İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

BİLGİ GÜVENLİĞİ, KİŞİSEL VERİLERİN KORUNMASI VE BİYOMETRİK VERİLERİN İŞLENMESİNE İLİŞKİN ÖNERİLER

YÜKSEK LİSANS TEZİ

Göksu Hazar ERDİNÇ

Bilişim Uygulamaları Anabilim Dalı

Bilişim Uygulamaları Tezli Yüksek Lisans Programı

Tez Danışmanı: Prof. Dr. Ertuğrul KARAÇUHA

KASIM 2017

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

BİLGİ GÜVENLİĞİ, KİŞİSEL VERİLERİN KORUNMASI VE BİYOMETRİK VERİLERİN İŞLENMESİNE İLİŞKİN ÖNERİLER

YÜKSEK LİSANS TEZİ

Göksu Hazar ERDİNÇ
(708141005)

Bilişim Uygulamaları Anabilim Dalı

Bilişim Uygulamaları Yüksek Lisans Programı

Tez Danışmanı: Prof. Dr. Ertuğrul KARAÇUHA

KASIM 2017

İTÜ, Bilişim Enstitüsü'nün 708141005 numaralı Yüksek Lisans Öğrencisi Göksu Hazar ERDİNÇ, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "BİLGİ GÜVENLİĞİ, KİŞİSEL VERİLERİN KORUNMASI VE BİYOMETRİK VERİLERİN İŞLENMESİNE İLİŞKİN ÖNERİLER" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Prof. Dr. Ertuğrul KARAÇUHA** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Prof. Dr. Mustafa ALKAN** Gazi Üniversitesi	.....
	Yrd. Doç. Dr. Çiçek ERSOY İstanbul Teknik Üniversitesi	.....

Teslim Tarihi : **17 Kasım 2017**
Savunma Tarihi : **14 Aralık 2017**

Aileme,

ÖNSÖZ

Bu çalışmada kişisel verilere ilişkin mevzuat, bilgi güvenliği kavramı ve biyometrik verilerin işlenmesi konuları araştırılmıştır. Bilgi güvenliği çerçevesinde kavramın özü irdelenerek teknik güvenliğin kapsamında olan kriptolojiden bahsedilmiştir. Kişisel verilere ve biyometrik verilere ilişkin olarak tarihçesi, terminolojisi, önemli düzenlemeler Avrupa Birliği, Türkiye ve diğer Avrupa, Asya ülkeleri ile karşılaştırmalı olarak yazılmıştır.

Kişisel verilerin korunması, bilgi toplumunda korunması gereken en önemli değerlerden bir tanesidir. Bu konuda kişisel verisi işlenen ilgili kişilerin ve kişisel verileri işleyen veri sorumluları ve veri işleyenlerin bilinçlendirilmesi ve gerekli denetim mekanizmalarının sağlanması büyük önem arz etmektedir. Yasal ve teknik önlemlerin bir arada alınarak gerekli stratejilerin belirlenmesi ile kişisel verilerin korunması en yüksek seviyede sağlanabilecektir.

Tez çalışmamın planlanmasında, araştırılmasında, oluşturulmasında, anketimin hazırlanmasında bana yol gösteren ve benden desteklerini esirgemeyen sayın hocam Prof. Dr. Ertuğrul Karaçuha'ya, sayın Mustafa Ünver'e ve Nur Saygı'ya, ve son olarak anketime katkıda bulunan tüm katılımcılara teşekkürlerimi sunarım.

Kasım 2017

Göksu Hazar Erdinç
(Avukat, Araştırma Görevlisi)

