vb. kavramlar daha çok duyulmaya başlanmış, 2020 yılında tüm Dünyayı sarsan koronavirüs sebebi ile de sanal alışveriş en üst sınırlarına ulaşmıştır.

Meydana gelen teknolojik gelişmeler bahsi geçen sanal alışveriş kavramını iyice büyütmüş, alışverişte bulunan tüm aktörlerin teknolojik gelişmelere ayak uydurması gerekliliği ortaya çıkmıştır. Bu aktörlerden en büyüklerinden biri olan bankalar teknolojik gelişmelerin hızına yetişmek maksadıyla kredi kartı satış hacimlerini büyütmüş, milyonlara ulaşan müşterilere ulaşmıştır. Fakat her büyüyen ve gelişen sektör gibi bu sektörün de karşılaştığı sanal saldırılar (virüsler, zararlı yazılımlar, hackerler vb.) ve iç saldırılarda (çalışanların bilgi sızdırması vb.) artmış ve bu saldırılardan en çok zarar gören kısmın müşterilere ait kişisel veriler olduğu görülmüştür. Bu minvalde müşterileri korumak maksadıyla Dünya genelinde bazı önlemler alınması gerekmiştir. Avrupa da General Data Protection Regulation adı verilen bankaların yanında, tüm kişisel veri işleyen, saklayan kurum kuruluşların tabi olduğu yasalar oluşturulmuş, bu yasanın Türkiye'ye yansıması da Kişisel Verileri Koruma Kanunu adı verilen (KVKK) uygulaması olmuştur. Bu yasaların uygulamasının yapılabilmesi için yönetmelikler ve iyi uygulama rehberleri hazırlanmış, ilgili kanun ve uygulamalara uyum zorunlu tutularak, tüm kişisel veri işleyen saklayan kurumların özenli davranmaya sebebiyet vermiştir. Bu tip idari önlemlerin yanı sıra teknik önlemlerin alınması da gerekmiş, bu teknik önlemler için belirli dönemler için gözden geçirmelerin eklenmesi sağlanmıştır. Alınan hem idari hem de teknik önlemlerin bankacılık sektörü başta olmak üzere veri saklayan ve veri işleyen diğer sektörlerde de büyük ölçüde anlamlı olduğu fakat, ölçülemeyen birtakım faktörlerin önleminin alınamadığı görülmüştür. Bu faktörlerden en büyüğü ise kurum çalışanlarının içinde bulunduğu insan faktörüdür. Son yıllardaki veri sızıntıları araştırıldığında, en büyük oranın çalışanların verileri maddi kazanç karşılığında kurum dışına çıkarması olarak görülmektedir. Her ne kadar idari ve teknik önlemler alınsa dahi veri sızıntısının tam olarak önüne geçilemediği görülmektedir. Bu noktada en iyi çözümün temin edilen kişisel verinin azaltılması olacağı su götürmez bir gerçektir. Konusu Banka Kredi Kartı Süreçlerinde Kişisel Verilerin Büyük Veri Yöntemleri İle Gizliliğinin Korunması olan tezimiz içerisinde, teknolojik gelişmeler, yaşanılan dijital dönüşüm ve müşteri alışkanlıkları bankacılık sektöründe sıklıkla kullanılan kredi kartlarını baz alarak bankaların kişisel veri kavramını, bu verilerin müşterilerden temin edildiği kredi kartı başvuru sürecinden, kredi kartından yapılan harcamanın ödendiği

sürecin tamamında bankalarca yapılan işlemleri, Türkiye'de ve Dünyada yürürlükte olan kişisel veri koruma yasaları, bunların kredi kartı ile ilgili maddeleri, bankalarca alınan idari ve teknik önlemler hakkında bilgi verilmeye çalışılmıştır. Bahsi gecen idari ve teknik önlemlerin yeterli olmadığı durumlara da yer verilmiş, hangi yöntemler ile verilerin sızdırıldığı, sızdırılan verilerin daha çok pazarlama ve maddi kazanç sağlama amacıyla kullanıldığı istatistikler ve basına yansımış haberler, KVKK`nin bildiri sayfası kullanılarak gösterilmeye çalışılmıştır.

Tez konusuna da ilham veren, KVKK`nin bildiri sayfasında örneğine rastlanan bankaların kredi kartı sahibi müşterilerinin hesap özeti bilgilerini e-posta adreslerinde meydana gelen karışıklık sebebi ile üçüncü kişilerle sehven paylaşabildiği görülmüş, bu bilgi ışığında 5 farklı müşterinin 2 farklı bankaya ait 2021 Haziran-2023 Haziran dönemi için alınan kredi kartı hesap özetleri ile basit bir analiz yapılmaya çalışılmış, KVKK kısıtlamaları, müşterilerin özel hayatlarını paylaşmak istememesi sebebi ile sadece 5 farklı müşterinin 2 yıllık hesap özetlerinin temin edildiği, söz konusu verinin örneklem anlamında yeterli olmadığı kanaatine varılarak, SQL dili kullanılarak mevcut 5 müşteri üzerinden yapay 100 müşteri oluşturulmuş ve analiz üretilen 100 müşteri üzerinden tekrarlanmıştır. Basit bir analiz ile gerçekleştirilen işbu çalışmanın sonuçları değerlendirildiğinde, yalnızca müşterilerin hesap özetlerine bakılarak (yaptıkları harcamalar) cinsiyetleri, gelir bilgisi aralığı, çalışılan isin özellikleri, yaşanılan ülke, şehir bilgisi, sağlık geçmişi, madde, sigara veyahut alkol kullanımı, mezun olunan okul bilgisi, müşterinin kişisel mal varlığı bilgisi (araba, ev) vb. hakkında tahminde bulunabildiği görülmüştür. Bu durumun özellikle bankacılık sektörü ile çalışan, ürün satışında öne geçmeyi arzulayan üçüncü taraf kişi ve kurumlar tarafından ne kadar iştah acıcı olduğu anlaşılabilir. Bu tehlikeyi bertaraf etmek, kişisel verilerin üçüncü tarafların eline geçmesini önlemek maksadı ile neler yapılacağı araştırılmış hem anonimlik hem de banka işlemlerinde kimlik doğrulamasının yapılmasını sağlayacak hibrit grup kimlik doğrulama sisteminin var olduğu görülmüş ve öneri olarak bu sistemin bankacılık sektörü ve veri işleyen, saklayan tüm kurum ve kuruluşlara verilmiştir.

PRIVACY AND USE OF BIG DATA IN BANK CREDIT CARD PROCESSES

SUMMARY

The concept of shopping has been at the center of human life since the early ages of history, it has initiated the civilization processes through the transition to settled life, and in fact, it has emerged as one of the concepts that made a great contribution to the formation of current civilizations. With the rapid development of technology, the concept of shopping has moved from the physical world to the virtual world, ecommerce, shopping sites, cryptocurrencies, credit cards, etc. concepts are starting to be heard more. Due to the coronavirus that shook the whole world in 2020, virtual shopping has reached its highest limits.

The technological developments that have occurred have greatly expanded the concept of virtual shopping, and the necessity for all actors involved in shopping to keep up with technological developments has emerged. Banks, one of the largest of these actors, have increased their credit card sales volumes and reached millions of customers in order to keep up with the pace of technological developments. However, like every growing and developing sector, the virtual attacks (viruses, malware, hackers, etc.) and internal attacks (employees leaking information, etc.) faced by this sector have increased and it has been observed that the part that is most damaged by these attacks is the personal data of the customers. In this regard, some precautions had to be taken around the world in order to protect customers. In Europe, laws called General Data Protection Regulation, which are subject to banks as well as all institutions that process and store personal data, have been created, and the reflection of this law in Turkey is the so-called Personal Data Protection Law (KVKK). In order to implement these laws, regulations and good practice guides have been prepared, and compliance with the relevant laws and practices has been made mandatory, causing all institutions that process and store personal data to act carefully. In addition to such administrative measures, technical measures also had to be taken, and these technical measures were required for certain periods. It has been observed that both administrative and technical measures taken are largely significant in the banking sector and other sectors that store and process data, but some unmeasurable factors cannot be taken into account. The biggest human factor among these factors is the employees of the institution. When data leaks in recent years are investigated, the largest rate is seen as employees leaving the organization's data in exchange for financial gain. Even though administrative and technical measures are taken, it is seen that data leakage cannot be completely prevented. At this point, it is an undeniable fact that the best solution would be to reduce the personal data provided.

Protecting the personal information of customers trading in financial markets is important in increasing the reliability of both the banking system and existing financial markets, in increasing compliance with global laws, in preventing all kinds of abuse using customer information, in protecting the brand value of financial markets, in protecting financial market actors as a result of the acquisition of personal data. It will

make a great contribution to reducing data storage and security costs. With the developing technological developments, it can be seen that blockchain-based studies that aim to minimize the personal information of the customers in question have begun to be used. The most striking cases can be observed that the personal data used in the banking sector is used not only for the transactions to be made by the customers, but also for marketing purposes by the bank through the analyzes obtained from this data, and even these data are shared with third parties. From this situation, it can be clearly seen how important the use of blockchain-based technologies in the banking sector is in terms of speed, efficiency, transparency and reliability. In the thesis, the figures for the use of credit cards in the banking sector, especially in the world and in Turkey, are given, how high the usage rates are, examining the personal data that banks receive from customers in credit card use in terms of quality and quantity, the laws and rules for the protection of personal data in the world and Turkey. Practices, compliance with these laws and rules, abusive transactions, especially the sharing of customers' personal data with third parties by bank employees have been revealed. As a result, the results obtained in a very short time from the artificial data created with the data received from the customers are an important beginning in terms of showing the level that these data will reach by using more comprehensive and purposeful technological tools.

With the development of technology, e-commerce transactions and, in parallel, credit cards, the use of which has increased considerably in e-commerce transactions, whether private life information and spending habits information of the relevant customers can be accessed through the statements showing the expenditures made within a certain period of time sent to the customers or not, and personal information can be obtained with this information. It has been tested whether marketing techniques can be presented and whether this information will lead to abusive situations. It is clear that when it becomes possible for banks and third parties to use the information obtained only through credit card expenditures of individual customers in the financial world, there will be a problem related to the diversity of personal data that needs to be solved and the inability to protect this data, and the development of a system to solve this problem will be inevitable. At this point, my thesis will provide guidance on how to create a financial system by minimizing the use of personal data.

The fact that technological developments are advancing incredibly means that the risks for the banking sector and the e-commerce sector, which grow and develop with technology in the world in Turkey, are increasing. For this risk, there is a worldwide rule to practice on the security of risks in the personal data layer, entering the security data. In Turkey, the Personal Data Protection Law was created in response to the General Data Protection Regulation, and for the credit card, which we focus on in our work, the Banking and Credit Card Law were created and related regulations. The adoption of such administrative measures serves as a preventive measure against the loss of personal data. Furthermore, banks and e-commerce sites have adopted technical measures relating to virus protection, network security and how data is recorded and destroyed. However, as explained in the previous sections of our work, despite the precautionary measures taken, it is not possible to prevent data leaks, especially from employees, and completely protect yourself from social engineering. For this reason, it was proposed to reduce the type and number of personal data collected from customers, to guarantee anonymity using group authentication and to use identity verification systems.

It is important to see that e-commerce applications have replaced traditional commerce both globally and in Turkey, and credit cards are an element that accelerates and nourishes the use of e-commerce. As can be noted, it can be said that both the use of credit cards and the development of e-commerce concepts are explained in the best scenario under normal conditions, in a sterile environment without any external forces or dangerous situations. In fact, it is a great need to state that this development process in the real financial market encountered major problems, and although some of these problems were solved, a significant part of them was ignored. It would be an optimistic judgment to say that the actors in the financial markets, namely banks, commercial enterprises, and lastly and most importantly, individuals, always make the right decisions and make financial market movements without considering undeserved interests. Especially in recent years, identity fraud and identity forgery transactions, especially data leaks, have become widespread in financial markets, there are problems in eliminating internal and external attacks occurring in banks, technology companies and even government institutions, and commercial enterprises engaged in e-commerce do not have sufficient technology security infrastructures. It appears that it cannot be provided. Various practices, laws and rules have begun to be implemented around the world to solve these problems. In particular, the protection of the security infrastructures of e-commerce sites with SSL certificates, the use of 3D Secure methods at the time of payment, the security standards used to process credit cards of major card brands called PCI DSS Payment Card Industry Data Security Standard. When taken into consideration, the existing protection methods are effective for individual/commercial use in the financial market. It will be seen that it aims to protect the information that all customers share with financial organizations (banks, government institutions, e-commerce sites).

In our thesis, the subject of which is PRIVACY AND USE OF BIG DATA IN BANK CREDIT CARD PROCESSES, technological developments, digital transformation and customer habits are based on the credit cards that are frequently used in the banking sector. An attempt has been made to provide information about the transactions made by the Banks during the entire payment process, the personal data protection laws in force in Turkey and the World, their credit card-related articles, and the administrative and technical measures taken by the Banks. Situations where the mentioned administrative and technical measures are not sufficient are also included, and the methods by which the data is leaked, the statistics and the news reflected in the press, where the leaked data is used for marketing and financial gain purposes, are tried to be shown using the KVKK's notification page. It has been seen that the bank's credit card holder customers' account statement information can be accidentally shared with third parties due to the confusion in their e-mail addresses, an example of which is found on the notification page of KVKK, which inspired the subject of the thesis. In the light of this information, 2021 June 2023 accounts of 5 different customers belonging to 2 different banks A simple analysis was attempted with the credit card account statements received for the June period. Due to KVKK restrictions and customers not wanting to share their private lives, 2-year account statements of only 5 different customers were provided, and it was concluded that the data in question was not sufficient in terms of sample, and it was available using SQL language. An artificial 100 customers were created out of 5 customers and the analysis was repeated on the 100 generated customers. When the results of this study, which was carried out with a simple analysis, are evaluated, only by looking at the account statements of the customers (their expenditures), their gender, income information range, characteristics of the job they work in, country of residence, city information, health history,

substance, cigarette or alcohol use, information about the school they graduated from, It has been observed that the customer can make predictions about asset information (car, house), etc. It can be understood how distressing this situation is, especially for third party individuals and institutions working with the banking sector and wishing to get ahead in product sales. In order to eliminate this danger and prevent personal data from falling into the hands of third parties, it was researched what to do, it was seen that there was a hybrid group authentication system that would provide both anonymity and authentication in bank transactions, and as a recommendation, this system was used in the banking sector and all institutions that process and store data and given to organizations.

1. GİRİŞ

İnsanoğlu dünya üzerindeki mevcudiyetinden itibaren uhdesinde bulunmayan malların ihtiyaç olan mallarla takas edilmesini sağlayarak ticarete ilk adımını atmıştır. Başlarda bu değiş tokuş sadece yiyeceklerle sınırlıyken ilerleyen zamanlarda giyecek, yakıt ve sonunda hizmet değiş tokuşuna kadar gelmiştir. Takas ekonomisi olarak adlandırılan bu ekonomik iletişimin öznesini oluşturan mal ve hizmetlerin değişiminde mal ve hizmetin taşınamaması verilen mal ile alınacak malın değerinin tam olarak belirlenememesi vb. meydana gelen zorlukların çözümü paranın bulunması ile sona ermiştir.

M.Ö. 7. yüzyılda Lidyalılar döneminde Anadolu topraklarında bulunan madeni paranın özellikle ticaret alanında gelişmiş bir kavim olan Lidyalılar tarafından bulunması şaşırılmayacak bir durumdur. Paranın bulunması ile takas ekonomisinin yerini para ekonomisi almıştır. Paranın bulunması ile ticaretin coğrafi alanı genişlemiş, dünyanın bir ucundan diğer ucuna mal ve hizmet götürülmesi, böylece medeniyetin ve küreselleşmenin ilk atılması sağlanmıştır. Bunun yanı sıra bir mal ve hizmetin değerinin ölçülmesi, kapital ekonomilerin gelişmesi, bankacılık sistemi ve dolayısıyla ekonomik gelişmelere bağlı olarak toplumlar ve devletler meydana gelmiştir. Nakit para olarak adlandırılan yukarıda da bahsedilen değiş tokuş yerine farklı ve etkili başka bir aracın gün yüzüne çıkması ise bankacılık sistemi, teknolojik gelişmeler ile bağlantılı olarak 1950'li yıllarda Diners Club tarafından çıkarılan bir tür sadakat kart olarak da görülebilecek müşteriler için oluşturulmuş para yerine geçen kartlar ile sağlanmıştır. Zamanla önce American Express Card, Visa Inc.ve MasterCard ile dünya genelinde kullanılabilecek, para yerine işlem yapılan bir ödeme aracı olan kredi kartının inşasına şahit olunmuştur (Forbes Advisor, 2021). Bankalararası Kart Merkezi (BKM) kuruluşu tarafından verilen istatistiklere göre Türkiye'de 2023 yılının mayıs ayı sonunda 107,1 milyon adet kredi kartı kullanıldığı 2022 yılının mayıs ayı ile kıyaslandığında kredi kart adedinde yüzde 19’luk bir artışın olduğu görülmüştür. Bunun yanı sıra 2023 yılının mayıs ayında 507,7 milyar TL ödemenin kredi kartları ile gerçekleştirildiği görülmüştür (Bankalararası Kart Merkezi, 2023). Dünya

istatistiklerine bakıldığında ise Dünya çapında kredi kartı sahiplerinin sayısı istikrarlı bir şekilde artarak 2023'te 1,25 milyara ulaştığı, 2018'deki 1,1 milyardan yıllık %2,79'luk bir büyümenin mevcut olduğu görülmüştür (Clearly Payments, 2023). Buartışın sebepleri incelendiğinde e-ticaretin bu artışta büyük bir sorumluluğunun olduğu görülmüş, özellikle 2020 yılında başlayan korona virüs salgını ile alışveriş için evden dışarı çıkamayan insanlar için e-ticaret adeta bir yardım eline dönüşmüştür. İnternetin dünya üzerindeki kullanımının artması, Elektronik Veri Değişimi (EDI) ve tele-alışveriş gibi ilk teknolojilerin 1970'lerde tanıtılması bugün bildiğimiz modern e-ticaretin ana başlangıç noktası olarak kabul edilebilir. 1991 yılında Amazon, ABD'de ürünleri çevrimiçi satmaya başlayan ilk e-ticaret sitelerinden biri olmakla birlikte, o zamandan beri binlerce işletme e-ticaretin yaygınlaşmasında etkili olmuştur (Miva, 2023). E-ticaretin dünya genelindeki artışını rakamlarla göstermek gerekirse Forbes tarafından yapılan araştırmada 2021 yılında perakende e-ticaret satışlarının dünya çapında tahmini 4,9 trilyon ABD doları olduğu tahmin ediliyor. Sonraki dört yıl içinde bu sayının %56 artarak 2026 yılına kadar yaklaşık 8,1 trilyon dolara ulaşacağı tahmin ediliyor (Statista, 2022). Türkiye özelinde bu istatistiklerin ise dünya istatistiği ile uyumlu olduğu görülebilir. Elektronik Ticaret Bilgi Platformu tarafından belirlenen istatistiklere göre 2019 yılında 381,5 milyon TL e-ticaret işlemi gerçekleştirilmiş, 2022 yılında ise bu tutar 800.7 milyon TL'ye kadar ulaşmıştır (Elektronik Ticaret Bilgi Formu, 2023). E-ticaretin kullanımının bu kadar yaygınlaşması söz konusu olduğunda, e-ticaret işlemlerinin gerçekleştirildiği ödeme araçlarının öneminin de yadsınamayacağı açıktır. E-ticaret uygulamalarında kullanılan ödeme araçları Elektronik Ticaret Bilgi Platformu tarafından belirlenen istatistiklerde kredi ve banka kartları, havale/EFT/ diğer işlemler ve kapıda ödeme olarak ayrılmış, 2021 yılı için toplam 494.947 milyar TL e-ticaret hacminin 227.3 milyar TL tutarındaki kısmının kredi kartları ile yapıldığı, 2022 yılında ise 800.7 milyar TL tutarında e- ticaret 486.7 milyar TL tutarındaki kısmının kredi kart ile yapıldığı görülmüştür (Elektronik Ticaret Bilgi Formu, 2023). Yukarıda tarih boyunca ticaretin gelişimi, kullanılan araçlar, teknolojik gelişmelerle ticaret ve finansal araçlardaki değişiklikler hakkında bilgi verilmiştir. Bu bilgiler ışığında hem küresel mecrada hem de Türkiye'de e-ticaret uygulamalarının geleneksel ticaretin yerini aldığı, kredi kartlarının ise e-ticaretin kullanımını hızlandıran ve besleyen bir unsur olduğunu görmek önemlidir. Dikkat edileceği üzere hem kredi kartı kullanımını hem de e-ticaret kavramlarının gelişiminin normal şartlar altında, steril, herhangi bir dış güç ve tehlikeli bir durumun olmadığı bir

ortam üzerinden en iyi senaryo ile anlatıldığı söylenebilir. Esasında reel finansal pazar içerisinde bu gelişim sürecinin büyük sorunlarla karşılaştığı, busorunların bazıları çözülse de önemli bir kısmının görmezden gelindiğinin belirtilmesi büyük bir ihtiyaçtır. Finansal piyasalar içerisindeki aktörlerin yani bankaların ticari işletmelerin, son ve en önemli olarak bireylerin her zaman doğru kararlar aldığını finansal piyasa hareketlerini hak edilmemiş menfaatler gözetilmeden yaptıklarını söylemek iyimser bir yargı olacaktır. Özellikle son yıllarda finansal piyasalarda başta veri sızıntıları olmak üzere, kimlik dolandırıcılığı, kimlik sahteciliği işlemlerinin yaygınlaştığı, bankalarda, teknoloji firmalarında hatta ve hatta devlet kurumlarında meydana gelen iç ve dış saldırıların bertaraf edilmesinde sorunların olduğu, e-ticaret yapan ticari işletmelerin yeterli teknoloji güvenlik altyapılarını tam olarak sağlayamadığı görülmektedir. Bu sorunların çözümü için dünya genelinde çeşitli uygulamalar, kanunlar, kurallar uygulanmaya başlanmıştır. Özellikle e-ticaret sitelerinin güvenlik altyapılarının SSL sertifikası ile korunması, ödeme anında 3D Secure yöntemlerinin kullanılması, PCI DSS Ödeme Kart Endüstrisi Veri Güvenliği Standard adı verilen büyük kart markalarının kredi kartlarını işlemek için kullanılan güvenlik standartları Avrupa kuruluşları uyumlu olması zorunlu tutulan General Data Protection Regulation (GDPR) adı verilen ve kişisel verilerin korunmasını öncülleyen bir takım kural setleri oluşturulmuştur (European Union, 2016). Dikkat edildiğinde mevcut koruma yöntemlerinin finansal piyasa içerisindeki bireysel/ ticari olsun tüm müşterilerin finansal organizasyonlarla (bankalar, devlet kurumları, e-ticaret siteleri paylaştığı bilgilerin korunması amacını taşıdığı görülecektir. İşbu çalışmamızda mevcut finansal sistem içerisindeki özellikle bankacılık sisteminin bireysel müşterilerden edindiği kişisel veriler, bu verilerin banka içerisinde ve dışarısında pazarlama amacı ile kullanımı, verilerin edinilmesi ve korunmasındaki zorluklar, Türkiye' de ve dünyada meydana gelen kişisel verileri konu alan suiistimal örnekleri ve söz konusu kişisel verilerin baz alınarak kişilerin özel hayatları, tüketim davranışlarının edinebileceği kanıtlanmaya çalışılmış, söz konusu problemin çözümü için blok zincir tabanlı bir sistemin kurularak kişisel verilerin en aza indirilmesi hedeflenmiştir.