İÇİNDEKİLER

Sayfa

KISALTMALAR

AB	**:** Avrupa Birliği
ABD	**:** Amerika Birleşik Devletleri
AES	**:** Advanced Encrytion Standard (İleri Şifreleme Standardı)
AP	**:** Autoriteit Persoonsgegevens (Kişişsel Verileri Koruma Kurumu)
APPI	**:** Act on the Protection of Personal Data (Kişisel Verilerin Korunmasına İlişkin Yasa)
Auto	**:** Automatic (Otomatik)
BTK	**:** Bilgi Teknolojileri ve İletişim Kurumu
CNIL	**:** Commission Nationale de l'Informatiquenet Libertés (Ulusal Veri Koruma Komisyonu)
DDoS	**:** Distributed Denial of Service (Dağıtık Hizmet Engelleme)
DES	**:** The Data Encryption Standard (Veri Şifreleme Standardı)
DOJ	**:** Department of Justice (Adalet Bakanlığı)
ECC	**:** Elliptical Curve Cryptography (Eliptik Eğri Şifrelemesi)
FDA	**:** Food and Drug Administration (Gıda ve İlaç İdaresi)
GDPR	**:** General Data Protection Regulation
HHS	**:** Department of Health and Human Services (Sağlık ve İnsan Hizmetleri Bakanlığı)
ID	**:** Identification (Tanımlama)
INSEE	**:** Institut National de la Statistique et des Études Économiques (Ulusal İstatistik Ve Araştırmalar Enstitüsü)
KVKK	**:** Kişisel Verilerin Korunması Hakkında Kanun
LIL	**:** Loi Informatique et Libértes (Kişisel Verilerin Korunması Yasası)
MEDULA	**:** Medikal Ulak
NIST	**:** National Institute of Standards and Technology
PCC	**:** Personal Information Protection Commission (Kişisel Verileri Koruma Komisyonu)
PIN	**:** Personal Identification Number (Kişiyi Tanımlama Numarası)
RAM	**:** Random Access Memory
RC4	**:** Ark Four
SGK	**:** Sosyal Güvenlik Kurumu
SGK KDK	**:** Sosyal Güvenlik Kurumu Kimlik Doğrulama Kılavuzu (Biyometrik Yöntemlerle Kimlik Doğrulama Sistemlerine Ait Kılavuz)
SUT	**:** Sağlık Uygulama Tebliği
T.C.	**:** Türkiye Cumhuriyeti
VERBİS	**:** Veri Sicil bilgi Sistemi
Vb.	**:** ve benzeri
Ve/ya	**:** ve/veya
3DES	**:** Triple Data Encryption Standard (Üçlü Veri Şifreleme Standardı)

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

BİLGİ GÜVENLİĞİ, KİŞİSEL VERİLERİN KORUNMASI VE BİYOMETRİK VERİLERİN İŞLENMESİNE İLİŞKİN ÖNERİLER

ÖZET

Bilgi güvenliği, bilişim toplumu kavramının da ortaya çıkmasıyla birlikte önem kazanan kavramlardan birisi olmuştur. Türkiye'de de Devlet, bilgi güvenliğini sağlamak için çeşitli eylem planları hazırlamış ve bu eylem planlarını hayata geçirerek uygulamada birtakım yenilikler meydana getirmiştir.

Özel hayatın gizliliği ve bireylerin mahremiyeti gibi konular uluslararası hukuk mevzuatı uyarınca korunduğu gibi Türkiye Cumhuriyeti Anayasası ve Kanunlar çerçevesinde güvence altına alınmıştır. İnternetin gelişmesi ve sosyal medyanın sıkça kullanılmaya başlaması ile birlikte yeni bilişim suçları oluşmuştur. Devletin ceza kanunları ile cezalandırmaya tabi tuttuğu suçların bir kısmı dijital ortamlardan da işlenmeye başlamıştır. Örneğin bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme, banka veya kredi kartlarının kötüye kullanılması gibi suçlar 5237 Sayılı Türk Ceza Kanunu çerçevesinde düzenlenen bilişim suçlarındandır. Her ne kadar Türkiye mevzuatında Türk Ceza Kanunu, Elektronik İmza Kanunu, Fikri Mülkiyet Hukuku ve düzenlemelerle birtakım bilişim suçları düzenlenmiş olsa da; bireylerin mahremiyetini yakından ilgilendiren kişisel verilerin saklanması, işlenmesi, yok edilmesi, silinmesi, anonimleştirilmesi gibi kavramlar bilişim kültürüne girerek Devlet tarafından düzenleme yapılmasına ihtiyaç duyulmuştur. Kişisel verilerin olduğu kadar hem kamu hem özel sektörde tüzel kişilere ait veriler bilişim sistemleri aracılığıyla dijital ortama kaydedilmektedir. Kişisel verilerin düzenlenmesi ihtiyacı, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile giderilmiştir.

KVKK, 1995 yılında Avrupa Birliği tarafından çıkarılan 95/46 sayılı AB Verilerin Korunması Yönergesi de göz önünde bulundurularak yapılmıştır; ancak 25 Mayıs 2016 tarihinde 2016/679 Sayılı Kişisel Verilerin Korunması Tüzüğü (General Data Protection Regulation ("GDPR") yürürlüğe girerek AB Yönergesi güncellenmiştir. Yeni yönergede kişisel verilerin kullanılmasına yönelik yeni haklar, daha detaylı düzenlemeler yer almaktadır. Türkiye'deki kişisel veri mevzuatına göre daha detaylı düzenlenmeler mevcuttur. Türkiye kişisel veri mevzuatının AB düzenlemeleri temel alınarak oluşturulduğu ve kişisel verilerin işlenmesi ile ilgili uygulamadaki boşluklar düşünüldüğü takdirde Kanun'un güncellenmesi gerektiğini söylemek yerinde olacaktır. Kişisel verilerin korunması bakımından bir ülke ne kadar güvenilir ise o derecede gelişmiş olduğunu ve refah düzeyinin değerlendirileceğini söylemek yerinde olacaktır.

Kişisel veriler, genel olarak kişisel veriler ve özel nitelikli kişisel veriler olarak ikiye ayrılmaktadır. Kişinin adı ve soyadı, kimlik bilgileri, pasaport bilgileri, resmi, adresi gibi bilgiler kişisel veri kapsamında değerlendirilebilir. Özel nitelikli kişisel veriler ise kişiye ilişkin 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 verilerdir ve bu veriler hassas nitelikte olduğu için daha fazla koruma altına alınmıştır.

Özel nitelikli kişisel veri olan biyometrik veriler de en fazla başvurulan tekniklerden birisi olmuştur. Teknolojinin ilerlemesi ile birlikte biyometrik veriler, insanların hayatında önemli yer kaplamaya başlamıştır. Şifrelerin kolayca kırılabilmesi ve artık eskisi kadar pratik olmaması sebebiyle, her bir kişiye özgü, tek, kişilere ait biyometrik veriler kullanılmaya başlanmıştır. Biyometrik veriler özel nitelikli kişisel veriler olduğu için bu verilerin korunması büyük önem taşımaktadır. Yasal mevzuat kadar teknik olarak da yüksek güvenilirlikli sistemler aracılığıyla biyometrik verilerin işlenmesi ve saklanması da önem teşkil etmektedir. Bu doğrultuda, biyometrik verinin kullanım alanları, ilgili mevzuat hükümleri çeşitli ülkelerin mevzuatları ile karşılaştırılarak öneriler sunulacaktır.

RECOMMENDATIONS ON INFORMATION SECURITY, PERSONAL DATA PROTECTION AND PROCESSING OF BIOMETRIC DATA

SUMMARY

Information security has become one of the vital concepts which has gained importance together with the emergence of the concept of information society. Privacy, integrity and accessibility are regarded as the three elements of the information security. For the privacy element, it guides the State's policies as it can be seen that subjects related to secrecy in private life and privacy of individuals were regulated according to international law as well as being regulated by our national Constitutional law and Codes.

Firstly, it would be beneficial to determine that, together with the development of the internet and the frequent use of social media, new informatics crimes have come into the existence. Some of the crimes that were regulated by the Criminal Law are mainly; entering the information system, blocking the system, corrupting the data, destroying or changing the data, abusing the bank or credit cards. Although Turkish legislation enacted some criminal offenses in the Turkish Criminal Code, Electronic Signature Law, Intellectual Property Law and Regulations; the concepts of hiding, processing, destruction, deletion and anonymization of personal data which are closely related to the privacy of individuals needed a seperate regulation. As far as personal data is concerned, all public and private sectors collect, process and use personal data. In Turkey, the conditions and rules for processing the personal data are regulated by the Protection of Personal Data Act (Kişisel Verilerin Korunması Kanunu "KVKK") Numbered 6698.