1.1 Tezin Amacı

Teknolojinin gelişmesi, e-ticaret işlemlerinin ve buna paralel olarak e-ticaret işlemlerinde kullanımı bir hayli artan kredi kartlarının müşterilere iletilen belirli bir

dönem aralığında yapılan harcamaları gösteren ekstreler üzerinden ilgili müşterilere ait özel hayat bilgileri, harcama alışkanlığı bilgilerine ulaşılıp ulaşılamayacağı, bu bilgiler ile kişiye özel pazarlama tekniklerinin sunulup sunulamayacağı, bu bilgilerin suiistimal içeren durumlara yol açıp açmayacağı test edilmiştir. Bireysel müşterilere ait yalnızca kredi kart harcamaları üzerinden edinilen bilgilerin finansal dünya içerisinde bankalar ve 3. taraflar tarafından kullanılabilirliği mümkün olduğunda çözülmesi gereken kişisel veri çeşitliliği ve bu verinin korunamaması ile ilgili bir problemle karşılaşacağı ve bu problemin çözümü için bir sistemin geliştirilmesinin kaçınılmaz olacağı açıktır. Bu noktada tezimi kişisel veri kullanımının en aza indirgenerek nasıl bir finansal sistemin oluşturulacağı konusunda yol gösterici olacaktır.

1.2 Tezin Özgün Değeri

Finansal piyasalarda işlem yapan müşterilerin kişisel bilgilerinin korunması, hem bankacılık sisteminin hem de mevcut finansal piyasaların güvenilirliğinin artmasında, dünya eksenindeki yasalara uyumun arttırılmasında, müşteri bilgileri kullanılarak yapılacak her türlü suiistimal işleminin önüne geçilmesinde, finansal piyasaların marka değerinin korunmasında, kişisel verilerin edinilmesi sonucu finansal piyasa aktörlerinin yapacakları veri saklama ve güvenlik masraflarının azalmasında büyük katkı sağlayacaktır. Gelişen teknolojik gelişmeler ile söz konusu müşterilere ait kişisel bilgilerin en aza indirilmesini öngören blok zincir tabanlı çalışmaların kullanılmaya başlandığı görülebilir. Özellikle blok zinciri tabanlı sistemlerinin merkezi olmayan yapısı, kullanılan kriptografik anahtarlarının kullanılması fikir birliğini sağlayan bir sistem olması ve böylece şeffaflık ve güvenilirliği sağlaması açısından bankacılık sektöründe kullanılmasının yararlı olacağını göstermektedir (Sakho & Jianbiao, 2019). Bankacılık sektöründe kullanılan kişisel verilerin sadece müşteriler tarafından yapılacak işlemler için değil, banka tarafından bu verilerden elde edilecek analizler ile pazarlama amacı ile kullanıldığı hatta bu verilerin 3. kişiler ile paylaşıldığı en çok dikkat çeken durumlar olarak gözlemlenebilir. Blok zincir tabanlı teknolojilerin bankacılık sektöründe kullanılmasının hız, verimlilik, şeffaflık ve güvenilirlik açısından ne kadar önemli olduğu bu durum üzerinden de net olarak görülebilir. Tez içerisinde bankacılık sektörü içerisinde özellikle kredi kartları kullanımının Dünya ve Türkiye üzerindeki rakamları verilerek kullanım oranlarının ne kadar yüksek

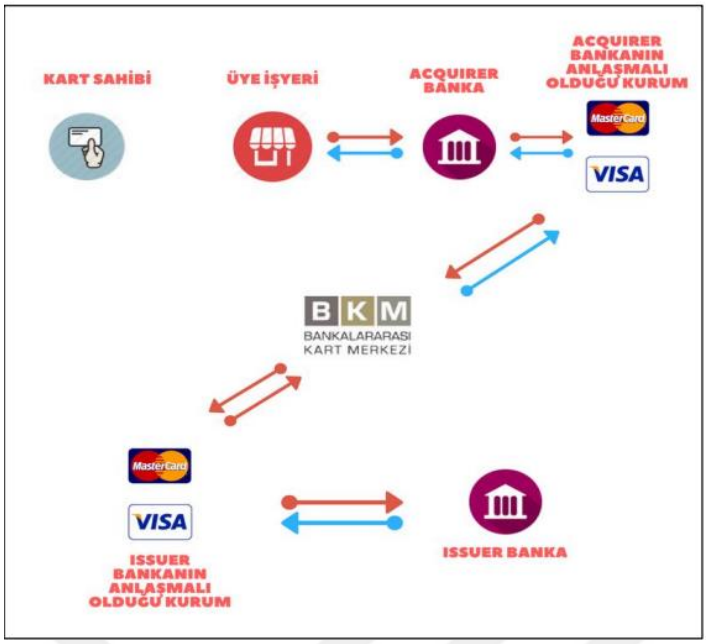
seviyelerde izlediği, bankaların kredi kart kullanımında müşterilerden aldığı kişisel verilerin nitelik ve nicelik bakımından incelenmesi, Dünya ve Türkiye özelinde kişisel verilerin korunması için meydana getirilen kanun ve kuralların uygulamalar, bu kanun ve kurallara uyum durumu ve meydana gelen suiistimal içeren işlemler, özellikle banka çalışanları tarafından 3.taraflarla müşterilerin kişisel verilerinin paylaşılması durumlarının varlığı ortaya çıkarılmıştır. Sonuç olarak müşterilerden alınan veriler ile oluşturulan yapay veri üzerinden çok kısa bir sürede elde edilen sonuçlar bu verilerin daha kapsamlı ve amaca hizmet eden teknolojik araçlar kullanılarak hangi düzeye ulaşacağını göstermesi açısından önemli bir başlangıçtır. Toplamda 5 müşterinin kredi kart hareketleri üzerinden bu kadar kişisel veriye ulaşılabilmesi, bu verileri elinde tutan ve belirli süreler ile de tutmak zorunda olan bankalar tarafından kullanılacak özel araçlar ile nasıl bir pazarlama gücüne sahip olacağı aşikârdır. Tezin öneriler kısmında anlatılan blok zincir tabanlı sistem ile hem bankacılık sektörü üzerindeki şüpheler kalkacak hem de banka müşterileri yapacakları bankacılık işlemlerinde daha güvenli hissedeceklerdir.

2. BANKA KREDİ KARTI SÜREÇLERİ

2.1 Kredi Kartı Tanımı ve Kredi Kartı Süreci

Günümüzde mahallerdeki bakkallardan lüks alışveriş merkezlerine, müzelerden restoranlara alınan hizmetin karşılığında ödenecek ücretin büyük çoğunluğu kredi kartları ile sağlanmaktadır. Özellikle korona virüs salgını sonrası temassız kart modern hayatın bir parçası olmuştur. Kredi kart sahipliklerine bakıldığında 2023 yılı mayıs ayı sonunda Türkiye'de 107,1 milyon adet kredi kartı kullanıldığı, bu rakamın Dünya'da ise 1,25 milyara ulaştığı görülmektedir (Bankalararası Kart Merkezi, 2023). Banka Kartları ve Kredi Kartları Kanununda geçen ibare ile kredi kartı "Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmayan kart numarasını ifade etmektedir." (Banka Kartları ve Kredi Kartları Kanunu, 2006). Bu tanımdan yola çıkıldığında esasen fiziki bir para değiş tokuşu olmadan mal ve hizmet satım alımını sağlayan bir ödeme aracı akla gelmelidir. Günümüzde kredi kartı kullanımını olanaklı kılan en büyük aracı kuruluşlar bankalardır. Bankalar sayesinde bireysel ve ticari müşteriler kendilerine verilen limitler dahilinde kredi kartı çıkarabilmektedirler.

Her ne kadar kredi kartı dünyasındaki tek aktörler müşteriler ve bankalar olarak görülse de bu süreç bir kuruluşlar ve müşteriler arası sistem bütünüdür. Aşağıda Şekil 2.1 Kredi Kartı İş Akış Şeması söz konusu sistemin anlaşılması için önem taşımakta olup bankalar ve müşteriler dışındaki aktörlerin görünmesini kolaylaştıracaktır.



Şekil 2.1: Kredi Kartı İş Akış Şeması

Yukarıdaki şemada da görüleceği üzere kredi kartı iş akış şeması üzerinde kredi kartı müşterisi, müşterinin mal ve hizmet aldığı üye işyeri, acquirer banka (üye işyerinin bankası), inquirer banka (müşterinin bankası), BKM (Bankalararası Takas Merkezi), Kart Sahibi Kuruluşlar (Visa, Mastercard) görülmektedir.

Kredi kartı müşterileri, bir banka yardımı ile alışveriş işlemlerinde nakit yerine kredi kartı kullanmak isteyen ve banka tarafından finansal ve yasal olgunluğa ulaştığı tespit edilmiş kişi ve kuruluştur. Hem bireysel kişilere hem de ticari iş ile iştigal eden kuruluşlara kredi kartı verilebilmektedir. Kredi kartı müşterisi mal veya hizmet alımını gerçekleştireceği üye işyeri (market, AVM, kitapçı vb.) üzerinden ödemesini mevcut kredi kartını kullanarak yapar ve böylece iş akışının ilk işlemini gerçekleştirmiş olur.

Üye İşyeri, ürettiği mal ve hizmeti daha çok müşteriye ulaştırmak için yalnızca nakit değil aynı zamanda kredi kartı ile de satış yapmaya karar veren ve bunun için bir bankaya ihtiyaç duyan kişi veyahut kuruluşlardır. Bankaya başvuru yapan üye işyeri sahibi, bankanın belirlediği bir limit hesabı üzerinden kendisine tahsis edilen POS (Point of Sales) adı verilen müşteri kredi kartı ile işlem yapmaya yarayan bir cihaz edinmektedir. Bu cihaz sayesinde müşterinin aldığı mal veya hizmet karşılığında müşteri kredi kartı limitlerinde eksilme aynı zamanda üye işyeri hesaplarında ise satış işlemi gerçekleşmektedir.

Acquirer Bank (üye işyeri bankası), üye işyeri sahibinin kredi kartı ile mal veya hizmet satışını sağlayan, üye işyerine POS (Point of Sales) cihazını ve satışlarını toplu olarak görebileceği bir limit hesabı tanımlayan banka olarak tanımlanabilir. İlgili banka aynı zamanda yasal otoriteler, kart sahibi kuruluşları ile üye işyeri sahibi yerine işlemleri gerçekleştirmektedir.

Inquirer Bank (kredi kartı müşteri bankası), bireysel ve ticari fark etmeksizin belirli limit ve şartlar dahilinde müşterilerine kredi kartı limit tahsisi yapan, kartı fiziki olarak basılmasını sağlayan, yasal otoriteler ve kart sahibi kuruluşları ile kredi kartı müşterisini temsilen işlemlerde bulunan bankalardır. İlgili bankalar aynı zamanda banka tarafından sunulan seçenekler dahilinde müşteriler tarafından seçilen aylık dönemler içerisinde ilgili kredi kartına ait hesap dökümlerini müşterilere ileterek yapılacak ödemeleri takip etmektedir.

Ödeme Merkez Kuruluşları (BKM-Bankalararası Kart Merkezi), kredi kartları sürecinin sağlıklı yürüyebilmesi, otoritelerin kanun ve kurallarına uyumun sağlanması için hem müşteri ve üye işyeri bankalarıyla hem de kart sahibi kuruluşlar ile ilişkileri yürüten, sistemin güvenli ve hızlı bir şekilde ilerlemesini sağlayan bir merkez olarak tanımlanabilir. Türkiye'de bu görevi yerine getiren kuruluş Bankalararası Kart Merkezi (BKM)'dir. BKM Türkiye'de kredi kartı sistemine dahli bulunan bankaların prosedürleri geliştirmek, standardizasyonu oluşturmak, bankalar arasındaki takas ve hesap işlemlerini sürdürmek, yurtdışı kredi kartı kuruluşları ile iletişimi sağlamakla görevlidir (Bankalararası Kart Merkezi, n.d.).

Kart Sahibi Kuruluşlar (Visa, Mastercard, Troy), kredi kartlarının ön yüzünde amblemi olan, kredi kartının nasıl bir operasyonel işlemi elektronik alt yapıyı takip edeceğinin belirleyen ödeme yöntemi markası olarak tanımlanabilmektedir. Mastercard Amerika Birleşik Devletleri'nde Visa Card ise Birleşik Krallık da kurulmuştur. Aralarında görülebilecek en büyük fark kredi kartının üstünde bulunan kredi kartı numarasının ilk hanesindeki sayıdır (Paratic, 2016). Bu sayı 4 ise Visa Card, 5 ise Mastercard sistemini kullanıyor diyebiliriz. Troy ise Türkiye'de kurulmuş olup, şu an için yalnızca Türkiye'deki ATM ve POS`larda işlem yapılmaktadır (Troy, n.d.).

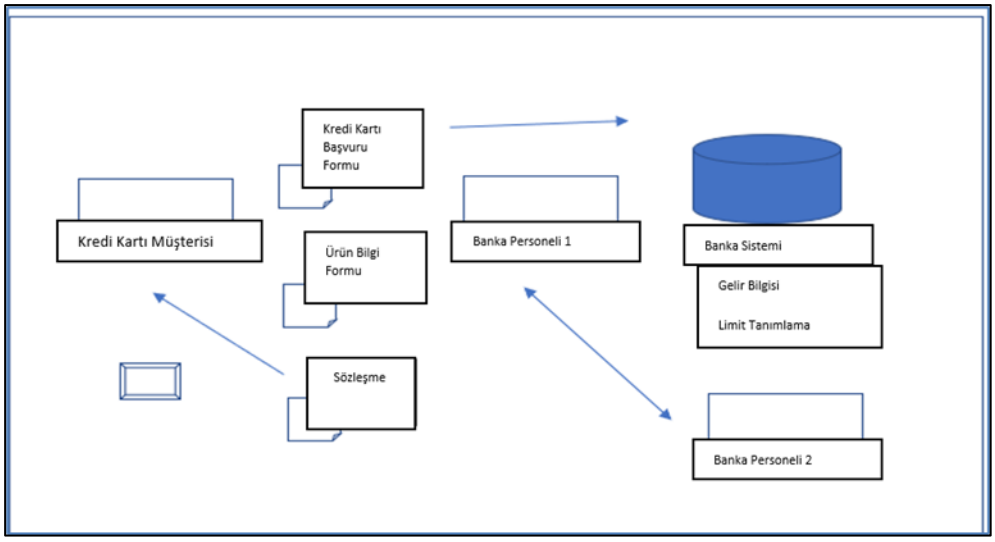
Yukarıda iş akış şeması ve yapılan açıklamalardan da anlaşılacağı üzere; bir kredi kartı süreci bireysel veyahut ticari müşterinin kendi bankası üzerinden kredi kartı temin etmesi, bu kartı üye işyeri kişi kuruluşlardaki mal ve hizmet alımlarında kullanması,

daha sonra üye işyeri ve müşteri bankalarının arasında Bankalararası Ödeme Merkez Kuruluşu sayesinde mutabakat sağlayarak işlemi tamamlaması ile mümkün olmaktadır. Bu iş akışı sürecinin tezimiz amacına hizmet edeceği düşünülen ve ayrıntılı olarak incelenecek kısımları kredi kartı sahibi müşterilerin bankalara olan başvuruları ve kredi kartı kullanımı sonucu meydana gelen hesap hareketleri dökümünün müşterilere ulaştırılmasıdır.

2.2 Başvuru Süreci

Bireysel ve ticari müşteriler kredi kartı ile mal ve hizmet almak istediklerinde banka vasıtası ile işlem yapmak zorundadırlar. Burada kasıt yalnızca banka şubeleri değil, bankaların alternatif dağıtım kanalı olarak adlandırdıkları mobil uygulamalar, internet bankacılığı ve ATM' leri de göz önünde bulundurulmalıdır. Kredi kartı başvuru sürecine değinilirken banka şubelerine fiziken gitmek ve alternatif dağıtım kanalları kullanılarak kredi kartı başvurusunda bulunmak ayrı olarak ele alınmalıdır.

Banka şubesine gelen kredi kartı müşterisinin daha önce ilgili bankanın müşterisi olup olmadığı ilk kırılma noktası olarak karşımıza çıkmaktadır. İlgili müşteri ilk kez ilgili bankanın müşterisi olacak ise kişi için müşteri olma ve akabinde hesap açma süreci işlemektedir. Banka şubeleri üzerinden gerçekleştirilen Kredi Kartı Başvuru Süreci için oluşturulmuş Şekil 2.2 aşağıda yer almaktadır.



Şekil 2.2: Şube Kredi Kartı Başvuru Süreci

1- Müşteri olma süreci için ilk önce potansiyel müşteri kişisinin kimlik kartı, pasaportu ve T.C. kimlik kartı, müşteri adres bilgileri ve müşteri iletişim bilgileri (cep telefon numarası, e-mail adresi vb.) kullanılarak müşteri formu adı verilen bankalarca hazırlanmış bir evraka müşteri el yazısı ile doldurulması istenir. İlgili müşteri formunun hukuki geçerliliğini sağlamak maksadı ile ilgili bilgilerin potansiyel müşteri tarafından verildiği, ilgili bilgilerin banka sisteminde kullanılacağı müşteriye bildirilir ve potansiyel müşterinin bilgisinin olduğu hatırlatılarak formun imzalanması istenir.
2- İmzalanan müşteri formunu temin eden banka memuru ilk olarak ilgili kişinin belgesi üzerindeki kimlik numarasını kullanarak sisteme potansiyel müşteri girişi işlemlerini başlatır.
3- Potansiyel müşteriden temin edilen kimlik beyanını gösteren belge, potansiyel müşterinin bilgilerini yazdığı müşteri formu taranarak, fiziki belge üzerindeki bilgiler elektronik ortama yani banka veri tabanına dahil edilir. Potansiyel müşteri iletişim bilgileri, müşteri adres bilgilerinin de sisteme girişi sağlanır.
4- Banka memuru teknolojik altyapıların gelişmesi ve kamu hizmetleri ile yapılan anlaşmalar dahilinde ilgili potansiyel müşterinin kimlik bilgilerini kullanarak ilgili kişinin gerçekten söz konusu kişi olup olmadığını, banka hesabı açılması için gereken yaş sınırı, (18 yaş üstü kişiler kendileri adına hesap açabilirken, 18 yaş altı kişiler veli/vasileri yardımı ile açabilir.) fiili ehliyet durumunu göz önünde bulundurarak sürece devam eder. Müşterinin cep telefonu numarasına sürecin yürütülebilmesi hem de suistimal içeren işlemleri önlemek için kısa mesaj gönderir.
5- İlgili hesabın ilk işlemlerini gerçekleştiren banka memuru müşteri olma sürecini uçtan uca tek başına görevler ayrılığı sebebi ile devam edemez ve onay için bir başka banka memurunun onayına gönderir. İkinci banka memuru sistem üzerinden gelen onay işlemini ilgili potansiyel müşterinin kişisel bilgilerini kontrol eder, ilgili kişinin gerçekten o kişi olduğuna kanaat getirir ve ilgili müşteri olma işlemini gerçekleştirir.

Kredi kartı başvurusu yapmak için gereken ilk kırılma noktası olan müşteri olma hali tamamlandıktan sonra süreç her bir kredi kartı başvurusu gerçekleştirecek müşteri için aynı şekilde işlemeye başlayacaktır. Kredi kartı başvuru sürecine bu aşamadan sonra tek bir akışla devam edecektir.

1- Potansiyel müşteriden gerçek müşteriye geçen ilgili başvuru sahibinin kredi kartı başvurusunda bulunması için banka üzerinde hesap sahibi olması gerekmektedir. Bu sebeple müşteri olan ilgili kişi için hesap tanımlama işlemi yapılmaya başlanır. Bu hesap tanımı mevduat hesabı olarak adlandırılır.
2- Hesap açma işlemleri aynı banka memuru tarafından sistem üzerinden devam ettirilir. Bu aşamada müşterinin hesap açılımına onay verdiğini gösteren, ilgili bankacılık ürünü olan hesap açılımının özelliklerini (adı varsa faiz oranı, masraf tutarları vb.) gösteren evrakın müşteri tarafından imzalanması istenir ve ilgili evrak sisteme taranarak hesap açma işlemi yukarıda müşteri olma sürecinde de olduğu gibi farklı bir banka memurunun onayına düşer ve ilgili incelemeler gerçekleştirildikten sonra hesap açma işlemi tamamlanır. Bu hesap açma işlemi sonrasında müşteri ve bankanın hak ve yükümlülüklerini, bankacılık ürününün özelliklerini, faiz oranını gösteren "Sözleşme" olarak adlandırılan yasal bir evrak müşteri tarafından "okudum, anladım, kabul ediyorum" ibaresi yazılarak imzalanır ve banka veri tabanına taranır ve fiziki olarak 10 yıl süre ile saklanır (Bankacılık Kanunu, 2005). Söz konusu işlemler tamamlanırken eş zamanlı olarak müşteri cep telefonuna müşteri olduğu, adına hesap açıldığına dair bilgileri içeren kısa mesajlar gönderilmektedir.

Müşteri olma ve hesap açılımı işlemleri tamamlandıktan sonra kredi kartı başvuru sürecinin başlaması için herhangi bir engel bulunmamaktadır.

Kredi kart başvuruları için müşterilerden daha önce müşteri olma ve hesap açma süreçlerinde olduğu gibi kredi kartı başvuru formunu doldurması beklenmektedir. İlgili form müşterinin Ad Soyad, T.C. kimlik numarası, Anne/Baba Adı, Doğum Tarihi, Adres Bilgileri Eğitim Durumu, Mesleği ve Pozisyonu, Aylık/Yıllık Gelir Bilgisi, İstenen kredi kartı limit miktarı bilgilerini içermektedir. Müşteri olma ve hesap açma süreçlerinden farklı olarak aylık ve yıllık gelir, istenen kredi kartı miktarı bölümlerinin bulunduğu görülebilir. İlgili bilgilerin kredi kartı başvuru sürecinin ana bilgileri olduğu sürecin ilerleyen kısımlarında daha net anlaşılacaktır.

Kredi Kartı Başvuru Formu bilgileri kullanılarak "Skorlama" adı verilen müşterinin bir çeşit finansal değerlendirmesi yapılır. Bu skorlama işlemi bankalar tarafından kurulan elektronik sistemler aracılığı ile özellikle müşteri gelir bilgisi, müşterinin finansal ürün geçmişi, ödeme alışkanlıkları, yaşı vb. verilerin kullanıldığı bir algoritma olarak düşünülmelidir. İlgili algoritma Türkiye Kredi Kayıt Bürosu (KKB) tarafından

oluşturulmuş ve Türkiye'de işlem yapan bankaların kullanımına açılmıştır. Bu algoritma sonucu müşteriye 0-1900 arasında segmentlere bölünmüş olup 0 en düşük puanı ve dolayısı ile müşteri için kredibilitenin en düşük olduğu noktayı göstermektedir. Bankaların iç işleyişine göre değişmek ile kredi kartı sahibi olabilmek için en az 700 puana sahip olmak elzemdir (Kredi Kayıt Bürosu, n.d.).

Kredi kartı sahibi olmak için bankalarca yapılacak her türlü müşteri değerlendirmesi Bankacılık Denetleme ve Düzenleme Kurulu (BDDK) tarafından Banka Kartları ve Kredi Kartları Hakkında Yönetmelik ile Türkiye'deki bankalara duyurulmuştur. İlgili Yönetmelik'in 22. maddesinde "*Kart çıkaran kuruluşlar, kredi kartı almak isteyen kişilerin yasaklık veya engel durumu, ekonomik ve sosyal durumu, aylık veya yıllık ortalama geliri, diğer kart çıkaran kuruluşlarca bu kişilere tahsis edilen kredi kartı limiti, bir model veya skorlama sistemi sonuçları, müşterini tanı ilkeleri ile bilgi alışverişi şirketlerinden temin edilecek bilgileri dikkate alarak yapacakları değerlendirmeye istinaden kullanım limiti tespit etmek zorundadır." ve "Kart çıkaran kuruluşların, müşterileri hakkında müşterinin kredi ödeme performansı, varlık ve yükümlülükleri, sosyal statüsü, eğitim düzeyi, yaşı ve benzeri ödeme gücünün değerlendirilmesinde etkili olabilecek hususlara ilişkin alacakları beyan ve temin edecekleri belgeler çerçevesinde yapacağı değerlendirmeler ilgili kuruluşça yapılacak teyit niteliğini taşır. Kart çıkaran kuruluşlar, karşılığı nakit, nakit benzeri kıymet ve hesaplar ile kıymetli maden olması durumunda, karşılık olan tutarı geçmemesi ve rehin sözleşmesi yapılması şartıyla, gelir beyanı ve gelir teyidi zorunluluğuna tabi olmaksızın kredi kartı limiti tespit edebilir."* şeklinde belirtiği kurallar çerçevesinde işlem yapılır (Bankacılık Düzenleme ve Denetleme Kurumu, 2008). İlgili Yönetmelik maddesinin keskin sınırlara sahip olmadığı, bu açıdan banka kredi kartı başvuru işlemlerini bir nebze de olsa esnek bıraktığı, riski banka'nın ve dolayısı ile kart müşterisinin üzerinde topladığı yorumu yapılabilir. Bu esneklik bankalar tarafından kâr amacı güdülerek esasen kredi kartı verilemeyecek nitelikteki müşteri gruplarına da hizmet verilmesinin önünü açmakta olduğu açıktır.

Skorlama işlemi sonrasında banka iç değerlendirmeleri sonucunda ilgili müşteriye kredi kartı verilip verilmeyeceği kararı verilir. Bu karar bankaların yukarıda yönetmelikte de bahsedildiği gibi esnek bir süreç olup banka risk iştahına göre şekillenmektedir.

Müşteri kredi kartı başvurusunun olumlu olduğu durumda, müşteri için belirlenecek kart limiti söz konusu hale gelir. Bu limitin belirlenmesi "Limit Kontrol Sistemi" adı verilen (LKS) ve Yönetmelik'in 22. maddesi 3. bendinde yer alan *"ilk defa kredi kartı sahibi olacak bir gerçek kişinin tüm kart çıkaran kuruluşlardan temin ettiği kredi kartları için tanınacak toplam kredi kartı limiti, ilk yıl için, ilgilinin aylık ortalama net gelirinin iki katını, ikinci ve sonraki yıllar için ise dört katını aşamaz.*" ibaresine uygun olmalıdır (Bankacılık Düzenleme ve Denetleme Kurumu, 2008).

Kredi kartı başvurusunu gerçekleştiren ve ilgili başvurunun olumlu tamamlandığı durumda ilgili müşteriye Kredi Kartı Ürün Sözleşmesi adı verilen kredi kartına ait bilgilerin, faiz oranlarının, ödeme günlerinin, müşteri ve banka'nın yasal haklarını gösteren bir sözleşme imzalatılır ve banka veri tabanına taranır ve fiziki olarak 10 yıl süre ile saklanır (Banka Kartları ve Kredi Kartları Kanunu, 2006). Söz konusu işlemler tamamlanırken eş zamanlı olarak müşteri cep telefonuna kredi kartı başvurusunun olumlu olduğuna dair bilgileri içeren kısa mesajlar gönderilmektedir.

Kredi kartının kullanıma açılım işlemi kredi kartının basılması ve müşteriye ulaştırılması ve müşteri tarafından ATM'ler cep telefonu veyahut mobil bankacılık kanalı kullanılarak aktifleştirilmesi sonucunda başlamaktadır. Buraya kadar anlattığımız işlemler bir kredi kartının başvurudan müşteriye ulaştığı süreçte yapılan işlemleri göstermektedir. Tezimizin konusu olan ve esasında bu süreçten sonra başlayan en önemli kısım müşterinin ödemelerinin müşteriye bildirilmesini sağlayan hesap özeti veyahut ekstre adı verilen bilginin müşteriye nasıl ulaştırıldığı, bu ulaşım yolunun güvenilirliğidir. Kredi kartı başvuru süreci içerisinde en önemli kısımlardan biri müşteri kredi kartı borcunun ödeneceği tarihlerin belirlenmesi, bu tarihler öncesinde müşterinin ilgili hesap döneminde yaptığı harcamaların müşteriye ulaştırıldığı kanallardır. Yönetmelik'in 19. maddesinde hesap özeti başlığı altında kredi kartı hamillerine gönderilecek hesap özetlerinde; kredi kartı hamilinin ad, soyadı ve adresine, kredi kartıyla yapılan işlemlere ilişkin dönem borcuna, Toplam kredi kartı limitine, Hesap kesim tarihine, Son ödeme tarihine, Bir sonraki hesap kesim tarihi ve son ödeme tarihine, Ödenmesi gereken asgari tutara, kredi kartıyla yapılan nakit çekim işlemlerinin veya mal ve hizmet alımlarının tutar ve tarihlerine, kredi kartlarına uygulanan akdi faiz oranlarına, kredi kartlarına uygulanan gecikme faizi oranlarına, kredi kartlarına ilişkin olarak ilgili hesap özetinde tahakkuk ettirilen yıllık ücret, faiz ve diğer her türlü ücret ve komisyon tutarlarına, kredi kartı ile gerçekleştirilen yabancı

para cinsinden işlemlerde, işleme konu döviz cinsi ve tutarı ile kart hesabına borç kaydedilen para birimi ve tutarına, ilişkin bilgilerin bulunması zorunludur." İbaresi kullanılmıştır. Bu sebeple bankalar ile kredi kartı müşterileri arasında imzalanan Kredi Kartı Sözleşmesi'nde ve kredi kartı başvuru formu üzerinde işbu hesap özeti/ekstrenin gönderileceği kanalın seçilmesi beklenmektedir. Bu kanallar ikametgâh adresi, müşteri e-posta adresi olarak belirlenmektedir. Bunun yanı sıra BDDK tarafından yayınlanan Elektronik Bankacılık ve Hizmet Yönetmeliği'nin 37. maddesi 8. bendinde 1 Temmuz 2020 tarihinde *"Bankanın elektronik ortamda müşterilerine ileteceği hassas veri veya sır niteliğinde veri içeren her türlü ekstre, dekont, hesap özeti gibi bilgilerin elektronik bankacılık hizmeti sunulan kanallar üzerinden gönderilmesi esastır. Banka, bu gibi bilgilerin sunulmasında elektronik dağıtım kanallarının kullanılması için müşterilerine gerekli yönlendirmeleri yapmakla yükümlüdür*." şeklinde yapılan değişiklikte ile artık müşteri isteğine bağlı olarak hesap ekstresi dijital ekstre olarak banka internet ve mobil uygulamaları üzerinden görülebileceği belirtilmiştir (Bankacılık Düzenleme ve Denetleme Kurumu, 2008). Bu değişiklik ile hesap ekstrelerinin e-posta ve adres üzerinden müşterilere gönderimini azaltması öngörülmektedir. Bu azaltmaya gidilmesi esasında BDDK'nın da e-posta ve ikametgâh adresine gönderilen ekstrelerin 3. Kişilerin eline geçmesinden çekincesini göstermesi ve tezimizin odak noktası olan müşteri kişisel verisinin açığa çıkma tehlikesini göstermesi açısından önemlidir.

Kredi kartı başvuru sürecinden bahsederken ana olarak şube üzerinden ve alternatif dağıtım kanalları kullanarak kredi kartı başvurusunda bulunma durumundan bahsedilmiş idi. Tezimizin bu baslığı ile banka şubeleri aracılığı ile kredi kartı başvuru sureci hakkında bilgi verilmiştir. Alternatif dağıtım kanalları yolu ile nasıl kredi kartı başvurusu yapılacağı bir diğer baslıkta ele alınacaktır.

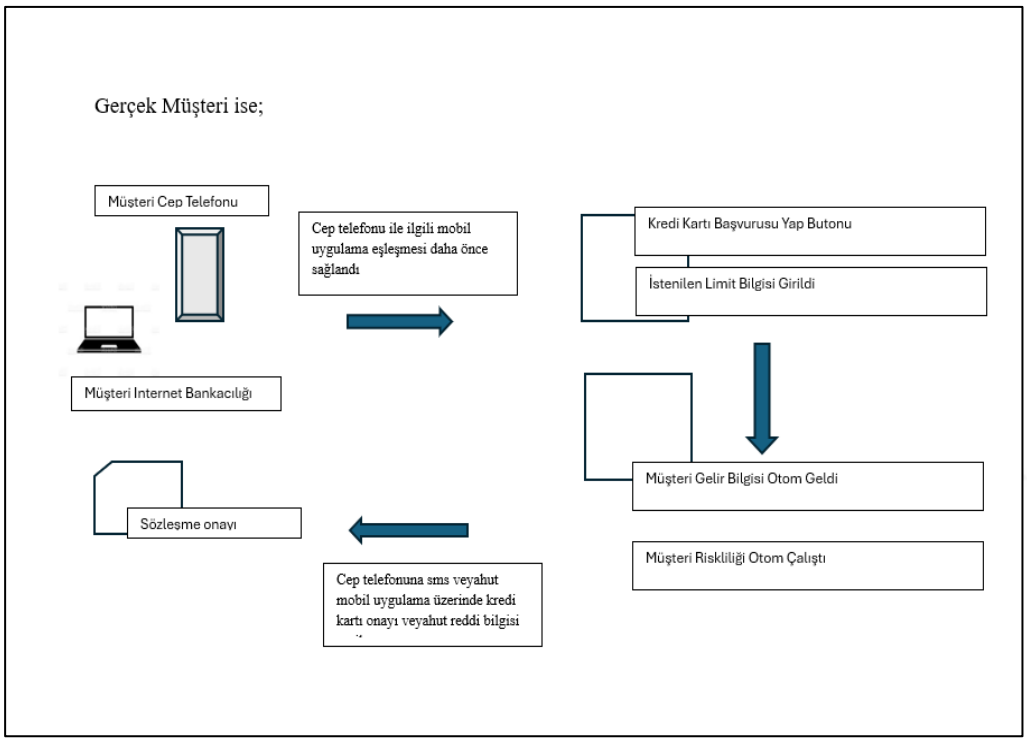
2.2.1 Alternatif dağıtım kanalları ile yapılan kredi kartı başvuru süreci

Teknolojik gelişmelerin dünya genelinde vardığı seviye bankacılık sektörünü sürekli gelişime ve bu teknolojiye entegre edecek yeni uygulamaları devreye almaya itmiştir. Şube bankacılığı olarak adlandırılan ve Türkiye'de halen geçerliliğini koruyan fiziki yapılan bankacılık artık yerini alternatif dağıtım kanalları adı verilen ATM, mobil bankacılık, internet bankacılığı ve 2021 yılından beri bankacılık sektörüne entegre

edilen uzaktan kimlik tespiti ve elektronik sözleşme ile düzenlenen uygulamalara bırakmaktadır.

Alternatif dağıtım kanalları üzerinden tez konumuzun da ana temasını oluşturan kredi kartı başvurusunu yapmak için ilgili bankanın müşterisi olmak gerekmektedir. Alternatif dağıtım kanalları kullanılarak kredi kartı başvuru süreci de şube yolu kredi kartı başvuru süreci gibi müşteri olup olmamaya göre farklı adımlara sahip olacaktır.

Şekil 2.3 Alternatif dağıtım kanalı yoluyla kredi kartı başvurusu tablosu alternatif dağıtım kanalları ile kredi kartı başvuru sürecini göstermektedir.



Şekil 2.3: Alternatif Dağıtım Kanalı yoluyla Kredi Kartı Başvurusu

Şemada görüldüğü üzere kredi kartı başvurusunda bulunmak isteyen müşteri başvuru yapacağı bankanın hâlihazırda müşterisi ise;

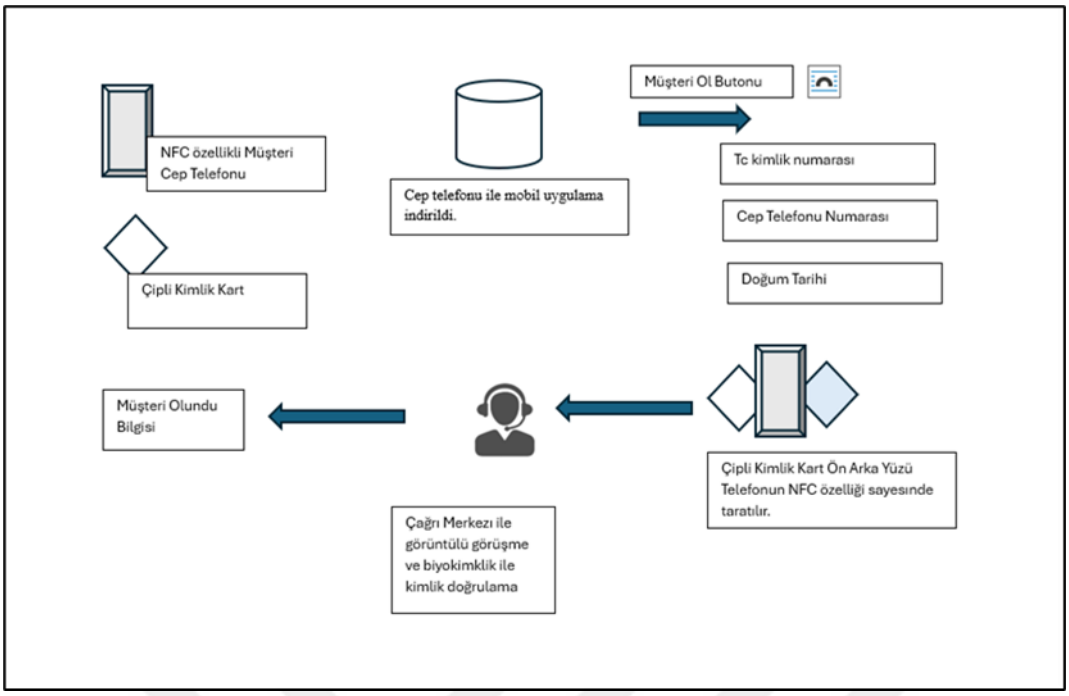
1- Müşteri cep telefonu üzerinden bankanın mobil uygulamasını indirmek, banka internet sitesini kullanmak veyahut ATM üzerinden kredi kartı başvuru sürecini başlatabilmektedir.
2- Alternatif dağıtım kanalları üzerinden giriş yapabilmek için müşterinin hâlihazırda sahip olduğu şifre ile sisteme girmesi gerekmektedir. Şube üzerinden yapılan kredi kartı başvuru sürecinde olduğu gibi alternatif dağıtım kanalları için özel olarak hazırlanmış kredi kartı başvuru formunu doldurarak

onaylaması gerekmektedir. Bu kredi kartı başvuru formu şube üzerinden yapılan kredi kartı başvuru formunun dijital hali olup talep edilen kredi kartı tipi baz alınarak müşterinin bilgilendirilmesi amaçlanmakta bunun yanında müşteri verilerinin banka veri tabanında saklanması için de bir gerekçe sunmaktadır. Kredi kartı başvuru formu üzerinde seçilen kredi kartı tipi, akdi ve gecikme faiz oranları, ödeme dönemleri ve hesap özeti/ekstrenin iletileceği müşteri iletişim bilgileri yer almaktadır.

3- Kredi kartı başvuru için eğer banka veri tabanında gelir bilgisi yok ise müşteriden bu bilgi de Alternatif dağıtım kanalları üzerinden talep edilmektedir.
4- Kredi kartı başvuru süreci şube üzerinden yapılan başvurunun benzeri olarak müşteri skorlama işlemine tabi tutulmakta ve bankanın iç değerlendirilmesi sonucunda müşteriye kredi kartı başvuru sonucu sms üzerinden gelmektedir. Müşteri kredi kartı başvurusunun yanı sıra sms ile gelen bilgiye istinaden alternatif dağıtım kanallarına girmekte, dijital kredi kartı sözleşmesini imzalamaktadır.