Protection of Personal Data Act (KVKK) was adapted from the 95/46 numbered Directive on the Protection of European Union Data issued by the European Union; but the EU Directive was updated on May 25, 2016 with the entry into force of the 2016/679 numbered General Data Protection Regulation ("GDPR"). The new EU directive introduces new rights and more detailed regulations for the use of personal data. It would be beneficial to emphasize that since Turkey's personal data legislation is adapted from EU regulations, the personal data law needs to be updated. KVKK regulates the rules, conditions and punishments regarding the processing of personal data. General rules are determined within the context of KVKK. KVKK does not have as detailed provisions as GDPR. More detailed provisions will be regulated by the secondary law.

Secondly, personal data are generally divided into personal data and sensitive personal data. Information such as the name and surname of the person, identity information, passport information, social security number, address, telephone number, birth date can be evaluated within the scope of personal data. Sensitive personal data may include personal information relating to the person, such as his or her race, ethnicity, political thought, philosophical belief, religion or other beliefs, costume and clothing, association, foundation or trade union membership, health, sexual life, criminal conviction and security measures biometric and genetic data and so on. Sensitive data needs more protection due to its nature. If the sensitive datas are disclosed, the people may be subject to difficult situations such as ostracisation and so on.

Personal data shall be protected by legal and technical means. Legal regulations aim to deter persons from violating the law and influence both public and private sectors to collect, process, store personal data in a lawful manner. On the other hand, providing technical and physical security is as important as the legal regulations. Most of the personal data are stored in digital environment. Those digital environment shall be protected against cyber attacks in order to provide information security. Cryptography is one of the vital subjects which provide technical security for data protection. The encryption methods and descriptions will be evaluated within the context of the study.

Moreover, physical security means protecting the data against natural disasters (such as tsunami, earthquake, flood), extraordinary cases (such as fire), theft and so on. It would be beneficial to secure the digital devices such as databases, computers in a protected region.

The level of the personal data protection provides a competitive advantage to the firms, because the more security is provided by the company, the more trustworthy it will be. The State and people will rely on those firms regarding the collection, use, storage, processing the personal data. Many firms regarding the private and public sector collect personal data and shall comply with the legal regulstions and technical standards and policies.

Personal data are mostly used in the area of statistics, scientific and historical studies. As a result of this, the procedure of anonymization plays an important role in evaluating the personal datas. Those statistics help the firms and other bodies to identify people's needs and they carry on new studies or determine new policies regarding those information. Big data is especially used in categorising personal data, and sometimes the data are collected without taking the data subjects' consent. Since the explicit consent of the data subject (the person whose datas are processed) is not taken, ethical problems occur when the usage of Big Data is considered. However, the legal regulations should not prevent the development of technology. Consequently, a balance needs to be provided between the legal regulations and the technology.

There are many regulations worldwide ralated to the protection of personal data. Most of the regulations comply with each other, however thaere are also different policies and rules regulated within the scope of those regulations. Personal data law of Asia, Europe, Turkey and European Union will be evaluated in order to compare the personal data regulations and propose the ideal recommendations for the processing of personal data issue.

In addition to these, biometric data, which has the characteristic of a sensitive data, has been one of the most frequently used techniques recently. Together with the development of technology, biometric data has begun to take an important place in people's lives. Since the passwords can be easily broken and they are not practical as they were used to be, people began to use their bionmetric data for authentication. Biometric data is peculiar to people and it is impossible to forget the biometric datas because people are carrying the biometric data with them. Face recognition, voice recognition, finger prints, iris pattern recognition, DNA can be described as biometric datas that are frequently used.

What's more, it is also important to process and store biometric data through technically sophisticated systems as well as legal regulations. Biometric data help to prevent fraud, so it can be considered as one of the most practical and safe techniques to be used for authentication. In this direction, the usage areas of the biometric data will be presented by comparing the relevant legislation provisions with the legislation of various countries.

The aim of this study is to propose recommandations for protecting the personal data in the ideal level and determine the gaps in the existing regulations. A survey was prepared for identifying the awareness level of the people and to determine the problems occured in the field of data protection. The results of the survey will contribute to specify the needs, problems, and the opinions of the data subjects and data processors.

To sum up, personal data has been one of the important subjects when information security is taken into consideration. In the case of violation of processing the personal data, irrevocable risks may occur. The bigger the risk is, the more harmful results may realize. In addition to the regulations and supervision of the State, the institutions which take place in both public and private sector must take the necessary steps in order to comply with the regulation and provide the information security. Together with the survey results, and the evaluation of different personal data legislations, proposal will be given regarding enhancements, suggestions for personal data including biometric data protection in Turkey, as well as defining the risks and the vulnerabilities in this field.