2.2.2 Uzaktan müşteri olma yolu ile kredi kartı başvurusu

Kredi kartı başvurusunda bulunacak müşteri eğer ilgili bankanın müşterisi değil ise Uzaktan Müşteri Olma hizmetini kullanabilecektir. Bu hizmetin kullanımı 01.04.2021 tarih ve 31441 sayılı Resmî Gazetede BDDK tarafından yayınlanan "Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik" ile kullanılmaya başlanmıştır. Söz konusu uygulama ile şubeye ulaşımı olmayan potansiyel müşterilerin bankalara kazandırılmasını amaçlayan bankacılık uygulamalarının güvenilirliğini arttırmak için birtakım kurallar getirmiştir (Bankacılık Denetleme ve Düzenleme Kurulu, 2021). Bu kurallar gözetilerek potansiyel müşterilerin uzaktan kimlik tespiti ile gerçek müşteri olma süreci sağlıklı bir hale getirilmiştir. Aşağıdaki Şekil 2.2'de uzaktan müşteri olma iş akış şemasını görebilirsiniz.



Şekil 2.4: Uzaktan Müşteri Olma İş Akış Şeması

1- Bu süreç için potansiyel müşteri cipli kimlik kartını ve NFC özelliği taşıyan bir cep telefonu kullanmalıdır. Müşterisi olunacak bankanın mobil uygulaması indirilerek "Müşterisi ol" menüsüne giriş yapılır.

2- Müşteri ol menusu tıklandıktan sonra müşteriden başvuru formu doldurması istenmektedir. İlgili başvuru formu T.C. Kimlik numarası, Cep Telefonu Numarası ve Doğum Tarihi Bilgisi talep edilmektedir. Bu veriler alındıktan sonra kısa mesaj ile bir şifre gelmekte ve bu şifre ile sisteme dahil olmaya başlanmaktadır.

3- T.C. Kimlik Kartının ön ve arka yüzü cep telefonu kamerası kullanılarak sisteme okutulmaktadır.

4- NFC destekleyen cep telefonu ile T.C. Kimlik Kartı taratılarak eşleşme sağlanmaktadır.

5- T.C. Kimlik Kartı tarandıktan sonra potansiyel müşterinin biyokimlik ile kendini banka sistemine taratması istenmektedir. Potansiyel müşteri kendini cep telefon kamerasına tanıtmaktadır.

6- Sonraki adımda ise bankanın görüntülü görüşme işlemini gerçekleştiren banka personeli ile iletime geçilir. İlgili personel sizin kişisel bilgilerinizi doğrulamak ve müşteri olmanızı kolaylaştırmak için görevlendirilmiştir

7- Banka personeli kimlik kartınızı kameraya göstermenizi ister, size verdiğiniz kişisel bilgileri doğrulamak maksadı ile sorular sormaktadır.
8- Doğrulamalar yapıldıktan sonra müşterinin cep telefonu numarasına geçici bir dijital şifre gönderilir ve müşteri olma süreci tamamlanmaktadır.
9- Müşteri olma işlemi tamamlandıktan sonra mobil uygulama ve internet bankacılığı alternatif dağıtım kanalları kullanılarak kredi kartı başvuru sürecine bir önceki baslıkta anlatılan şekilde devam edilir.

Bankaların kredi kartı başvuru süreçleri ilgili bankanın müşterisi olup olmamakla farklı kırılımları getirdiğini yukarıda anlatılan süreçler ile açıkça görmüş bulunduk. Dikkat edilirse ister şube üzerinden isterse alternatif dağıtım kanalları ile olsun müşterilerden kişisel bilgi talebi almadan herhangi sürecin başlatılamayacağı görülebilir. Şube vasıtası ile kredi kartı başvurusu yapılırken müşterinin tüm kimlik bilgileri, (Ad Soyad T.C. kimlik numarası) iletişim bilgileri (Cep telefonu numarası, elektronik posta adresi, ev adresi, işyeri adresi), gelir bilgileri, finansal geçmiş bilgisinin banka tarafından veri olarak alınarak saklandığı görülmektedir. Bunun yanı sıra uzaktan müşteri olma sürecinde bahsi gecen verilerin yanı sıra müşterinin biyokimliğinin de kullanıldığı görülmüştür.

Bankalar müşterilerinden aldıkları bu kişisel bilgileri alırken müşterilerin bilgisi dahilinde yapıldığını göstermek maksadı ile Müşteri Başvuru Formu, Ürün Bilgi Formu, Sözleşme vb. akitler düzenlemekte olup kendilerini güvence altına almaya çalışmışlardır. Bu akitler aynı zamanda müşterilerin de korunması için bir önlem olarak denetleyici ve düzenleyici otoriteler tarafından zorunlu tutulmaktadır. Tezimizin bir sonraki başlığı bankaların neden ve nasıl müşteri verilerini saklamak ve güvenliğini sağlamak zorunda olduğunu daha ayrıntılı olarak inceliyor olacağız.

3. FİNANSAL KURUMLARIN MÜŞTERİ VERİSİ İLE İLİŞKİLERİNİ BELİRLEYEN DÜZENLEMELER

3.1 Avrupa Birliği Uygulamaları

Avrupa Birliği içerisinde yer alan ülkelerin kendi aralarındaki finansal alışverişlerinin bankalar, finansal kurum ve kuruluşlar arasındaki regülasyonların düzenlenmesi ve en önemlisi bireysel tüketicilerin haklarının korunması, kişisel veri, müşteri sırrı kavramlarının benimsenmesi maksadı ile birtakım çalışmalar içerisinde bulunmuştur. Bunların en önemlileri European Commission tarafından yayımlanan Payment Service Direction (PSD 1-2), Payment Service Regulation "PSR" kural setleri, European Consumer Credit Directives, General Data Protection Regulation (GDPR) ve Strong Customer Authentication (SCA) olarak görülmektedir.

Avrupa Birliği üye ülkelerinin daha güvenli ve daha yenilikçi ödeme hizmetleri oluşturmak amacıyla 2007 yılında Payment Service Direction 1 (PSD1) adı verilen kurallar bütününü uygulamaya başlamıştır. Bu uygulamanın AB üye ülkeleri arasında güvenli ve hızlı ödeme işlemlerini gerçekleştirmek amaçlanmıştır. 2007 yılından bu yana, bu Direktif Avrupa ekonomisine önemli faydalar sağlamış, pazara yeni girenlerin ve ödeme kurumlarının erişimini kolaylaştırmış ve böylece tüketicilere daha fazla rekabet ve seçenek sunmuştur. Teknolojik gelişmeler sebebi ile büyüyen ödeme sistemleri çeşitleri sebebi ile PSD1 uygulamasının değiştirilmesi gerekmiş ve 12.01.2016 tarihinde Payment Service Direction 2 PSD2 yürürlüğe girmiştir. Ödeme hizmeti sağlayıcıları için eşit şartların iyileştirilmesi, ödemeleri daha güvenli ve daha emniyetli hale getirilmesi tüketicilerin korunması açısından önem arz etmektedir (European Unıon). 28.06.2023 tarihinde PSD 2 uygulaması genişletilerek PSD3 haline getirilmiş ve ek olarak Payment Service Regulation PSR adı verilen bir yönetmelik hazırlanmıştır. Söz konusu güncellemeler ile Ödeme hizmeti sağlayıcılarının dolandırıcılıkla ilgili bilgileri kendi aralarında paylaşması, tüketici haklarını iyileştirilmesi, hesap özetlerinin daha şeffaf hale getirilmesi, özellikle banka dışı ödeme hizmeti sağlayıcılarının tüm AB ödeme sistemlerine uygun güvenlik

önlemleriyle erişmesine izin verilmesi, bankalar ile banka dışı kuruluşlar arasındaki oyun alanının daha da eşitlenmesi, Özellikle banka dışı ödeme hizmeti sağlayıcılarının tüm AB ödeme sistemlerine uygun güvenlik önlemleriyle erişmesine izin vererek bankalar ile banka dışı kuruluşlar arasındaki oyun alanının daha da eşitlenmesi, Açık bankacılık hizmetleri sağlamanın önündeki engelleri kaldırması, çoğu ödeme kuralını doğrudan uygulanabilir bir düzenlemeyle yürürlüğe koyarak ve uygulama ve cezalara ilişkin hükümleri güçlendirerek uyumlaştırması ve yaptırımı güçlendirmesi hedeflenmektedir (European Unıon).

Kişisel Verilerin Korunması Kanunu'nda ise daha çok spesifik olarak bireysel müşterilerin kişisel verilerinin kullanılması ve yöntemleri belirtilmektedir. Kişisel Verilerin Korunması Kanunu'nda kişisel verinin; kimliği belirli veyahut kimliği belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlandığı görülmüştür (Kişisel Verilerin Korunması Kanunu, 2016). General Data Protection Regulation bakıldığında ise kişisel verinin "*Personal data are any information which are related to an identified or identifiable natural person"* olarak tanımlandığı görülmektedir (European Union , 2016). Dikkat edilirse her iki tanımın da birbirinin aynısı olduğu görülecektir. Bu tanımlardan yola çıkılarak Bir kişinin "kimliği belirli" olması, o kişinin bir topluluk içerisinde o topluluğun diğer üyelerinden ayırt edebilmesini sağlamasının anlaşılması gerekirken, "kimliği belirlenebilir" ibaresi ile kişinin kimliği halihazırda belirlenmemiş olsa dahi kişinin kim olduğunun tespitinin mümkün olacağı durumları ifade etmektedir. O zaman bireye ait Ad Soyadı bilgisi, kimlik numarası, pasaport numarası, cinsiyeti, yaşadığı ülke, iletişim adresleri vb. bilgilerin tamamı kişisel veri tanımlamasının içerisinde yer alabilir. Görüldüğü üzere kişisel veri kapsamının sınırları tam olarak belli olmamakla birlikte, kişilerin tanımlanabilir, ayırt edilebilir olduğu her durumu kapsadığı söylenebilir.

Kişisel verinin dünya üzerinde nasıl belirlendiği, korunduğu karşımıza en çok çıkan düzenlemenin GDPR olarak kısaltılan General Data Protection Regulation olduğu görülmüştür. GDPR Avrupa Birliği ülkelerinde yaşayan kişilerin; kişiler, kurumlar ve hatta devlet karşısında kişisel verilerinin korunmasını esas alan bir örgütlenme olarak kavramlaştırabilir. İlk kez 2016 yılının Nisan ayında yürürlüğe girdiği ve 2018 yılının Mayıs ayıda ise tüm Avrupa üye ülkeleri tarafından baz alınan bir çerçeve haline gelmiştir. GDPR'ın ilk başlangıç noktasının 1998 yılında yürürlüğe giren G 95/46/AT sayılı "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin

Korunmasına İlişkin Direktif" düzenlenmesi olduğu söylenebilir. Bu düzenleme bir çerçeve olarak sunulmuş, hukuki olarak Avrupa Birliği üye ülkelerinin kendi lokal mevzuatlarını oluşturmalarında etken olmuştur (European Union , 2016).

GDPR'ın en önemli özelliklerinden biri yalnızca Avrupa Birliği vatandaşlarını veyahut Avrupa Birliği ülkelerini değil her türlü bilgi, mal ve hizmet alışverişinde bulunduğu kişi, kurum ve kuruluşları, bunun yanında internet üzerinden yapılan işlemleri de kapsamasıdır. GDPR özelinde bakıldığında kişisel veri kavramının çok geniş tutulduğu görülmektedir. GDPR 'ın 4. maddesinin tanımlar kısmında kişisel verilerin isim, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlandığı her türlü bilginin kişisel bilgi olduğu belirtilmiştir (European Union , 2016).

- Kişisel bilgiyi kullanan tarafı kişisel veri sahibinin yazılı izni olmadıkça bu veriyi kullanamayacağı belirtilmiştir.
- Kişisel bilgiyi kullanan tarafın bu veriyi amacı belirlenmiş durumlarda kullanabileceği belirtilmiştir.
- Kişisel veri sahibi ile kişisel veriyi kullanan taraf arasında yapılan akit, sözleşmelerin bir kopyasının kişisel veri sahibine verilmesi gerektiği belirtilmiştir.
- Kişisel veriyi kullanan taraf kişisel verilerin hatalı veyahut kullanım süresinin geçtiğini kişisel veri sahibine bildirmeli ve kişisel veri sahibi ile gerekli düzeltmeleri yapmalıdır.
- GDPR Bölüm 8.5 "İşleme Süresi, Verilerin Silinmesi veya İadesi" başlığında kişisel veriyi kullanan taraf, kişisel veri sahibi ile olan işlemler sonrasında kişisel verileri silmek ve silindiği bilgisini kişisel veri sahibine iletilmesi gerekmektedir.
- GDPR Bölüm 8.6 "İşleme Güvenliği" başlığında kişisel veriyi kullanan tarafın kazara veya yasa dışı imha, kayıp, değişiklik, izinsiz ifşa veya erişime yol açan güvenlik ihlaline karşı koruma da dahil olmak üzere, verilerin güvenliğini sağlamak için uygun teknik ve organizasyonel önlemleri uygulaması gerekmektedir.

- GDPR Bölüm 8.7 “Hassas veriler” başlığında kişisel veri sahibinin ırk veya etnik kökeni, siyasi görüşleri, dini veya felsefi inançları veya sendika üyeliğini, genetik verileri veya bir gerçek kişiyi benzersiz şekilde tanımlamak amacıyla biyometrik verileri, sağlık veya bir kişinin cinsel hayatına ilişkin verileri o veya cinsel yönelim veya cezai mahkûmiyet ve suçlarla ilgili verileri anlaşılmalıdır.

İlgili maddelere bakıldığında aşağıda yer alan çıkarımlar yapılabilecektir.

- Kişisel veri tanımının yanı sıra bu verilerin sahiplerini, veriyi kullanacak olan kurum ve kuruluşları, üçüncü tarafları, denetleyici ve düzenleyici otoriteleri ve bunların hangi durumlarda kişisel veriye erişiminin olabileceğini belirttiği, her bir aktörün görev ve sorumluluklarının belirlendiği görülmüştür.
- Bahsi geçen kişisel verilerin elde edilmesi, kullanımı, depolanması ve imhası konusunda açıklamalarda bulunduğu,
- Kişisel veri sahibinin iznini en büyük kontrol noktası olarak belirlediği, yapılacak tüm veri güncellemesi, değiştirilmesi esnasında bu kontrol noktasının özellikle kullanılması gerekliliğini
- Kişisel veri kullanımının kişisel veri sahibi ve kişisel veriyi kullanacak olan taraf arasında yapılacak yazılı sözleşme ve yazışmalarla belirleneceğini
- Kişisel verilerin izinsiz kullanımı durumunda yaptırımların içeriği
- Kişisel veri sahibine verilen unutulma hakkı ile kişisel verilere ait iz düşümlerinin hem elektronik hem de fiziki ortam üzerinden imhası hakkında geçerli, ayrıntılı, kişisel veri sahibinin güvence veren bir uygulama olduğu görülmüştür.

Tezimiz konusu olan kredi kartı başvuruları da GDPR’ın konusuna giren bir kişisel veri olduğu su götürmez bir gerçektir. Avrupa Birliği üye ülkeleri özelinde kredi kartı uygulamalarının GDPR’a uygun hale getirilmesi sürecinde neler yapıldığı incelenmiştir. Bu incelemeler sonucunda;

- Kredi kartı başvuru sürecinde Avrupa Birliği ülkeleri genelinde müşterinin şube üzerinden işlem yapmak istediğinde bir başvuru formu doldurduğu ve imzaladığı, eğer bu başvuru online yapılıyor ise bir başvuru ekranının meydana getirildiği, böylece müşterilere işlem gerçekleştirilmeden önce bilgi verilmesi kurallara uyulduğu,
- Başvuru Formu üzerinde Ad Soyad bilgisi, sosyal güvenlik numarası, doğum tarihi, cinsiyet, elektronik posta adresi, çalışılan is bilgileri, gelir bilgisi,

medeni durumu bilgileri, ev/iş adresi, telefon numarası istendiği, bu bilgiler alındıktan sonra "Tüm bilgilerimin doğru olduğunu onaylıyorum. Kredi kartının verilmesi amacıyla verdiğim bilgilerin kontrol edilmesi için bankaya yetki veriyorum" ibaresinin eklendiği, böylece müşterilerden açık rıza alındığı,

- Kredi kartı başvurusu onaylandıktan sonra kredi kartı bilgileri, limit bilgisi, hesap kesim tarihi, hesap özeti tercihi (mobil uygulama, e-posta, posta vb.), akdi ve gecikme faizi, banka ile müşterinin haklarının açıklandığı bir sözleşmenin imzalandığı, böylece müşteri ile banka arasında yazılı bir anlaşmaya varıldığı, müşteri bilgilendirme kuralına riayet edildiği görülmüştür.

3.2 Türkiye Uygulamaları

Kişisel veri kavramı Türkiye'de ilk olarak 6 Şubat 2004 tarihli ve 25365 sayılı Resmî Gazete 'de yayımlanan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik (VKY) ile yapılmıştır. Bu yönetmelikte kişisel verinin tanımı da yapılmış, *"kişisel verinin tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgiyi"* temsil ettiği söylenmiştir (Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik , 2008). Tez tarihi itibari ile halen kullanımda olan Türkiye`de temel alınan kişisel veri düzenlemesi ise 7 Nisan 2016 tarihinde 29677 sayılı Resmî Gazete 'de yayımlanan Kişisel Verilerin Korunması Kanunu (KVKK)`dur (Kişisel Verilerin Korunması Kanunu, 2016).

Kişisel Verileri Koruma Kanunu `nın özellikle bankacılık alanında incelenmeye değer birtakım maddeleri aşağıya çıkarılmıştır.

Kişisel Verileri Koruma Kanunu "Kişisel verilerin işlenme şartları" başlıklı 5. maddesi *"Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması..."* ibaresi bankacılık işlemlerinde kişisel verilerin sözleşme düzenlenmesi şartı ile kullanılabileceği konusunda bilgi vermektedir.

Kişisel Verileri Koruma Kanunu "Özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6. maddesi *"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir."*

Kişisel Verileri Koruma Kanunu Veri sorumlusunun aydınlatma yükümlülüğü başlıklı 10. maddesi *"Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; Veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi hakkında bilgi verilmelidir*." ibaresi yer almakta olup veri sorumlusu olarak bankaları baz alınırsa, bankacılık işlemlerinde kullanılan KVKK Aydınlatma Metni ile uygulanmaya çalışılmaktadır.

Kişisel Verileri Koruma Kanunu Veri güvenliğine ilişkin yükümlülükler başlıklı 12. maddesinde "Veri *sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur. Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder. İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde*

edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." ibaresi yer almaktadır. *"Veri sorumlusu olarak banka kabul edilir ise müşterilerden alınan verilerin erişimini engellemek 3. Taraflarla olan paylaşımları engellemek, bu engellemeleri hem idari hem de teknik ve bilgi teknolojileri alanında düzenlemek ile sorumludur. Bankalar her yıl düzenli olarak Teftiş Kurulları ve Dış Denetçiler yardımı ile verilerin paylaşılıp paylaşılmadığını denetlemekte, 3. Taraflarla olan ilişkilerinde yapılan işlemlere gerekli önemi vermektedir.*"

Kişisel Verilerin Korunması Kanunu Türkiye'de özellikle kişisel veri ile işlem gerçekleştiren sektörlerin başında gelen bankalar, e- ticaret siteleri, kamu kurum ve kuruluşlarının iç yönetmeliklerini bu kanun özelinde yenilemeleri gerekmiştir. Esasen bankalar özelinde müşteriler ile yapılan işlemlerde KVKK öncesinde de adı kişisel veri olmasa da "müşteri sırrı" kavramına rastlanmaktadır. 01.11.2005 tarih 25983 sayılı Resmî Gazetede yayımlanan Bankacılık Kanunu özellikle müşteri işlemlerinde dikkat edilecek durumları belirtmesi açısından önemlidir.

Bankacılık Kanunu'nun Sırların saklanması başlıklı 73. maddesinde *"Kurul başkan ve üyeleri ile Kurum personeli, Fon Kurulu başkan ve üyeleri ile Fon personeli görevleri sırasında öğrendikleri bankalara ve bunların bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıkları ve müşterilerine ait sırları bu Kanuna ve özel kanunlarına göre yetkili olanlardan başkasına açıklayamaz ve kendilerinin veya başkalarının yararlarına kullanamazlar. Kurumun dışarıdan destek hizmeti aldığı kişi ve kuruluşlar ile bunların çalışanları da bu hükme tâbidir. Bu yükümlülük görevden ayrıldıktan sonra da devam eder"* ibaresi görülmektedir (Bankacılık Kanunu, 2005).

Bu maddede müşteri sırrı kavramından bahsedildiği, ilgili sırrın üçüncü kişilerle paylaşılmaması, kendileri ve başkaları yararına kullanılması üstünde durmuştur.

Bankacılık Kanunu'nun Müşteri hakları başlıklı 76. maddesinde "*Bankalar, müşterilerinin, verilen hizmetlerden kaynaklanan her türlü sorularına cevap verecek bir sistem kurmakla ve bu hizmetle ilgili bilgiyi müşterilerine bildirmekle yükümlüdür. Bankalar, kredi sözleşmelerinin onaylı bir örneğini müşterilerine vermek zorundadır. Talepleri hâlinde müşteri ile yapılan diğer işlemlere ilişkin her türlü belgenin bir örneği de müşterilere verilir."* ibaresine yer verilmiştir.

Bu madde ile müşterilerle yapılacak işlemlerin müşteri bilgilendirilerek yapılması, yapılacak sözleşmelerin yazılı olarak oluşturulması, bu yazılı sözleşmenin bir nüshasının müşteriye verilmesinin uygun olduğu belirtilmiştir.

Bankacılık Kanunu'nun Sırların Açıklanması başlıklı 159. maddesinde *"Bu Kanunun 7'üncü maddesinin birinci ve üçüncü fıkralarında belirtilen yükümlülüğe uymayanlar için bir yıldan üç yıla kadar hapis ve bin günden iki bin güne kadar adlî para cezası hükmolunur. Banka ve müşterilere ait sırları açıklayan üçüncü kişiler hakkında da aynı cezalar uygulanır"* ibaresi yer almaktadır. Bu madde ile de bankalar tarafından müşteri sırrını üçüncü kişilerle paylaşan veyahut bu sırları banka veya kişisel amaçları doğrultusunda kullanılmasının adli para cezası ile cezalandırılacağı öngörülmüştür.

Bankacılık Kanunu, Kişisel Verileri Koruma Kanunu'nun öncesinde müşteri sırrı kavramını, bu sırrın korunmasının gerekliliğini belirtmesi, müşteri bilgilendirilmesinin önemini, müşteri ile yapılacak her türlü işlemin sözleşme ile yazılı getirilmesini bir çerçeve haline getirmesi açısından önemlidir. Kredi kartı müşterilerinden alınan bilgilerin banka içindeki veri tabanlarında, fiziksel ortamda saklama, silme şekilleri, Banka içi ve dışından gelebilecek tehditlere karşı alınan birtakım önlemler bulunmaktadır. Bu önlemler Kişisel Verileri Koruma Kanunu Veri Güvenliği Rehberinde teknik ve idari olmak üzere ikiye ayrılmıştır (Kişisel Verileri Koruma Kurumu, 2018).

3.2.1 Teknik önlemler

Yapılandırması Banka`ya göre hazırlanmış güvenlik duvarı ve ağ geçitleri tüm bankaların kullanmak zorunda olduğu güvenlik önlemleridir. Banka dışından çoğunlukla internet üzerinden gelen saldırılar bu şekilde engellenebilir. Güvenlik duvarı internet üzerinden gelecek tehlikeleri engellerken, ağ geçitleri ise banka personelinin ulaşabileceği internet sitelerini sınırlandırır.

Yama Yönetimi, banka tarafından kullanılan güvenlik yazılımın güncellenmesi, yama yönetimi adı verilen sürekli kullanılan donanım ve yazılım unsurlarının güncellenmesini sağlayan yönetim biçimlerinin önemi tartışılmaz olacaktır.

Erişim Sınırlaması, banka genelindeki kişisel verilere ulaşım için oluşturulacak görev ve rollere göre ayrılmış erişimlerin önemi büyüktür. (Erişim-yetki-kontrol matrisi) Bu erişimlerin süresi, görülebilecek kişisel verinin amacı, hangi kişisel verinin ne kadar boyutta olacağı önemli kriterler olarak belirlenmektedir.

Parola İşlemleri, banka sistemine girişlerde kullanıcı adı, parola ile sisteme giriş yapılmalı, tercih edilecek parolanın tahmin edilemeyecek şekilde düzenlenmesi amaç haline getirilmektedir. Parolaların belirli dönemler boyunca değiştirilmesi zorunlu tutulmaktadır. Bunun yanında kaba kuvvet saldırıları adı verilen şifreyi çözmek için kullanılan tehlikelerden korunmak için belirli sayıda şifre denemesine izin verilmektedir. İşten ayrılan çalışanların kullanıcı adı ve parolalarının sistemi girişinin engellenmesi sağlanmaktadır. Her türlü işlemi gerçekleştirebilen admin adı verilen kullanıcıların sadece ihtiyaç halinde kullanımı sağlanmaktadır.

Anti Virüs Yazılımları, zararlı yazılımlardan korunmak için kullanılabilecek en önemli önlemlerden biri de anti virüs programlarının kullanılmasıdır. Kullanılan yazılımların güncellemelerinin yapılması ve kontrolu yapılmaktadır.

Internet ile olan veri paylaşımlarında kullanılacak internet sitesinin yeterli güvenlik önlemlerine sahip olması sağlanmakta, teknolojinin gelişimi takip edilerek Secure Socket Layer (SSL) / Transport Layer Security (TLS) adı verilen internet sitelerinde veri sızıntılarını önlemeye yarayan sistemler kullanılmaktadır.

Veri Güvenliğinin Takibi, Veri Güvenliğini sağlamanın yanı sıra bu güvenliği korumak ve takibini yapmak da önemlidir. Bu sebeple bankalar; yapılan her türlü işlem kaydının tutulması (log kaydı), her türlü sızıntının bankanın diğer birimlerine ulaştırılması için raporlama sistemleri kurulmaktadır. Sistemi koruyan tüm yazılımların listesi yapılmakta, dönemler bazında kontroller yapılarak eksiklikler giderilmektedir. Sistemi koruyan tüm yazılımların uygun şekilde çalışıp çalışmadığının tespiti için Sızma testi adı verilen dışarıdan gelecek atakların bir örneği olan testlerin yapılması ve raporlanması sağlanmaktadır.

Veri Güvenliğini sağlarken verilerin saklandığı ortamların güvenilirliğine de dikkat edilmektedir. Verilerin yer aldığı fiziki ortamın sel, deprem, yangına karşı önlemleri alınmış bir ortam olması sağlanmakta, verilerin saklandığı kâğıt veyahut cihazların çalınmalara karsı güvenlikli bir ortamda tutulması sağlanmaktadır. Banka içinde veyahut dışında kullanılan elektronik postalarda, evrak ve işlemlerde kişisel veri kullanılıyor ise belirtilmekte ve farklı şekillerde sınıflandırılmaktadır. Örnek vermek gerekirse banka içinde gönderilen bir elektronik posta içerisinde kişisel veri var ise ilgili elektronik postanın kişisel veri içerdiği etiketlenmekte, böylece kontrolu sağlanmaktadır. Banka personelinin kullandığı kişisel telefon, bilgisayar vb. araçların

eğer banka ile ilgili bir veri akışında kullanılıyorsa, güvenlik önlemlerinin alınması sağlanmaktadır. Örnek olarak kişisel cep telefonu üzerinden banka e-posta adresi kullanılarak gönderilen e-postaların ekine ulaşılamaması verilebilir.

Verilerin Bulut Veri Tabanında Tutulması, Bankalar Denetleme ve Düzenleme Kurulu´nun (BDDK) 15.03.2020 tarih, 31069 sayılı Resmi Gazete `de yayımladığı "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" kapsamında *"Birincil veya ikincil sistemler kapsamında olan bir faaliyet için dış hizmet ya da bulut bilişim hizmeti alınması halinde, dış hizmet sağlayıcının sunduğu hizmete ilişkin faaliyetleri yürütmede kullandığı bilgi sistemleri ve bunların yedekleri de birincil ve ikincil sistemler kapsamında ele alınır ve yurt içinde bulundurulur."* ibaresi yer almaktadır. *Bu minvalde* Türkiye´deki bankalar ancak ve ancak Türkiye sınırları içerisinde bulut bilişim veri tabanlarını tutmak zorundadırlar. Bunun yanı sıra ilgili verilerin yedeklenmesi, senkronizasyonlarının sağlanması, iki faktörlü kimlik doğrulama ile güvenliğinin sağlanması gerekmektedir (Bankacılık Denetleme ve Düzenleme Kurulu, 2020).

3.2.2 İdari önlemler

Kişisel verilerin güvenliğini sadece teknik önlemler ile sağlamak mümkün olmamaktadır. Bunun yanı sıra birtakım idari önlemlerin de alınması gerekmektedir. Bu önlemler aşağıya çıkarılmıştır.

Kişisel verinin riskinin belirlenmesi, bankalar özelinde müşterilerden alınacak kişisel verilerin segmentlere ayrılması her bir segment özelinde veriye önem derecesi atanmaktadır. Bu risklilik derecesi belirlenirken bu verinin açığa çıkma olasılığı ve açığa çıkarsa vereceği zararın anlaşılması önemlidir. Bu risklilik derecesi belirlendikten sonra verinin korunması için yöntemler belirlenmektedir.

Her ne kadar teknik önlemler alınsa da veriyi banka içerisinde isleyen ve suistimale, hata yapmaya en açık olan mekanizma banka çalışanlarıdır. Bu sebeple banka çalışanlarına düzenli olarak kişisel veri farkındalık eğitimleri verilmektedir. Banka çalışanlarının yeterlilik ve kıdem süresi dikkate alınmadan tüm çalışanlara ilgili eğitimlerin atanması gerekliliktir.

Banka tarafından oluşturulacak riskli alanların belirlenmesi, bu riskli alanlardaki risklerin azaltılması için alınacak önlemler, bu önlemlerin kontrol edilme süreleri, banka genelindeki her bir çalışana ilgili politikanın anlatılması ve uygulatılması

sağlanmaktadır. Ayrıca bu politikalara uyumun sağlanamadığı durumlarda alınacak aksiyonların da belirlenmesi politikalar içerisinde belirtilmektedir.

Bankalar müşteriler ile ilişkilerinde müşteri talebinin dışında herhangi bir bilgi talebinde bulunmamalıdır. Bu bilgilerin bankaya getireceği ek risklerin farkında olmalı, özellikle daha önce ilişki kurulan müşterilerin kişisel verilerinin güncelliğini kontrol etmekte, söz konusu verilerin güncellenerek veri tabanlarında saklanması sağlanmaktadır.

Bankalar iç işleyişlerindeki eksiklikleri gidermek veyahut ek bir emek sarf etmemek için kanun denetleyici ve düzenleyici kurumlar tarafından belirlenen şartlar altında destek almaktadırlar. Destek alınan kuruluşlar ile herhangi bir durumda kişisel verilerin paylaşılması gerektiğinde banka mutlak surette müşterilerden yazılı bir form alarak verilerin destek firması ile paylaşılacağını beyan etmek zorundadır. Bunun yanı sıra Kişisel Verilerin Korunması Kanunu 12. madde de belirtildiği üzere destek alınan kurulusun kişisel verileri koruma kanunu hükümlerine uyması gerekliliği bulunmaktadır. Destek alınan kuruluş ile yapılan sözleşmede paylaşılan verilerin özellikleri, önem derecesi, riskliliği, hangi amaç ile kullanılacağının belirtilmesi gerekmektedir (Kişisel Verilerin Korunması Kanunu, 2016).

Bankacılık Kanunu sonrası tezimizin de ana temasını oluşturan kredi kartları için özel olarak oluşturulmuş Banka ve Kredi Kartları Kanunu da kişisel veri kavramının önemini ve özellikle bir bankacılık ürünü olan kredi kartları kapsamında alınacak önlemleri belirtmesi açısından önemlidir. Banka ve Kredi Kartları Kanunu 23.02.2006 tarih, 26095 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir. Bu kanunun amacı kartların çıkarılması ve kullanılmasına ilişkin kuralları belirlemektir (Banka Kartları ve Kredi Kartları Kanunu, 2006).

Kanunun Kart çıkarma ve buna ilişkin yükümlülükler başlıklı 8. maddesinde; *"Kart çıkaran kuruluşlar, talepte bulunmayan veya sözleşme imzalamayan kişiler adına hiçbir şekil ve surette kart veremezler."* ve *"Kart çıkaran kuruluşlar, kartın verilmesi anında kart hamilini yeteri derecede bilgilendirmek ve talep edilmesi halinde, gerçekleştirilmiş işlemlere ait kayıtları otuz günü geçmemek üzere işlemin mahiyetine uygun bir süre zarfında sağlamakla yükümlüdür."* ibaresi yer almaktadır.

Kanunun Kredi Kartı Limiti başlıklı 9. maddesinde; *"Kart çıkaran kuruluşlar, kredi kartı almak isteyen kişilerin yasaklılık veya engel durumu, ekonomik ve sosyal durumu,*

aylık veya yıllık ortalama geliri, diğer kart çıkaran kuruluşlarca bu kişilere tahsis edilen kredi kartı limiti, bir model veya skorlama sistemi sonuçları, müşterini tanı ilkeleri ile 29 uncu madde çerçevesinde temin edilecek bilgileri dikkate alarak yapacakları değerlendirmeye istinaden kullanım limiti tespit etmek zorundadır." ibaresi yer almaktadır.

Kanunun Hesap Özet başlıklı 10. maddesinde; *"Kurulca belirlenecek usul ve esaslar çerçevesinde, kredi kartı hesap özeti düzenlenmesi, yazılı veya kart hamilinin talebi üzerine elektronik ortam veya başka etkin yollarla bildirilmesi zorunludur."* ibaresi yer almaktadır.

Kanunun Bilgilerin saklanması başlıklı 23. maddesinde; *"Üye işyerleri, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına açıklayamaz, saklayamaz ve kopyalayamaz. Üye işyerleri, kart bilgilerini üye işyeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamaz, satamaz, satın alamaz ve takas edemez. Üye işyeri anlaşması yapan kuruluşlar, bu fıkranın uygulanmasını gözetmekle yükümlüdür. Kart çıkaran kuruluşlar, edindikleri kişisel bilgileri gizli tutmak, kendi hizmetlerinin pazarlanması dışında başka amaçlarla kullanmamak ve kanunla yetkili kılınan kişi, kurum ve kuruluşlar dışında kalanların bu bilgilere ulaşmasını engellemek amacıyla gereken önlemleri almakla yükümlüdür."* ibaresi yer almaktadır.

Kanunun Sırların saklanması isimli 31. maddesinde; *"Kurul üyeleri ile Kurum personeli, görevleri sırasında öğrendikleri bu Kanun kapsamındaki kuruluşlara, kart hamillerine ve kefillere ait sırları kanunen açıkça yetkili olanlardan başkasına açıklayamaz ve kendi yararlarına kullanamazlar."* ibaresi yer almaktadır.

Banka ve Kredi Kartları Kanunu`nun uygulanması için bir yönetmeliğe ihtiyaç duyulmuş ve bu yönetmelik Banka ve Kredi Kartları Kanunu Hakkında Yönetmelik başlığı ile 10.03.2007 tarih 26458 sayılı Resmî Gazete 'de yayımlanarak yürürlüğe girmiştir (Bankacılık Düzenleme ve Denetleme Kurumu, 2008).

İlgili Yönetmeliğin 17. maddesinde; "*Kart çıkaran kuruluşlar ile kart hamilleri arasındaki ilişkiler, Kanun ve ilgili diğer mevzuat çerçevesinde Kanunun 24'üncü maddesinin birinci fıkrasında belirtilen yöntemler yoluyla kurulacak sözleşmeler ile düzenlenir. Sözleşmenin kullanılan uzaktan iletişim aracına uygun olarak en az on iki*

punto büyüklüğünde, açık, sade, anlaşılabilir ve okunabilir bir şekilde olması ve bir örneğinin kâğıt üzerinde veya kalıcı veri saklayıcısı ile kart hamiline ve varsa kefiline verilmesi zorunludur." ve "Kart teslimi sırasında veya kart tahsisini müteakip teslimden önce banka kartı hamillerine aşağıda yer alan hususlarda kâğıt üzerinde veya kalıcı veri saklayıcısı ile bilgilendirme yapılması zorunludur. Kart hamilinin sorumluluğunun kartın zilyetliğine geçtiği andan itibaren başlayacağı ve kartın imza hanesinin kart hamili tarafından imzalanması gerektiği, kart hamilinin, kartı ve kartın kullanılması için gerekli şifre bilgilerini güvenli bir şekilde koruması ve bu bilgilerin başkaları tarafından kullanılmasına engel olacak önlemleri alması gerektiği, bunların kaybolması, çalınması halinde veya iradesi dışında gerçekleşmiş herhangi bir işlemi öğrenmesi durumunda kart çıkaran kuruluşa derhal bildirim yapmak zorunda olduğu, kart hamilinin, yapacağı kayıp veya çalıntı bildiriminden önceki yirmi dört saat içinde gerçekleşen hukuka aykırı kullanımdan doğan zararlardan yüz elli Yeni Türk Lirası ile sınırlı olmak üzere sorumlu olacağı, bildirimin yapılmaması halinde bu sınırın uygulanmayacağı, kart hamilinin yüz elli Yeni Türk Lirası tutarındaki sorumluluğunun sigortalanmasına ilişkin usul ve esaslar, yabancı para cinsinden yapılan işlemlerde bankaca uygulanacak kurun belirlenme esasları ve bunun hesap özetine yansıtılmasına ilişkin esaslar, şifrenin üçüncü kişilerle paylaşılmaması ve üçüncü kişilerin eline geçmemesi için gerekli önlemlerin alınması gerektiği, kayıp veya çalıntı durumunda bildirimde bulunulabilecek yöntemler ve kanallar, kart kullanımı hakkında ayrıntılı bilgi alınabilecek diğer yöntemler ve kanallar, sözleşmede belirtilen ücret, komisyon ve masrafların kart hamilinin hesabına borç kaydedileceği, kart hamilinin adres ve diğer iletişim bilgilerinde meydana gelen değişiklikleri on beş gün içinde bildirmesi gerektiği, kart teslimi sırasında veya kart tahsisini müteakip teslimden önce kredi kartı hamillerine aşağıda yer alan hususlarda kağıt üzerinde veya kalıcı veri saklayıcısı ile bilgi verilmesi zorunludur. İkinci fıkrada yer alan hususlar, kart limiti, kartın düzenlendiği tarihteki faiz oranları, dönem borcunun bir kısmının ödenmesi halinde kalan hesap bakiyesi üzerinden faiz hesaplanacağı, kalan hesap bakiyesine, asgarî tutar ve üzerinde ödeme yapılması durumunda akdi faiz, asgarî tutarın altında ödeme yapılması durumunda ise asgari tutarın ödenmeyen kısmı için gecikme faizi, kalan hesap bakiyesinin asgari tutarı aşan kısmı için akdi faiz uygulanacağı da dahil olmak üzere, kart uygulamasından doğan borçlarda bileşik faiz uygulanmayacağı, kart borcunun öğrenilebileceği ve ödenebileceği yöntemler ve kanallar," ibareleri bulunmaktadır.

Yönetmeliğin 22. maddesinde; **"***Kart çıkaran kuruluşlar, kredi kartı almak isteyen kişilerin yasaklık veya engel durumu, ekonomik ve sosyal durumu, aylık veya yıllık ortalama geliri, diğer kart çıkaran kuruluşlarca bu kişilere tahsis edilen kredi kartı limiti, bir model veya skorlama sistemi sonuçları, müşterini tanı ilkeleri ile 27'nci madde uyarınca kurulacak bilgi alışverişi şirketlerinden temin edilecek bilgileri dikkate alarak yapacakları değerlendirmeye istinaden kullanım limiti tespit etmek zorundadır. Kurul tarafından Kanunun 9'uncu maddesinin ikinci fıkrası kapsamında 47'nci maddesi uyarınca belirlenen tutardaki limitler hariç olmak üzere, aylık veya yıllık ortalama gelir düzeyi, kart hamili tarafından beyan edilen ve ilgili kuruluşlarca teyit edilen gelirler üzerinden tespit edilir. Kart çıkaran kuruluşların, müşterileri hakkında müşterinin kredi ödeme performansı, varlık ve yükümlülükleri, sosyal statüsü, eğitim düzeyi, yaşı ve benzeri ödeme gücünün değerlendirilmesinde etkili olabilecek hususlara ilişkin alacakları beyan ve temin edecekleri belgeler çerçevesinde yapacağı değerlendirmeler ilgili kuruluşça yapılacak teyit niteliğini taşır. Kart çıkaran kuruluşlar, karşılığı nakit, nakit benzeri kıymet ve hesaplar ile kıymetli maden olması durumunda, karşılık olan tutarı geçmemesi ve rehin sözleşmesi yapılması şartıyla, gelir beyanı ve gelir teyidi zorunluluğuna tabi olmaksızın kredi kartı limiti tespit edebilir."* ibaresi bulunmaktadır.

Türkiye`deki bankaların işlemlerini denetleyen düzenleyen otoritelerin kredi kartı uygulamalarının güvenliğini sağlamak, müşteriyi meydana gelecek zararlardan korumak için yukarıda bahsi gecen yönetmelikler çıkarmasına sebebiyet vermiştir. Söz konusu kanun, yönetmeliklerin bankalar özelinde nasıl işlendiği aşağıda belirtilmiştir.