1. GİRİŞ

Kişisel verilerin korunmasına ilişkin birçok ülkede düzenlemeler mevcuttur. Ülkemizde de 2010 yılında Anayasa ile güvence altına alındıktan sonra 7 Nisan 2016'dan tarihinden itibaren Kişisel Verilerin Korunması Hakkında Kanun ile yasalaşmıştır. Bilgi güvenliğini, kişisel verilerin korunması felsefesi, tarihçesi ve terminolojisini anlamak yasaların yorumlanabilmesi açısından önem arz etmektedir.

1.1 Tezin Konusu Ve Önemi

Teknolojinin ilerlemesi ile birlikte bilgi toplumu kavramı oluşmuştur. Bilgi toplumu söz konusu olduğunda ön plana çıkan en önemli konulardan bir tanesi ise kişisel verilerin korunmasıdır. Kişisel verilerin korunması uluslararası mevzuat uyarınca korunduğu kadar çeşitli ülkelerin ulusal hukuku çerçevesinde de koruma altına alınmıştır. Kişisel veriler, temel hak ve özgürlükler kapsamında bulunan mahremiyet kavramının bir uzantısı olarak değerlendirilebilir. Mahremiyet, "gizlilik" ile eş anlamlı olarak kullanılmaktadır ve gizlilik kavramı da bilgi güvenliğinin üç temel bileşeninden bir tanesini oluşturmaktadır [1]. Bilgi güvenliği konusunu açıklamak kişisel verilerin korunması kavramının özünü kavrayabilmek açısından önem arz edecektir. Bilgi güvenliği konusu, önemli tanımlar ile açıklandıktan sonra fiziksel ve teknik koruma sağlayan yönü öncelikle irdelenecektir. Bu kapsamda da Kriptoloji başlığı ile temel şifreleme yöntemleri açıklanacaktır. Yasal mevzuatlar kadar yüksek güvenilirlikli sistemler de kişisel verilerin korunması konusunda caydırıcılık sağlayacaktır. Kriptoloji başlığı altında temel şifreleme yöntemlerinin tanımlanması ile verilerin korunmasına ilişkin yöntemler belirlenecektir.

Bilgi güvenliğinin teknik ve fiziksel güvenlik yönü açıklandıktan sonra yasal açıdan incelenmeye başlanacaktır. Kişisel verinin korunmasına ilişkin yasal düzenlemeler açıklanmadan önce kavramın tarihçesi ve terminolojisi irdelenerek kişisel veri terminolojisinde önem arz eden kavramların vurgusu yapılacaktır.

Türkiye'de kişisel veriler ilk defa 30.01.2016 tarihli ve 6669 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun" ve 7 Nisan 2016 tarihli Resmi Gazete'de "6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un ("KVKK") yayımlanıp altı ay sonra 26 Ekim 2017 tarihinde yürürlüğe girmesiyle hukuki çerçevesine kavuşmuştur. Avrupa Birliği de AB üye ülkelerinin bilgi güvenliğini temin edebilmek ve yeknesak bir düzen oluşturmak suretiyle kişisel veri düzenlemelerinde güncellemeler yapmıştır. Bu çerçevede, AB yurttaşlarının kişisel verilerinin üçüncü ülkelere aktarılmasında birtakım prensipler benimsemiş ve yurttaşlarının verilerini teminat altına almak için düzenlemeler yapmıştır. KVKK uyarınca da kişisel verilerin işlenmesi, silinmesi, anonimleştirilmesi, aktarılması gibi hususlar düzenlenmiştir; ancak bu düzenlemeler detaylı olmayıp Yönetmelikler ile mevcut olan boşlukların doldurulması beklenmektedir ve bu doğrultuda öneriler de sunulmaya çalışılacaktır.

Kavramların özü ortaya konulduktan sonra Avrupa Birliği, Türkiye, Amerika ve Japonya'da mevcut olan kişisel veri düzenlemeleri karşılaştırmalı olarak ele alınacaktır. Çeşitli ülke mevzuatları ile Türkiye mevzuatı karşılaştırılarak mevzuattaki boşlukların tespiti ve ne şekilde güncellenebileceği hususlarını ifade etmede ışık tutacaktır.

Kişisel verilerin yetkisiz kişiler tarafından ele geçirilmesi durumunda tehlikeli sonuçlar ortaya çıkacaktır. Kişilerin kişisel verileri kullanılarak birçok işlem gerçekleştirilebilmektedir veyahut bu verilerin ifşa edilmesi durumunda kişiler zor durumda kalabilmektedir. Kişisel verilerin ihlâli durumunda telafisi çok zor sonuçlar ortaya çıktığı için bu durum büyük risk teşkil etmektedir. Ülkeler arası kişisel verilerin aktarılması gerektiğinde, her ülke kişisel veriyi aktaracağı ülkenin kişisel verileri koruma düzeyini ve mevzuatlarını değerlendirerek verilerin aktarılıp aktarılamayacağına karar vermektedir. Kişisel veriler bir ülkede ne kadar ideal seviyede korunabiliyorsa o ülkedeki vatandaşların güveni ve ülkenin refah derecesi de o kapsamda gelişmiş olacaktır. Bilgi güvenliğinin bir parçasını oluşturan kişisel verilerin korunması için stratejiler yürütlmesi ve uygulamadaki sorunların çözülmesi önem teşkil etmektedir. Bu çalışma kapsamında muhtemel boşluklar ve sorunlar irdelenerek, oluşabilecek risklerin minimum düzeye indirilmesi için önerilerde

bulunulmaya çalışılacaktır. Bu kapsamda, tez çalışmasında uygulamadaki boşlukları ve kişilerin kişisel verilerin işlenmesi hakkında farkındalığı ve görüşlerini ölçmek amacıyla oluşturulan anketten de faydalanılacaktır.
Biyometrik veriler de kişisel verilerin bir parçası olup, özel nitelikli kişisel veriler özelliğini haizdir. Dolayısıyla, biyometrik verilerin işlenmesi konusunda genel kişisel verilerin işlenmesine göre daha fazla hassasiyet mevcuttur. Biyometrik verilerin korunmasına ilişkin mevzuat hükümleri açıklanmadan önce biyometrik veriye ilişkin tanımlar, kullanılma yöntemleri açıklanacaktır. Biyometrik verinin kullanıldığı sektörler de vurgulanarak karşılaştırmalı mevzuat hükümleri irdelenecektir.

Günümüzde bankacılık, sağlık, güvenlik gibi sektörlerde biyometrik verinin kullanımı fazladır; ancak ilerleyen zamanlarda hayatın büyük bir bölümünde, birçok sektörde olmak üzere çoğu işlemler biyometrik verileri kullanmak suretiyle gerçekleştirilecektir. Biyometrik verilere büyük ölçüde önem gösterilmesinin sebebi, bu veriler tamamen kişiye münhasır olduğu için sahtecilik ihtimalini neredeyse imkansız hale getirmesidir. Sahtecilik suçunun önüne geçebilmek ve bilgi güvenliğini bu surette sağlayabilmek için biyometrik veriler gerek Türkiye'de gerekse yurt dışında fazlaca kullanılacaktır. Biyometrik verilerin de önemini binaen Türkiye, AB, Fransa ve Amerika gibi ülke mevzuatları karşılaştırılarak korumanın kapsamı ve ilkeler ortaya konulmaya çalışılacaktır.

Tezin kapsamında ortaya konulacak öneriler açısından kişisel verilerin ve biyometrik verilerin işlenmesine ilişkin anket soruları hazırlanmıştır. Anket sonucunda çeşitli sektörlerde çalışan kişilerin hem kişisel verisi işlenen ilgili kişi hem de kişisel verileri işleyen veri sorumlusu ve veri işleyen olarak farkındalıkları ve görüşleri tezin sonuç ve öneriler kısmına katkıda bulunacaktır. Anket dışında çeşitli yasa ve yönetmelik hükümleri irdelenerek kişişsel verilerin ve biyometrik verilerin işlenmesine yönelik ilke ve kurallar ortaya konulacaktır. Sonuç olarak, uygulamadaki boşluların tespiti ve yaşanabilecek sorunların en az seviyeye indirgenebilmesi için anketten ve mevzuat incelemelerinden alınan çıktılarla somut öneriler oluşturmaya çalışılacaktır; tezin çalışma alanı ve esas gayesi bu şekilde belirlenmiştir.