Bankaya kredi kartı başvurusu yapacak müşteri, şube veyahut alternatif dağıtım kanalları (internet bankacılığı, mobil uygulama) kullanabilmektedir. Şube veyahut alternatif dağıtım kanalları kullanılarak yapılacak kredi kartı başvurularında Banka ve Kredi Kartları Kanunu 8. madde ve Kişisel Verileri Koruma Kanunu 13. madde ve Banka ve Kredi Kartları Kanunu Hakkında Yönetmelik`in 17.2 maddede belirtildiği üzere ilgili müşteriye kredi kartı başvuru formunun doldurulması beklenmektedir. Bu form içerisinde ad soyad bilgisi, sosyal güvenlik numarası, doğum tarihi, cinsiyet, elektronik posta adresi, çalışılan iş bilgileri, gelir bilgisi, medeni durumu bilgileri, ev/iş adresi, telefon numarası alınmakta olup müşterilere "Kişisel Verileri Koruma Kanunu Aydınlatma formu" adı verilen formun müşteriye onaylatılması gerekmektedir. Bu

formun içeriğinde paylaşılan kişisel verilerin işlenmesi, aktarılması, saklanması ve imhası konusunda müşteri hakları yer almaktadır.

Bankaya müşteri başvuru formu ile başvuran müşteri için gelir bilgileri, ödeme alışkanlıklarının belirlenmesi ve bu finansal bilgiler göz önünde bulundurularak kredi kartı limit tahsisi yapılmaktadır. Her banka kendi limit tahsis yöntemleri kullanarak risk iştahlarına göre kredi kart limit tahsisi gerçekleştirmektedirler. Bu limit belirleme süreci esasen Banka ve Kredi Kartları Kanunu 9.madde ve Banka ve Kredi Kartları Hakkında Yönetmelik 22. madde ile uyumludur.

Bankaya kredi kartı başvurusu yapan müşterilerin limit tahsisi gerçekleştirildikten sora kredi kartı bilgilerini içeren bir yazılı belge alınması gerekmektedir- Bu belge her banka özelinde değişmekte olup "Ürün Bilgi Formu" olarak adlandırılmaktadır- Bu form içerisinde kullanılacak kredi kartının adı, limiti, akdi ve gecikme faizi, hesap kesim tarihi, hesap, ödeme tarihi, kart borcunun öğrenilebileceği ve ödenebileceği uygulamaları bildirilmektedir. Bu bilgilendirme formu Banka ve Kredi Kartları Kanunu Hakkında Yönetmelik`in 17.3 maddesinde bildirilmiştir.

Bankaya kredi kartı başvurusunda bulunan, kendisine limit belirlenen müşteri ile son olarak bir sözleşme imzalanması gerekmektedir. Bu sözleşme içeriğinde banka ve müşterinin tüm yasal hakları, faiz oranları, sözleşme tarihi, hesap özeti işlemleri hakkında ayrıntılı bilgiler verilmektedir. Bu sözleşmenin yapılması, Banka ve Kredi Kartları Kanunu, 8.madde, Banka ve Kredi Kartları Kanunu Hakkında Yönetmelik 17.1 maddesi göz önünde bulundurularak işlem yapılmaktadır.

Kredi kartına sahip olan müşteriler kredi kartı ile yaptıkları harcamaların özeti kredi kartı ekstresi veyahut kredi kartı hesap özeti adı verilen, müşterice kredi kartı başvuru formunda belirtilmiş dönem ve iletişim kanalı ile görebilmektedirler. Banka ve Kredi Kartları Kanunu 10. madde ve Banka ve Kredi Kartları Kanunu Hakkında Yönetmelik'in 19.maddesinde yer verilmiştir.

Kredi kartı müşterilerinden alınan kişisel verilerin banka içinde ve dışında kullanımı, 3. Taraflar ile paylaşımı ne şekilde yapılacağı önemli bir konu haline gelmiştir. Bu konu ile alakalı olarak yapılan çalışmalarda bankalardan bilgi talep etmeye yetkili kurum ve kuruluşlar tam olarak hangi bilgi isteniyorsa o bilginin verilmesi, mümkün değil ise verilerin silinmesi veyahut maskelenmesi gerekmektedir. Kişisel Verilerin Korunması Kanunu`nun 4. ve 5. maddelerinde kişisel verinin paylaşılma şartlarına

uygunluk açısından söz konusu silme veyahut maskeleme işlemlerinin yapılması elzemdir (Kişisel Verilerin Korunması Kanunu, 2016).

Tezimizin bu bölümünde Avrupa ve Türkiye `deki bankalar için uygulanan kişisel veri düzenlemelerinden bahsedilmiş, bu düzenlemelerin bankalara getirdiği kurallar ve bu kuralların uygulanış şekilleri hakkında bilgi verilmiştir. Bankalar tarafından kişisel verinin korunması açısından alınan teknik ve idari önlemlerden bahsedilmiş, özellikle kredi kartı başvuru işlemleri ile ayrıntılı hale getirilmeye çalışılmış. Bankalar tarafından alınan bu önlemlerin her ne kadar değerli olsa da insan faktörünün kişisel veri ihlallerinde etkin bir rol oynadığı söylenebilir. Tezimizin bir sonraki başlığı Dünya ve Türkiye özelinde meydana gelen kişisel veri ihlallerini, nedenlerini gösterecek ve bizlere kişisel verinin bankalar ile olan ilişkilerde ne kadar korunabildiği konusunda bir istatistik verecektir.

4. VERİ İHLALLERİ

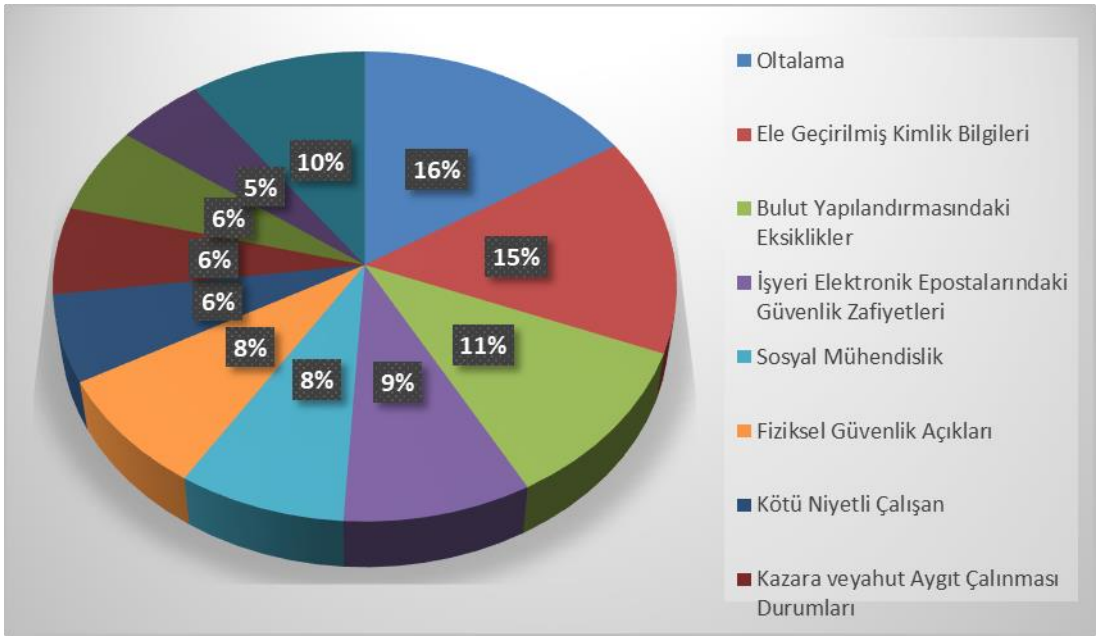
Veri İhlalleri Avrupa Birliği General Data Protection Regulation (GDPR)`de veri ihlali; *"...iletilen, saklanan veya işlenen kişisel verilerin kazara yasadışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlali"* olarak tanımlanmıştır (European Union , 2016). Kişisel Verileri Koruma Kanunu'nda ise tam olarak veri ihlali tanımı yapılmasa da Kanunun 12. maddesinde veri sorumlusunun alması gereken önlemlerden bahsedilmiş ve *"işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir."* ibaresine yer verilmiştir. Bu ibare ile veri ihlalini kanuni olmayan yol olarak tanımladığını söyleyebiliriz (Kişisel Verilerin Korunması Kanunu, 2016).

IBM tarafından 2023 yılı Veri İhlalleri Raporu`nda bir veri ihlalinin maliyetinin 4,45 milyon Amerikan doları olduğu, 2022 yılı ile kıyaslandığında bu oranın 4,35 milyon Amerikan doları olduğu ve %2,3 oranında bir artış gösterdiği görülmüştür. Tezimiz konusu sebebi ile finansal kurumlardaki maliyete bakıldığında ise %5,9 milyon Amerikan doları olduğu, genel ortalamanın üstünde kaldığı görülmüştür. Araştırmanın en önemli baslıklarından biri de ilgili veri ihlallerinin kaynaklarına bakıldığında görülebilir. Finansal kurumlara yapılan saldırıların %48'i kötü niyetli kişiler tarafından başlarken, %33'ü insan hatasından oluşuyor (IBM, 2023).

Çalışmanın devamında maliyeti yaratan en büyük kalemin Personel Identifiable Information adı verilen müşteri ve şirket çalışanlarının bilgileri olduğu, 2023 yılı için isim, sosyal güvenlik numarası vb. kişisel verilerin kayıt başına 183 Amerikan doları, çalışan bilgilerinin ise 181 Amerikan doları masrafa sebebiyet verdiği görülmüştür. 2023 yılı içerisinde ihlal edilen veri tipi olarak tüm ihlallerin %52'sine sahip veri tipinin bahsi gecen Personel Identifiable Information -PII adı verilen müşteri ve şirket çalışanlarının bilgileri olduğu görülmüştür (IBM, 2023).

Şekil 4.1'de görüldüğü üzere meydana gelen veri ihlallerinin yöntemlerine odaklanıldığında göze çarpan en büyük tehlikenin oltalama adı verilen müşterileri

çekici vaatler, hediyeler ile kandırarak kimlik bilgilerine ulaşma yöntemi ile kullanılarak yapıldığı ve bu oranın tüm atakların %16 sini oluşturduğunu açıklamıştır. Diğer atak tipleri ise istatistiklerine göre %15 ile çalıntı veya ele geçirilmiş kimlik bilgileri, %11 ile bulut yapılandırmasındaki eksiklikler, %9 ile işyerine ait elektronik postalardaki güvenlik eksiklikleri, %8 ile sosyal mühendislik, %8 ile fiziksel güvenlik eksiklikleri, %6 ile kötü niyetli çalışanlar, %6 ile kazara yapılan veyahut elektronik aygıt çalınması nedeni ile meydana gelen veri ihlalleri, %6 ile bilinmeyen ve yama yapılmayan durumlar ve son olarak %5 ile sistemsel hatalar görülmektedir.



Şekil 4.1: IBM tarafından yapılan 2023 yılı Veri İhlalleri Raporu Sonuçları

Comparitech tarafından Amerika Birleşik Devletleri özelinde 2018 yılı ocak ayı ile 2023 yılı Eylül yılları arası için yapılan veri ihlalleri çalışmasında finans alanındaki 2.260 adet veri ihlalleri sonucunda 232 milyon veri kaydının sızdırıldığı belirlenmiştir. Genel olarak bankalar, 2018'den bu yana takip edilen tüm finansal veri ihlallerinin yüzde 32'sini (720 adet ihlal) oluşturarak en fazla hedef alınan kuruluşlar oldukları, bunları sigorta şirketleri (563 adet ihlal) ve yatırım şirketleri (201 adet ihlal) takip ettiği belirtilmiştir. Bilgisayar korsanlığının (Ransomware) veri ihlalleri için en popüler yöntem olduğu, ihlallerin üçte birinin bu şekilde gerçekleştiği (2.260 ihlalden 734'ü). Kart ihlalleri (banka/kredi kartı ayrıntılarını içeren dolandırıcılık), 320 adet ihlalle ikinci en yüksek saldırı yöntemi olduğu araştırmada belirtilen önemli istatistiklerdir.

Araştırmada finans sektörünün karşı karşıya olduğu bir diğer zorluğun da fidye yazılımları olduğu, 2018 yılından 2023 yılı haziran ayına kadar finans sektörüne yönelik fidye yazılımı saldırıları ABD ekonomisine yalnızca aksama süresi nedeniyle 16,35 milyar dolara mal olduğu belirtilmektedir. Aynı şekilde son yıllarda finans sektöründe meydana gelen fidye yazılımı saldırılarının sayısı azalırken, etkilenen kayıtların sayısında da keskin bir artış yaşandı. 2022 yılında, finansal kuruluşlara yönelik fidye yazılımı saldırılarında 3,5 milyon kaydın ihlal edildiği; 2023'te ise bu sayı 9,2 milyon olduğu görülmektedir (Comparitech, 2022).

Avrupa Birliği ülkelerindeki istatistiklere bakılırsa SecurityScorecard tarafından yapılan araştırmada 2022 yılında, Avrupa Birliği'ndeki en büyük 240 bankanın %78'inin üçüncü taraf veri ihlaline maruz kaldığını ortaya çıkardı. Ancak bu ihlallere rağmen üçüncü taraf satıcıların yalnızca %3'ü ihlal edildi; bu da bir basın açıklamasına göre bilgisayar korsanlarının tedarik zinciri yazılımını kullanan tüm kuruluşlara erişim sağlamak için tedarik zinciri saldırılarını kullandığını gösteriyor (Security Scorecard, 2022).

Yukarıda verilen istatistiklerde dünya genelinde veri ihlallerinin artış gösterdiğini, bu artısın meydana gelmesinde finansal piyasa sektörünün büyük bir aktör olduğunu, veri ihlallerini önlemek için oluşturulan sistemlerin tamamen koruma sağlayamadığı, bu sistemlere harcanan tutarların giderek arttığı ve son olarak veri ihlallerinde çalınan verilerin büyük çoğunluğunun müşteri kimlik olduğu sonucu çıkarılabilir.

Tezimizin geri kalanında Dünyadaki finansal sektörlerde meydana gelen veri ihlalleri hakkında bilgiler verilecektir.

4.1 Dünyadan Veri İhlalleri Örnekleri

Dünya genelinde teknolojinin gelişmesi, e-ticaretin yaygınlaşması, finansal piyasaların iç içe geçmesi finansal piyasanın hareketlenmesine sebebiyet vermiştir. Finansal piyasalardaki bu genişleme beraberinde hem idari hem de teknik güvenlik önlemlerinin önemini de arttırmıştır. Fakat her ne kadar önlemler alınsa da veri ihlallerinin olması engellenememiştir. Buradaki amaç riskin azaltılması olmalıdır. Aşağıda Dünya genelinde meydana gelen özellikle finansal piyasalardaki veri ihlalleri örnekleri çıkartılmıştır.

Equifax, Amerikan çok uluslu bir tüketici kredisi raporlama ajansı olarak 1899 yılından beri hizmet vermektedir. İlgili firma müşterilerinin kişisel ve finansal verilerini kullanarak kredi raporlama sistemi üzerinden müşterilerine çıktı olarak kredibilite raporu sunmaktadır. 2017 yılında veri tabanlarından birinde yama yapılmamış Apache Struts çerçevesi (Java web application) nedeniyle 150 milyon müşterisinin kişisel ve finansal bilgilerini kaybetmiştir. Bu süreçte ilgili firma güvenlik açığını geç fark etmiş, bu süre zarfında da kamuoyunu bilgilendirmemiştir. Temmuz 2019'da kredi kurumu, Federal Ticaret Komisyonu, Tüketici Mali Koruma Bürosu (CFPB) ve 50 ABD eyaleti ve bölgesinin tamamı ile yapılan görüşmeler sonucu potansiyel olarak 700 milyon dolara çıkacak olan 575 milyon dolar ödemeyi kabul etmiştir. Ayrıca ihlal nedeniyle Birleşik Krallık'ta 500.000 İngiliz sterlini ödemesine karar verilmiştir.

Home Depot, Amerikan çok uluslu inşaat aletleri ve hizmeti satan şirket olarak kredi veyahut banka kartı ile ödeme yapılan POS sistemleri sebebi ile 2014 yılının Nisan ve Eylül ayları arasında 50 milyondan fazla kredi kartı numarası ve 53 milyon e-posta adresi çalınmasına sebebiyet vermiştir. Üçüncü taraflar Home Depot'un veri ağına girerek POS sistemine ulaşmıştır. Home Depot POS sağlayıcıları olan banka ve kredi kartı kuruluşlarına 134,5 milyon Amerikan doları buna ek olarak 2017 yılında 25 milyon Amerikan doları ödeme yapmıştır.

Capital One, kredi kartları, otomobil kredileri, bankacılık ve tasarruf hesapları konusunda işlem yapan Amerika Birleşik Devletleri menşeli bir firmadır. İlgili firma Amazon bulut sistemlerindeki yanlış yapılandırmanın bir Amazon çalışanı tarafından belirlenmesi ve kötü amaçla kullanılması sebebi ile yaklaşık 100 milyon müşteri verisinin sızdırılması olayına karışmıştır. 2019 yılında meydana gelen olay sonrasında ilgili firma müşterilerine 190 milyon Amerikan doları, ABD Para Denetleme Ofisi'ne ise 80 milyon Amerikan doları ceza ödemiştir.

First American Financial Corporation, Amerika Birleşik Devletleri menşeli bir firma olup, emlak sektörü, sigortalama, ipotek işlemleri gerçekleştirmektedir. Bu şirketin web sitesindeki güvenlik açığından dolayı 2018 yılının mayıs ayında müşterilerinin 885 milyondan fazla mali ve kişisel bilgisi açığa çıkmıştır. Söz konusu web sitesindeki kişisel verilere giden bağlantının kullanıcı erişimini doğrulamak için kimlik koruma politikası sunmadığı görülmüştür. Buradaki hatanın nedeni bir siber saldırı değil,

firmanın güvenlik sistemlerini konfigürasyonunu güvenli hale getirememesi, gerekli güncellemelerin yapılmaması kaynaklı olduğu görülmektedir.

JP Morgan Chase &Co, Amerikan menşeli bir yatırım bankası olup, dünya genelinde büyük bir müşteri havuzuna sahiptir. 2014 yılında Brezilya`dan ilgili bankanın veri tabanlarına yapılan saldırılar sonucu 83 milyon hesap bilgilerinin çalındığı bilgisi almıştır. Saldırının "high administrive privilege" kazanılarak "root access" e ulaşılarak meydana geldiği bilinmektedir. Bu saldırıda en önemli durumun yalnızca belirli müşterilerin bilgilerinin çalınması olmuştur.

Kanadalı bir yatırım bankası olan Desjardins Group 2019 yılında isinden memnun olmayan bir çalışanı sebebi ile 4,2 milyon müşterisine kişisel bilgileri açığa çıkmıştır. İlgili çalışan bu verilere privilige access ile erişim sağlamış, ilgili banka içerisinde etkin iç kontrol önlemlerinin alınmadığı ortaya çıkmıştır. Bunun yanı sıra bankanın işlem yaptığı diğer firmaların da bu durumdan etkilendiği, 1,8 milyon kredi kartı sahibinin de verilerinin sızdırıldığı ortaya çıkmıştır. Bu veri sızıntısı firmaya 108 milyon Amerikan doları maliyete sebebiyet vermiştir.

Avustralya Merkezli çok uluslu bir banka olan Westpac, 2013 yılında diğer bankalarla iletişimi sağlayan cep telefonu numarası veya e-posta adresiyle bankalar arasında transferleri kolaylaştıran üçüncü taraf sağlayıcısı PayID aracılığıyla bir kaba kuvvet (deneme yolu ile bilgilere ulaşılabilen bir saldırı türü) saldırısına maruz kalmıştır. Bu saldırı sonucu 98.000 müşteriye ait kişisel bilgilerin çalındığı belirlenmiştir.

Amerika Birleşik Devletleri`nin en önemli finansal kuruluşlarından biri olan Flagstar Bank 2022 yılında 1,5 milyon müşterisine ait verinin açığa çıkması ile karşı karşıya kalmıştır. Bu saldırının üçüncü taraf işlemleri sebebi işlem meydana geldiği söylenmiş, 2022 yılında ortaya çıkan bu durumun 2021 yılından beri süregeldiği öğrenilmiştir.

4.2 Türkiye'deki Veri İhlallerine Örnekler

Türkiye`deki veri ihlallerine örnekler, özellikle Kişisel Verileri Koruma Kurulu`nun sitesinde yer alan örneklerle desteklenmeye çalışılmıştır. Bankaların kurum olarak Kişisel Verileri Koruma Kurumu`na yaptıkları bildirimler ve bireysel şikâyetlere ayrı yer verilmiştir (Kişisel Verileri Koruma Kurumu, 2023).

4.2.1 Bankaların yaptıkları bildirimler

2019 yılında Türkiye `de bireysel ve ticari işlemlerde bulunan Denizbank AŞ'nin Beylerbeyi/İstanbul Şubesi'nde yapılan Teftiş Kurulu çalışmaları sonucunda ilgili şubede görev yapan bireysel işlemlerden sorumlu çalışanın Temmuz 2018 - Mayıs 2019 tarihleri arasında banka müşterisi olan 3.038 kişi ve banka müşterisi olmayan 2.851 kişiye ait bilgileri banka sistemi üzerinden sorguladığı, bu sorgulamaların gereğinden fazla olduğu görülmüş, söz konusu müşteri bilgilerinin üçüncü taraflarla paylaşıldığı kanaatine varılmıştır.