1.2 Tezin Amacı Ve İçeriği

Tezin amacı, öncelikle kişisel veri kavramını ve biyometrik veri kavramını irdeleyerek karşılaştırmalı hukuk sistemlerini ortaya koymak ve bu verilerin ideal seviyede işlenebilmesi için öneriler getirmektir. Türkiye'de 2010 yılında Anayasa'da belirtildikten sonra 2016 yılı itibari ile yürürlüğe giren kişisel verilerin korunması düzenlemeleri detaylı olarak incelenecektir. Kişisel verilerin korunması konusu uluslararası olarak birçok ülke tarafından düzenlemelerle koruma altına alınmıştır. Avrupa Birliği, Amerika, Fransa, Hollanda, Kanada Japonya gibi birçok ülke kişisel verileri korunması amacıyla düzenlemeler yapmıştır. Bu verilerin bir türü olan biyometrik verilerin kullanımı ise gün geçtikçe daha da artmakta, daha fazla önem kazanmaktadır.

Özellikle Avrupa Birliği yaptığı güncellemeler ile kişisel verilerin işlenmesi konusunda detaylı bir düzenlemeye sahiptir. AB, kişisel veri düzenlemeleri ile Ab vatandaşlarının kişisel verilerinin yüksek seviyede korunmasını teminat altına almayı hedeflemektedir. AB'de GDPR'ın çizdiği genel çerçevenin yanında AB'ye üye ülkelerin ulusal mevzuatları uyarınca da daha detaylı düzenlemeler söz konusu olabilmektedir. Bilişim toplumunun doğal bir sonucu olarak bireylere ait kişisel verilerin dijital ortamlarda saklanması artmıştır. Kopyalanması mümkün olmayan bireylere has biyometrik veriler bile dijital sistemlerde tutulabilmektedir. İşte bu sebeple bu verilerin korunması için gerek teknik/fiziksel ve gerekse yasal önlemlerin alınması gerekmektedir.

Tez çalışması kapsamında, Türkiye mevzuatı ile uluslararası mevzuatı karşılaştırılarak gerek uluslararası gerekse ulusal çapta uygulamadaki boşlukları açığa çıkarmak, yapılması gerekenlere ilişkin önerilerde bulunulmaya çalışılacaktır. Kişisel veri ve biyometrik veri kavramını inceledikten sonra verilerin korunması açısından Kriptoloji konusuna da yer verilecektir. Verilerin özellikle Türkiye'de, Avrupa Birliği'nde ve Amerika, Japonya gibi diğer ülkelerde korunması konuları açıklanarak Türkiye'deki kişisel verilerin ve özel nitelikli kişisel veri olan biyometrik verilerin korunmasına yönelik düzenlemelere, politikalara ve stratejilere ışık tutulmaya çalışılacaktır. Çalışmanın temel çıktılarından biri olan Anket ile uygulamadaki sorunlar ve kişilerin kişisel verilerin korunmasına ilişkin görüşleri dile getirilecektir ve bu doğrultuda sorun

teşkil eden noktalar çözüme kavuşturulmaya çalışılacaktır. Bu sorunlara çözüm getirilmesi için sunulacak öneriler de tezin amacını gerçekleştirmesinde büyük rol oynayacaktır.

2. BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI

Bilgi güvenliği son zamanların en güncel konularından birisidir. Bu başlık altında bilgi güvenliğinin kavramsal içeriğine değinildikten sonra kişisel verilerin korunmasının tarihçesi, kavram açıklamaları, ilkeleri ve karşılaştırmalı başka ülkelerdeki düzenlemelere değinilecektir.