Türkiye `de bireysel ve ticari işlemlerde bulunan Türk Ekonomi Bankası AŞ'nin 2019 yılında Alanya/Antalya ve Gebze Akse Sapağı/Kocaeli Şubesi`nde yapılan Teftiş Kurulu çalışmaları sonucunda toplam 3 çalışanın 10 Temmuz 2017 ve 26 Haziran 2019 tarihleri arasında 17.582 banka müşterisinin ve 7.706 banka müşterisi olmayan kişi için bankalara bireysel nitelikteki bilgileri sunan Kredi Kayıt Bürosu sistemi üzerinden gereğinden fazla sorgulama yaptıkları, bu müşterilere ait T.C. Kimlik numaralarını üçüncü taraflardan temin edip, ilgili T.C. kimlik veriler ile bağlantılı diğer kişisel bilgileri elektronik ortamlarda paylaştıkları kanaatine varılmıştır.2020 yılında yapılan tespit ile banka çalışanlarının 6.917 banka müşterisi, 2.317 banka müşterisi olmayan kişinin kredibilitelerinin olup olmadığını gösteren raporları şahsi telefonları aracılığı ile üçüncü kişilerle paylaştıkları görülmüştür.

2019 yılında Türkiye `de bireysel ve ticari işlemlerde bulunan Türkiye Garanti Bankası AŞ'nin bir çalışanı tarafından 346 müşterinin şube numarası, hesap numarası, cep telefonu numarası ve bu müşterilerin banka hesaplarından belirli bir yatırım firması hesabına gönderdikleri tutarların, banka dışından bir başka kişiye elektronik e-posta ile gönderildiği, gönderilen elektronik posta sahibinin ilgili Garanti Bank A.S çalışanının farklı bir yatırım bankasında çalışan bir tanıdığı olduğu tespit edilmiştir.

2019 yılında Türkiye `de bireysel ve ticari işlemlerde bulunan Türkiye Garanti Bankası AŞ'nin rutin veri sızıntısı testlerinde bir şube çalışanının müşterilerin risk merkezi bilgilerini (müşterilerin diğer banka ve finansal kuruluşlardaki bilgileri) elektronik e-posta ile banka dışına çıkardığı, bu verileri üçüncü taraflar ile para karşılığında paylaştığı tespit edilmiştir.

Kişisel Verileri Koruma Kurumu'na yapılan bireysel başvuralar incelendiğinde, bankada hem ticari hem de bireysel müşteri olarak işlem yapan bir müşterinin şikâyeti

incelenmeye değer görülmüştür. İlgili müşterinin kendi adına olan bireysel hesap bilgileri ve kredi kartı ekstresinin " h,,,,,@gmail.com adresine gönderilmesi gerekirken, müşterinin ortağı olduğu firmanın ticari işlerini, hesaplarını, ekstreleri yürüttüğü "y…@gmail.com" adresine sehven gönderildiği, sehven gönderimin yanı sıra ilgili ekstrenin pdf formatında (Portable Document Format; Taşınabilir Belge Biçimi) iletildiği, iletilen ekstrenin ilgili e-maili açan herkes tarafından açıkça ulaşılabilir olduğu, bu durum sonucunda müşteri ortağına ait olan kişisel harcamaların, ortağı olduğu firmanın diğer ortakları tarafından görüldüğünü belirtmiştir. Kurum bunun üzerine gerekli incelemeleri başlatmış ve isleme konu olan hesap sahibi bankanın Kişisel Verileri Koruma Kanunu`nun 8 inci maddesine aykırı bir "kişisel veri aktarımı gerçekleştirmiş olduğu" ve bu yönüyle veri sorumlusu bankanın, Kanunun 12'nci maddesinin birinci fıkrası kapsamında "kişisel verilerin hukuka aykırı işlenmesini önlemek ve muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı" kanaatine ulaşılmış ve 60.000 TL idari para cezası ödemesine hükmedilmiştir.

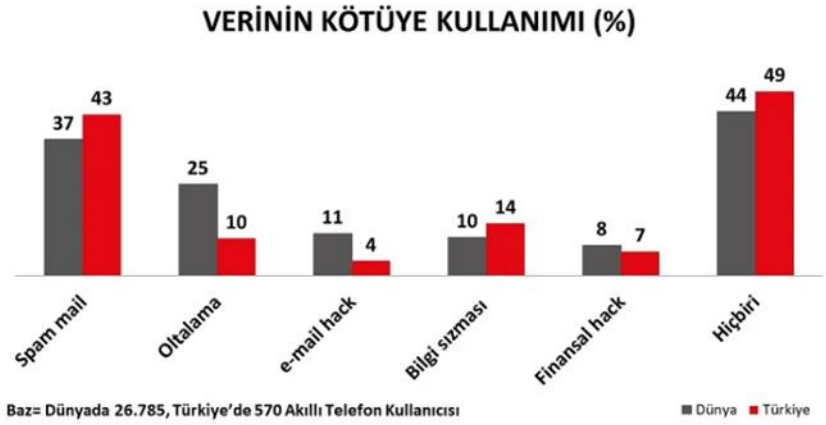
Tezimizin bu bölümünde Dünya`da ve Türkiye`de özellikle bankalar özelinde gerçeklesen müşteri veri sızıntılarına yer verilmiştir. Verilen örneklerde veri sızıntılarının temelde 3 farklı şekilde gerçekleştiği, ilkinin bankanın kendi güvenlik sistemlerindeki yeterli güvenlik seviyesini oluşturamaması olduğu, ikinci olarak banka dışından gelen siber saldırılar ve son olarak banka içindeki çalışanlar tarafından banka dışına çıkarılan veriler olarak gerçekleştiği söylenebilir. Özellikle Türkiye`deki örneklerde meydana gelen veri sızıntılarının üçüncü kategoride yer aldığı, banka içerisinde çalışanların, banka ve müşteri verisinin dışarıya çıkarılması, üçüncü kişilerle maddi kazanç olsun olmasın paylaşılması konusunda önemli bir sorun olduğu görülmüştür. Dünyada ve Türkiye`de kişisel verileri koruma kanunları ve bu kanunların öncü olduğu yönetmelikler, iyi uygulama rehberleri hem idari hem de teknik olarak tezimizin önceki bölümlerinde de bahsettiğimiz gibi veri sızıntılarını önlemeye, en aza indirmeye çalışmaktadır. Fakat görüldüğü üzere banka çalışanları olarak gösterebileceğimiz insan faktörünün varlığının bunu tamamen sağladığı söylenemeyecektir. Buna ek olarak bankalar tarafından alınan müşteri verilerin ne kadar fazla ve çeşitte olduğunu, bu sebeple herhangi bir saldırı veyahut veri sızıntısı durumunda bankaların karşılaşabileceği sorunların temin ettikleri kişisel veriler kadar büyük ve çeşitlilikte olacağı düşünülmektedir.

Tezimizin bundan önceki bölümlerinde Dünyada ve Türkiye'de kişisel veri sızıntılarının kredi kartı ve e-ticaretin artması ile birlikte arttığını, bankalarda özellikle kredi kartı özelinde başvuru süreçlerini, alınan kişisel bilgileri, müşterilere verilen bilgiler ve sözleşmelerin nasıl olduğunu, Dünyada ve Türkiye`de kişisel verilerin korunması için mevcut kanun ve uygulamaları, bu kanun ve uygulamaların kredi kartı uygulamalarına nasıl sirayet ettiği, alınan idari ve teknik önlemleri, alınan önlemlere rağmen meydana gelen veri ihlalleri anlatılmıştır. Tezimizin bundan sonraki bölümünde ise kişisel verinin sızdırılması sonucunda elde edilen veri ne için ve nasıl kullanılabilir, neden bu verilerin üçüncü tarafların eline geçmesi istenmemektedir vb. soruların cevabi bulunmaya çalışılmıştır.

5. KİŞİSEL VERİLERIN SIZDIRILMASININ SONUÇLARI

Dünyada ve Türkiye`de kişisel verilerin en azından otoriteler bazında dikkate alındığı, kanun ve uygulamaların oluşturulduğu, bu kanun ve uygulamalara uyumun zorunluluk haline getirildiği söylenebilir. Özellikle bankacılık sektöründe müşteri olma, banka ürün ve hizmetlerinden faydalanmak için kişisel verilerin alınması bir süreç haline gelmiştir. Bu süreç içinde müşteri olarak hangi verilerin kullanılmasına izin verdiğimiz, haklarımızın neler olduğu banka ile yapılan sözlemse ve dokumanlar kayıt altına alınmaktadır. Herhangi bir durum sonucunda kişisel verilerin sızdırılması bankalara büyük yaptırımlara sebep olmakta ve Kişisel Veriler Kanunu'nda yer almaktadır.

Alınan idari ve teknik önlemlerin etkili olmadığı durumlarda meydana gelen veri sızıntılarının hangi amaçlarla kullanıldığı araştırılmış, BAREM'in WIN Group iş birliğiyle gerçekleştirdiği araştırma sonuçlarının bu konuda baz bilgi verdiği görülmüştür (BAREM, 2021). Bu araştırmaya göre; 40 ülkede akıllı telefon sahibi 26785 kişiyle Türkiye'de ise akıllı telefon kullanan 570 kişi baz alınarak yapılmış olup, ilgili kişilere son 2-3 yılda kişisel verilerinin kötüye kullanımı ile hangi durumlarla karşılaşmış olabilecekleri sorulmuş, gelen cevapların spam e-posta alma, oltalama maili alma, e-mailinin ele geçirilmesi, kişisel verilerinin sızdırılması ve banka hesabı ya da kredi kartının ele geçirilmesi olduğu kaydedilmiştir. Bu cevapların sonuçlarına bakılmış ve aşağıda yer alan Şekil 5.1 şeması meydana gelmiştir.



Şekil 5.1: BAREM WIN Global Teknoloji Araştırması

Tablo incelendiğinde Dünyada kişisel veri sızıntıları sonucunda en çok spam e-posta alındığı, oltalama saldırıları ile karşılaşıldığı, e-mailin ele geçirildiği, bilgilerin sızdırıldığı, (farklı kişilere iletildiği) ve maddi kazanç sağlamak için kullanıldığının düşünüldüğü görülmüştür.

Türkiye özelinde en çok alınan cevaba göre sıralandığında; spam maillerin alındığı, bilgilerin sızdırıldığı (farklı kişilere iletildiği), oltalama saldırıları ile karşılaşıldığı, maddi kazanç sağlamak ve son olarak e-posta ele geçirmek için kullanıldığı düşünülmektedir.

2021 yılında yapılan bir araştırma, kişisel verilerin kişisel tatmini sağlamak, kişilere zorlayıcı teşviklerde bulunmak, kişilerin uyumluluğunun izlenmesi, itibarsızlaştırma, ayrımcılık, kişilerin zayıf noktasına ulaşmak, kişileştirilmiş ikna yöntemi olarak kullanma, kişisel veri sahibiyle iletişime geçme, kişisel veri sahibinin fiziki lokasyonuna ulaşmak, korunan alanlara ulaşmak, veri sahibinin eylemlerine ve planlarına stratejik tepki vermek, hükümet yetkililerinin veri sahiplerini izlemek ve kontrol etmek istemesi amaçları sebebi ile sızdırıldığını belirtmektedir.

Dünya genelinde kişisel verilerin kötüye kullanımının daha net anlaşılabilmesi için sadece bankacılık sektörü için değil, tüm sektörlerde bazı örnekler verilmeye çalışılmıştır.

Birleşik Krallık menşeli, siyasi veri analizi ile ilgilenen Cambridge Analytica firmasının 2018 yılında Facebook kullanıcılarının verilerini Amerika Birleşik Devletleri`nin başkanlık seçimlerinde oy veren vatandaşları manipüle etmek için kullandığı ortaya çıkmış ve bu olay ortaya çıktıktan sonra davalarla uğraşmak zorunda

kalmıştır. İlgili Facebook kullanıcıları verilerinin kullanılması için açık bir rıza göstermediği, bırakın üçüncü taraflarla paylaşılması, Facebook`un bile bu verileri islemeye hakkinin bulunmadığı görülmüştür.

Twitter, 2019 yılında kullanıcılarına ait verileri e-posta ve telefon numarası bilgilerini reklam veren firmalarla paylaşıldığını, veri sızıntısının sebebinin şirket içi bir hatadan meydana geldiği açıklanmıştır. Rekabet içerisinde kalmak, Pazar payını arttırmak için reklam veren firmaların bu tip bir duruma başvurduğu Avrupa Birliği Rekabet Kurumu tarafından belirtilmiştir. Twitter, bu veri sızıntısı sebebi ile 2020 yılında ikinci bir dava ile karşı karşıya gelmiştir.

Morgan Stanley`de çalışan finansal bir danışman, 2015 yılında Morgan Stanley veri tabanında yer alan 730.000 adet müşteri verisini Morgan Stanley'in rakibi ile paylaştığı, bunun yanı sıra bu eski çalışana ait kişisel bilgisayarın içindeki 900 müşteriye ait kişisel verilerin, bilgisayar korsanları tarafından ayrıca ele geçirildiği tespit edilmiştir.

Birleşik Krallık menşeli Leave EU siyasi kurulusu ile Eldon Insurance Company arasında müşterilere ait veri alışverişi yapıldığı ortaya çıkmış, Birleşik Krallık Bilgi Komiserliği Ofisi 2019 yılında müşteri verilerini için her iki kuruluşa da yaklaşık 83.000 dolar para cezası verdiği görülmüştür. Bu iki firmanın sahibinin aynı kişi olması böylesi bir veri alışverişine olanak sağlamıştır.

Google `in, kullanıcılarının konum bilgilerini korumak için bir yöntem izlememesi ve bu müşteri konum bilgilerinin reklam veren firmalar tarafından kullanılması sebebi ile Fransız Veri Koruma yetkilileri tarafından 2020 yılında yaklaşık 57 milyon dolar para cezasına çarptırılmıştır. Aynı zamanda, İrlanda Veri Koruma Komisyonu, Google'ın konum bilgilerini paylaşıp paylaşmadığı, bu verileri nasıl koruduğunun tespiti yapmak için araştırma isteminde bulunmuştur (Invisibly, 2021).

Yukarıda verilen örnekler, müşteri verilerinin paylaşılmasının, bu verilerin kullanılmasının hem siyasi avantaj sağlamak hem de maddi kazanç sağlamak için kullanılabileceğini, pazarlama stratejilerinin artık kişisel veri temin etmek ve bu veri üzerinde analiz yapmak ile oluşturulduğu, kişisel verilerin paylaşılmasının bir ülkenin Başkanlık seçimini etkileyecek kadar büyük sonuçlara sebebiyet verdiği, ilerde daha büyük amaçlar için kullanılabileceğini göstermektedir.

6- KREDİ KARTI HESAP ÖZETLERİ (EKSTRELER) İLE KİŞİSEL VERİ ANALİZİ UYGULAMASI

Tezimiz bankacılık sektörü özelinde, kredi kartı ürünü için bankalar tarafından elde edilen verilerin neler olduğu, bu verilerin temin edilmesinde müşterilerden alınan yazılı izinler, kredi kartı kullanımı sonrasında meydana gelen hesap özetinin müşteriye iletilmesi, bu hesap özetinin hangi kanallar ile iletildiği hakkında bilgilerin verilmesi ile başlamış, Dünya ve Türkiye'deki mevcut kişisel verilerin korunması kanunları, uygulamaları, örnekleri ile desteklenmiş, bankaların kişisel verinin korunması için aldıkları idari ve teknik önlemler verilmiş ve bu önlemlerin yeterli olmaması sebebi ile meydana gelen veri sızıntılarına yer verilmiş, son olarak sızdırılan verilerin hangi amaçlarla kullanılabileceği hakkındaki haberler ile bitirilmiştir. Dikkat edildiği üzere her ne kadar önlemler alınsa dahi meydana gelen sızıntıları üzerinden özellikle maddi kazanç sağlama, siyasi basari ve bunun yanında pazarlama odaklı bir sürecin var olduğu görülmüştür. Tezimiz özelinde bu durumu konsantre halde nasıl gösterebileceğimi düşünülmüş ve farklı banka müşterilerine ait kredi kart ekstre bilgileri üzerinden kişisel veri temini sağlayarak, müşteri özelinde hangi sonuçlara ulaşabileceğimiz görülmek istenmiştir.

İşbu tezimizi desteklemek maksadı ile 5 farklı müşteriye ait 2021 Haziran-2023 Haziran dönemleri arasındaki hesap ekstreleri temin edilmiş, ilgili veriler aşağıda şekilde toplulaştırılmıştır.

Veri; costumer id, transaction date, transaction company detail, price, currency, tag, city, neighbourhood, mall şeklinde microsoft excel üzerinden hesap özetleri kullanılarak sadeleştirilmiştir.

- Costumer ID: "Müşteri Numarası"
- Transaction Date: "İşlemin Gerçekleştiği Tarih"
- Transaction Company Detail: "Yapılan İşlemin İçeriği"
- Price: "Yapılan İşlemin Tutarı"
- Currency: "Yapılan İşlemin Para Birimi"
- Tag: "Yapılan İşlemin Ana Başlığı"
- City: "İşlemin Yapıldığı Coğrafi Şehir"
- Neighbourhood: "İşlemin Yapıldığı İlçe"

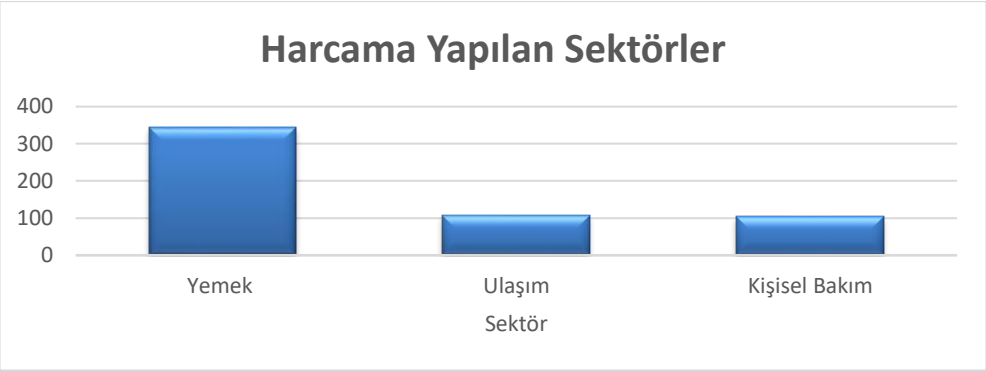
- Mall: “Alışveriş Yapılan İşletmenin Fiyat Seviyesi” i olarak belirlenmiştir.

Tezimiz için hesap özeti temininin 5 farklı müşteri özelinde kalmasının nedeni; Kişisel Verileri Koruma Kanunu sebebi ile temin edilememesi, bahsi gecen 5 müşteri haricinde müşterilerin kendi istekleri ile hesap özetlerini paylaşmak istememesidir. Bu sebeple mevcut 5 müşteri üzerinden Structured Query Language (SQL) veri dili kullanılarak 100 adet müşteri ve bu müşteriler için yapay kredi kartı işlemleri oluşturulmuştur.

Söz konusu yapay müşteri tabanı üzerinden mevcut 100 müşteri için oluşturulan müşteri verisi yalnızca Microsoft Excel kullanılarak analiz edilmeye çalışılmış ve aşağıdaki sonuçlara ulaşılmıştır.

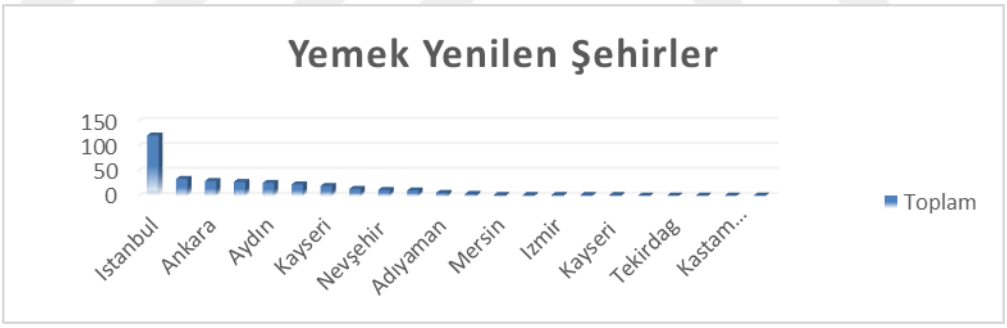
“5” numaralı müşterinin Haziran 2021-Haziran 2023 dönemi içerisinde;

286.508,1605 Türk Lirası tutarı ve 1.458 işlem ile toplam harcama tutarı en yüksek müşteri olduğu, ortalama yıllık harcamasının 143.000.000 TL, aylık harcamasının ise ortalama 11.000 Türk Lirası olduğu, bu sebeple maaş seviyesinin 11.000 Türk Lirası üzerinde olabileceği, 621 adet işlem ile 2022 yılında en çok harcamayı yaptığı, Şekil 6.1’de de görüleceği üzere, 345 adet işlem ile en çok harcamayı yemek sektörüne harcadığı, yemek sektörünü, 277 adet harcama ile giyim sektörü, 154 adet ile market sektörü, 109 adet ile taksi/ulaşım sektörü ve 104 adet ile kişisel bakım sektörünün izlediği görülmüştür. Yemek sektörüne yaptığı harcamaların %33 yüzdeyle orta fiyat seviyeli restoranlarda olduğu, bu restoranların %46`sinin İstanbul ilinde yer aldığı, %30’unun ise Kadıköy ilçesinde yer aldığı, bu sebeple iş veyahut ev adresinin Kadıköy’de yer aldığı çıkarımı yapılmıştır.

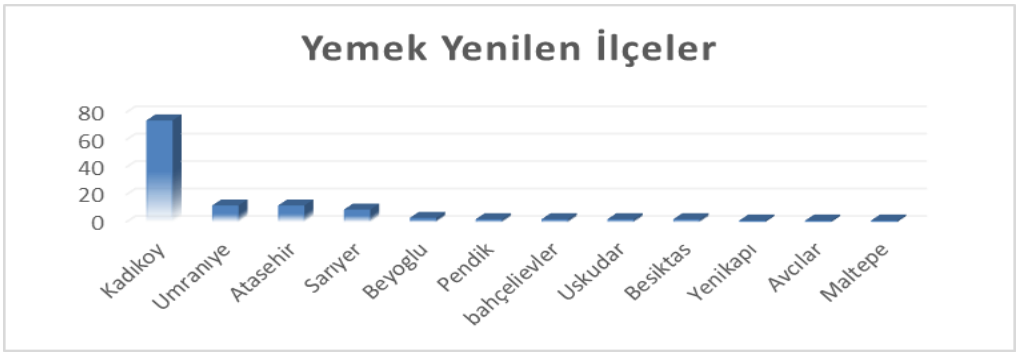


Şekil 6.1: Harcama Yapılan Sektörler

Şekil 6.2 ve Şekil 6.3 'de görüldüğü üzere, yemek sektörüne yaptığı harcamaların %32 ile düşük fiyat seviyeli restoranlarda olduğu, bu restoranların % 22'sinin Antalya`da, %17'sinin ise İstanbul'da, %15`inin Kayseri`de, %13`ünün Aydın'da %6,3'ünün Ankara`da, %6'sının Tekirdağ'da %5,4`ünün Adıyaman'da, %2,7'sinin Balıkesir'de yer aldığı, yaptığı harcama tarihlerine bakıldığında aynı il içinde aynı yılın aynı ayı içerisinde işlem yaptığı, böylece ilgili kişinin mesleğinin farklı il ve ilçelerin ziyaret edilmesi ile yapılan bir iş olduğu çıkarımı yapılmıştır.



Şekil 6.2: Yemek Yenilen Şehirler



Şekil 6.3: Yemek Yenilen İlçeler

Yemek sektörü içerisinde yaptığı harcamalarda Pub adı verilen alkollü içki mekânlarının yer aldığı, ayrıca ODTÜ başlıklı yemek mekânının bulunduğu, bu bilgilerle ilgili 5 numaralı müşterinin alkol kullanan biri olduğu, ODTÜ`de birinci dereceden yakını olduğu veyahut kendisinin ODTU mezunu olmuş olabileceği tahmini yapılmıştır.

İlgili müşteriye ait vergi ödemelerine bakıldığında, taşıt vergisi ödediği, ödenilen tutar kontrol edildiğinde, aracın 4-6 yaş arası, 114.000 km'yi aşmamış bir binek araç olabileceği, müşteriye ait ulaşım harcamalarına bakıldığında; Antalya, Ankara, Kayseri; Aydin, Tekirdağ illerine seyahat gerçekleştirdiği, ilgili seyahatler ile daha önce bahsi gecen yemek harcamalarının yapıldığı yerlerin uyumlu olduğu anlaşılabilmektedir.

Müşteriye ait sağlık harcamalarına bakıldığında %72 oranında İstanbul'un Kadıköy ilçesindeki özel bir hastanede yapıldığı, %28 inin ise Erzurum ilinde yer alan özel bir hastanede gerçekleştiği, Erzurum ilindeki özel hastanede yapılan harcamanın ilgili kişinin Erzurum'da bulunduğu zaman aralığında gerçekleştiği, buna ek olarak İstanbul Kadıköy ilçesindeki özel hastane işlemlerinin %27 sinin diş branşı ile ilgili olduğu, böylece ilgili müşterinin ev adresine yakın Kadıköy bölgesinde hastaneye başvurduğu, diş ile ilgili problem yaşamış olabileceği varsayılabilir.

İlgili müşteriye ait konaklama harcamalarına bakıldığında, ulaşım harcaması yaptığı Ankara, Kayseri, Antalya, Çerkezköy/Tekirdağ, Erzurum illerinde otel harcaması yaptığı, konaklama ve ulaşım harcama tarihlerinin birbirleri ile uyumlu olduğu, iş seyahati yapmış olabileceği öngörüsünün güçlendiği anlaşılmaktadır.

İlgili müşteriye ait kişisel bakim harcamalarına bakıldığında, %54 unun kişisel bakım mağazası alışverişi olduğu, %32 sinin ise kuaför masrafı olduğu, kuaförlerin adları ve adreslerine bakıldığında İstanbul Kadıköy adresinde ve kadın kuaförleri olduğu, böylece ilgili müşterinin cinsiyetinin kadın olabileceği tahmini yapılmıştır.

İlgili müşteriye ait giyim alışverişlerine bakıldığında, yemek sektöründen sonra en büyük harcamayı giyim sektörüne yaptığı, %45 inin orta fiyat seviyeli, %22 sinin yüksek fiyat seviyeli, %23 ünün ise düşük fiyat seviyeli olduğu, %5 inin ise gelinlik geriye kalan %5 inin ise takım elbise satan mağazalar olduğu, ilgili müşterinin takım elbise gerektirecek kamu veyahut beyaz yaka isinde çalıştığı, gelinlik harcaması sebebi ile evli veyahut nişanlı olabileceği kanaatine varılmıştır.

Yukarıda sadece bir müşteri özelinde yapılan basit bir analiz (hiçbir teknolojik analiz, yazılım kullanmadan) ile ilgili müşterinin maaş aralığı, cinsiyeti, ev ve iş adresi, işçi tanımı (beyaz yakalı olup olmadığı), seyahat gerektiren bir ise sahip olmadığı, kişisel varlıkları (araba sahibi olduğu) mezun olduğu okul, sağlık geçmişi (diş problemine sahip olduğu) hakkında tahminde bulunulmuştur.

İlgili çalışmayı mevcut 100 müşteri için tekrarladığımızda;
Müşterilerin yaptığı kişisel bakim harcamaları baz alınarak 92 adet müşterinin kadın kuaförünü kullandığı, makyaj malzemesi alışverişi yaptığı bu sebeple cinsiyetinin kadın olarak belirlenebileceği görülmüştür.

Müşterilerin yaptığı akaryakıt harcamaları ve araç sigortası ödemeleri baz alınarak 34 adet müşterinin araç sahibi olabileceği tahmin edilmiştir.

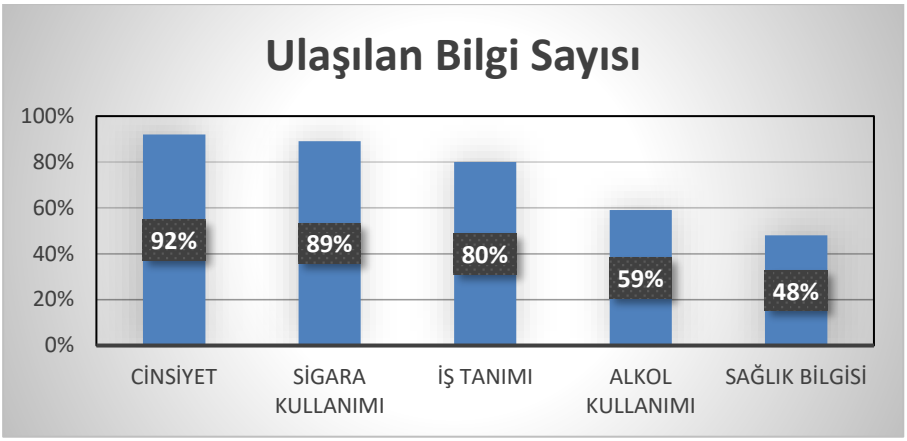
Müşterilerin yaptığı eğlence masraflarına bakıldığında 59 adet müşterinin alkol kullanıyor olabileceği kanısına varılmıştır.

Müşterilerin yaptığı giyim alışverişleri arasında business etiketli takım elbise satılan giyim markaları baz alındığında müşterilerden 80 tanesinin beyaz yakalı olabileceği tahmini yapılmıştır.

Müşterilerin yaptığı sağlık harcamalarına bakıldığında, 47 müşterinin diş hekimi harcamaları yaptığı, 1 müşterinin kontakt lens kullanıyor, 75 müşterinin optik mağazaları üzerinden güneş gözlüğü alışverişi yapmış olabileceği tahmininde bulunulmuştur.

Müşterilerin yaptığı sağlık harcamalarına bakıldığında 89 müşterinin sigara kullanıyor olabileceği tespit edilmiştir.

Bir müşteri ve 100 müşteri için yapılan analizlerde; müşterilere ait veriler kullanılarak azımsanmayacak kişisel bilgilere ulaşıldığı, müşterilerin yaptığı harcamaların yerleri, tarihleri, işlem tutarları, sıklığı bilgisi alınarak ilgili müşterilere ait *cinsiyeti, işçi tanımı (beyaz yakalı olup olmadığı), kişisel mal varlıkları (araba sahibi olduğu) sağlık geçmişi (diş problemine sahip olduğu), alkol ve sigara kullanımı* hakkında tahminde bulunulabildiği görülmüş, ilgili tahminlerin oranları Şekil 6.4 ‘de verilmiştir.



Şekil 6.4: Ulaşılan Bilgi Sayısı

Tezimizin diğer bölümlerinde de bahsedildiği üzere Dünyada ve Türkiye'de alınan her türlü idari ve teknik önlemlere rağmen veri sızıntısının mümkün olduğu ve teknolojinin gelişmesiyle e-ticaretin giderek artış göstermesi ile veri sızıntısında artış olacağı tahmin edilebilir. Alınan önlemler ve yapılan çalışmaların ana amacı müşterilerden alınan verilerin islenmesini önlemek, uygun ve güvenli bicimde saklamak ve belirli amaçlarla islenmesine izin vermek üzerine kuruludur. Bu minvalde eğer kişisel veri sayısının azaltılması mümkün olsaydı bu kadar veri sızıntısı ve önleme gerek olup olmadığı sorusu karşımıza çıkmaktadır. Tezimizin ana konusu olan kredi hesap süreci göz önüne alındığında sürecin başından sonuna kadar müşterilerden birçok kişisel verinin temin edildiği görülebilir. Bankalar tarafından istenen bu verilerin azaltılması mümkün olsaydı, veri sızıntılarının bu seviyelere ulaşamayacağı görüsü ile mevcut sisteme alternatif bir sistem oluşturulmaya çalışılmış, bu sistemin en iyi kriptografik yöntemler kullanılarak oluşturulabileceği düşünülmüştür. Dünyada kriptografik yöntemlerin kullanılması, müşterilerin anonim hale gelme hali önem kazanmakta ve desteklenmektedir (Aydın, Kurt, & Özdemir, 2021). Fakat bankacılık ve e-ticaret herhangi bir anlaşmazlığın, iadenin; suistimal içeren işlemin, kamu davalarının konusu olabilir ve bu durumlarda anonimlik kullanılamaz hale gelmektedir. Bir kullanıcının gizliliği, o kullanıcının kimlik doğrulama şemasına bağlıdır. Kimlik doğrulama şeması asimetrik kriptografi kullanılarak oluşturulur, fakat asimetrik kriptografi yeterli anonimliği sağlamak için yeterli değildir. Bu durumda hem anonim olmayacak hem de anonim işlemini içinde barındıracak bir kimlik doğrulama sistemin kullanılması gerekmektedir. Bu sistem "grup kimlik doğrulama" adı verilen ve bulunduğu gruptaki tüm kullanıcıların kimliğini doğrulayan bir sistemdir.

Grup kimlik doğrulama; aynı anda birden fazla kullanıcının üyeliğinin onaylanmasını, aynı anda kullanıcı sayısının doğrulanması ve tanımlanması işlemlerini gerçekleştirmesi sebebi ile özellikle anonimlik ile kimlik doğrulamayı beraber sağlamayı mümkün kılacaktır (Aydın, Kurt, & Özdemir, 2021).

Grup kimlik doğrulaması kanıtlayıcı ve bir doğrulayıcıya sahip olan çoğu geleneksel kullanıcı kimlik doğrulama şeması gibi bire bir kimlik doğrulama türü olmayıp, birden çok kanıtlayıcıya ve birden çok doğrulayıcıya sahip çoktan çoğa bir kimlik doğrulama türüdür.

Grup kimlik doğrulama şeması temel olarak iki asamadan oluşmaktadır. "Initialization" adı verilen ilk aşamada, grubun yöneticisi, gruptaki her üye için bir kimlik bilgisi olusturmakta ve güvenli ağlar üzerinden göndermektedir. İkinci asama olan "authentication" aşamasında ise her bir kullanıcı kendisine ait kimlik bilgisi ile bir token hesaplamakta ve yayımlamaktadır. Yayımlanan bu bilgiler tüm bu kullanıcıların ayni gruba ait olup olmadığının anlaşılmasında kullanılır. Grup kimlik doğrulama şemasındaki kullanıcıların yasal olup olmadığının tespiti iki şekilde yapılabilir, ilki eğer kullanıcı yasal değil ise kimlik doğrulama aşamasına geçemeden sonlanacaktır. Çünkü kimlik bilgisi olmadan authentication aşamasına geçememektedir. İkinci olarak ise üye olmayan herhangi birinin grup üyesi gibi davranması mümkün değildir çünkü kimlik bilgisin bulunmamaktadır.

Tezimiz özelinde ilgili grup kimlik doğrulamasının uygulandığı düşünülürse kabaca; Bankalararası Kart Merkezi'nin Grup Yöneticisi olarak belirleneceği, kredi kartı sürecinde görev alacak diğer aktörlere (kredi kartı kullanan müşteri, müşterinin alışveriş yaptığı satıcı, satıcı ve alıcıların bankaları ve son olarak kredi kartı kuruluşları (Mastercard, Visa) kimlik bilgisi oluşturacak ve bu bilgiler güvenli ağlarla iletilmesi gerekecektir. Kendilerine iletilen kimlik bilgilerini kullanan diğer aktörler bir token hazırlayacak ve bunu yayımlayacaktırlar. Bu tokenler yayımlandıktan sonra kimin yasal grubun içinde olup olmadığının tespiti kolaylıkla yapılacaktır. Böylece tezimizin de amacını oluşturan üçüncü kişilerin müşteri verisine erişmesini engellemek, kişisel veri teminini azaltmak ve kimlik doğrulamayı sağlayarak dava, kara para aklama veyahut anlaşmazlıklarda anonimleşmenin yarattığı sıkıntıların üstesinden gelmek kolaylaşacaktır (Zia, 2019).

7. SONUÇ

Teknolojik gelişmelerin akıl almaz bir hızla artıyor oluşu Dünya ve Türkiye'deki teknoloji ile büyüyen ve gelişen bankacılık sektörü ve e-ticaret alanının karşılaştığı risklerin de artmasına sebep olmaktadır. Bu risklerin bertaraf edilebilmesi için Dünya Genelinde en başta General Data Protection Regulatıons olmak üzere hem kişisel verileri baz alarak bireysel müşterileri koruyan bir uygulamalar bütünü oluşturulmuştur. Türkiye`de ise General Data Protection Regulatıons'ın karşılığı olarak Kişisel Verilerin Korunması Kanunu ortaya çıkmış, tezimiz özelinde yoğunlaştığımız kredi kartların için ise Banka ve Kredi Kartları Kanunu ve ilgili yönetmelikler meydana getirilmiştir. İdari olarak bu tip önlemlerin alınması, kişisel verilerin sızdırılmasında önleyici olmuş, bunlara ek olarak bankalar ve e-ticaret siteleri tarafından virüs koruyucular, ağ güvenliği, veri kaydetme ve imhasının nasıl yapılması gerektiği ile ilgili teknik önlemler alınmıştır. Fakat tezimizin daha önceki bölümlerinde de yer aldığı üzere her ne kadar önlemler alınsa da özellikle çalışanlardan kaynaklanan veri sızıntılarını engellemek, sosyal mühendislikten tamamen korunmak mümkün olmamaktadır. Bu sebeple müşterilerden temin edilen kişisel verilerin çeşidinde ve sayısında azalmaya gitmek, grup kimlik doğrulama yöntemi kullanarak hem anonimliği sağlamak hem de kimliği doğrulamayı sağlayan sistemlerin kullanılması önerilmiştir.

KAYNAKLAR

[1] **Aydın, Y., Kurt, G., & Özdemir, E.** (2021) *Group Authenticatıon for Drone Swarms*. IEEE.

[2] Banka Kartları ve Kredi Kartları Kanunu, (2006), *T.C. Resmî Gazete,* 26095

[3] Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, (2020), *T.C. Resmî Gazete,* 31069

[4] Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik, (2021), *T.C. Resmî Gazete,* 31441

[5] Banka Kartları ve Kredi Kartları Hakkında Yönetmelik, (2008), *T.C. Resmî Gazete*, 27087

[6] Bankacılık Kanunu, (2005), *T.C. Resmî Gazete,* 25983

[7] Bankalararası Kart Merkezi, (2023), Erişim tarihi: 20.12.2023, https://bkm.com.tr

[8] Bankalararası Kart Merkezi, (n.d), Erişim tarihi: 25.12.2023, https://bkm.com.tr

[9] **BAREM**, *BAREM WIN Global Teknoloji Araştırması – 1*, [Elektronik Sürüm], İstanbul, 2021

[10] **Clearly Payments,** *The Growth of the Credit Card Industry in 2023,* [Elektronik Sürüm], ABD, 2023

[11] **Comparitech,** (2022), Erişim tarihi: 20.12.2023, https://www.comparitech.com

[12] Elektronik Ticaret Bilgi Formu, (2023), Erişim tarihi: 05.12.2023, https://www.eticaret.gov.tr

[13] **European Unıon,** (2007), Erişim tarihi: 03.12.2023, https://ec.europa.eu

[14] **Forbes Advisor,** *When Were Credit Cards Invented: The Hıstory of Credit Cards,* [Elektronik Sürüm], ABD, 2021

[15] General Data Protection Regulation, *European Union,* (2016)

[16] **IBM,** (2023), *2023 yılı Veri İhlalleri Raporu, [Elektronik Sürüm], ABD, 2023*

[17] **Invisibly,** (2021), *Data Misuse 7 Examples, ABD, 2021*

[18] **Kişisel Verileri Koruma Kurumu,** (2023), Erişim tarihi: 25.12.2023, https://kvkk.gov.tr

[19] Kişisel Verilerin Korunması Kanunu, (2016), *T.C. Resmî Gazete,* 29977

[20] **Kredi Kayıt Bürosu,** (n.d), Erişim tarihi: 27.12.2023, https:// kkb.com.tr

[21] **Miva (2023*),*** *The History of e-commerce: How Did It All Begin,* ABD, 2023

[22] **Paratic,** (2016), *Visa ve MasterCard Arasındaki Farklar Nelerdir?* Erişim tarihi: 01.12.2023, www.paratic.com

[23] **Sakho, S., & Jianbiao, Z.** (2019). *Improving Banking Transactions Using Blockchain Technology.*

[24] **SecurityScorecard,** (2022), *SecurityScorecard Announces Significant Momentum in 2022, Growing by 49%,* ABD, 2022

[25] **Statista,** (2022), *Retail e-commerce sales worldwidefrom 2014 to 2026,* Erişim tarihi: 05.12.2023, https://www.statista.com

[26] Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, (2008), *T.C. Resmî Gazete,* 31324

[27] **Troy,** (n.d), Erişim tarihi: 03.12.2023, https://troyodeme.com

[28] Verileri Koruma Kanunu Veri Güvenliği Rehberi, (2018), *Kişisel Verileri Koruma Kurumu*

[29] **Zia, D.** (2019), *Cryptanalysis and Improvement of a Group Authentication Scheme with Multiple Trials and Multiple Authentications*

ÖZGEÇMİŞ

Ad-Soyad **:** Mahbub Dilan KOYUNCU KAYA

ÖĞRENİM DURUMU:

- **Lisans** **:** 2015, İstanbul Teknik Üniversitesi, İşletme Fakültesi, İşletme Mühendisliği
- **Yükseklisans** **:** 2018, Galatasaray Üniversitesi, Sosyal Bilimler Enstitüsü, Finansal Ekonomi Bölümü (Tezsiz)

ÇALIŞMA HAYATI:

- 2015 yılından itibaren Vakıflar Bankası T.A.O 'da Baş Müfettiş olarak çalışmaktadır.

YÜKSEK LİSANS TEZİNDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

- **Koyuncu Kaya M.D.,** Özdemir E. 2024. Protecting The Confidentiality of Personal Data in Bank Credit Card Processes with Big Data Methods. *International Congress – Fundamental and Applied Sciences (ICFAS 2024)*, July 9-11, 2024 İstanbul, Turkey.