2.1 Bilgi Güvenliği

Bilgi ve veri kavramları her ne kadar aynı gibi düşünülse de aslında farklı kavramlardır. Veri bilgiyi temsil ederken; bilgi ise veriyi anlamlandırır, açıklar [1]. Veri için işlenmemiş bilgi de diyebiliriz. Bu başlık çerçevesinde, bilgi güvenliği konseptini irdeleyerek kavramsal çerçevesini çizilecek, tanımlar ve ilkeler belirtilecektir. Ek olarak, bilgi güvenliğinin teknik fiziksel güvenlik olarak nitelendirebileceğimiz bilgi güvenliğini sağlamaya yönelik kriptoloji kavramı da ana hatları ile beraber bu başlık kapsamında irdelenecektir.

2.1.1 Kavramsal çerçeve

Bilgi güvenliği, üç temel bileşenden oluşmaktadır. Bilgi güvenliğinin temel üç bileşeni ise "gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability)"tir [1].

Bilgi güvenliğini sağlamak çeşitli açılardan önem arz etmektedir. Bunlardan ilki, "kuruluşların (kamu sektörü özellikle özel sektör/firmalar) malvarlığını korumak"olarak belirtilebilir. Bilgi güvenliğinin temel hedeflerinden bir tanesi kuruluşların malvarlığını koruyabilmektir [2]. Malvarlığından kasıt ise sadece kuruluşta yer alan mali bilgiler değil; bunun yanında kuruluşun bütün donanımsal ve yazılımsal sistemlerinde saklanan bütün bilgi birikimidir [2].

Bilgi güvenliğinin bir diğer işlevi de kuruluşa rekabetsel üstünlük sağlamasıdır. Ağ güvenliği özellikle ticaret ve finans sektörlerinde önem arz eden bir hususttur ve bilgi güvenliği ne kadar yüksek derecede sağlanırsa o kuruluş o derece güvenilir kabul

edilerek rekabet açısından üstünlük kazanacaktır [2]. Bilgi güvenliği, yasalar kapsamında da koruma altına alınmaktadır. Bilgi güvenliğinin sağlanması için mevzuat tarafından çeşitli kurallar ve yaptırımlar öngörülmektedir. Bu kapsamda, hukuka uygun olarak kuruluşların varlığını sürdürebilmeleri için yine bilgi güvenliğine ihtiyaç duyulmaktadır [2]. Kuruluşlar bünyesinde birçok kişisel veri saklanmaktadır ve bu verilerin ele geçirilmesi, değiştirilmesi, silinmesi gibi durumlarda telafisi mümkün olmayan sonuçlar ortaya çıkabilecektir. Bilgi güvenliği bir ülkede ne kadar yüksek derecede sağlanabiliyorsa o ülkenin refah düzeyinin de o derecede gelişmiş olduğu yorumunu yapmak mümkün olacaktır.

Gizlilik, kişilerin verilerinin ve bilgilerinin yetkisiz kişiler tarafından ulaşılamamasını, bilgilerin korunmasını ifade eder. Bu veriler kişinin sağlık, felsefi düşüncesi, sendika üyeliği gibi hassas nitelikteki veriler olabileceği gibi kimlik numarası, adresi, telefon numarası, kredi kartı bilgileri ve benzeri veriler de olabilir. Gerçek kişilerin verilerinin korunması kadar kurumların da verilerinin korunması önem arz etmektedir. Bilgilere erişilmesi kasıtlı olarak yapılmış olabilir; örneğin hackerlar aracılığıyla önemli bilgilere erişilebilir, bu bilgiler okunabilir. Bilgilerin ifşa edilmesi kasıt olmaksızın dikkatsizlik veyahut yetkisiz kişilere bilgi aktarımı şeklinde de gerçekleşebilir [3].

Önleme (prevention), tespit (dedection) ve müdahale (response) süreçleri güvenlik üçlüsü olarak değerlendirilmektedir [2]. Güvenlik açıkları, sistem açıkları, zayıf yönetim gibi zafiyetleri önleme amaçlı çalışmaların yapılması bilgi güvenliğinin sağlanması açısından son derece önem arz etmektedir. Saldırıları önleme amaçlı tedbirlerin alınmasına rağmen saldırıların gerçekleşmesini tamamen önlemek her zaman mümkün değildir. Dolayısıyla, önleyici çalışmalar kadar bilgi bütünlüğüne saldırı gerçekleştiğinde bunu tespit etmek ve saldırılara müdahale etmek de önem teşkil etmektedir [2].

Bütünlük, genel itibariyle bilgilerin bütününe zarar gelmeksizin doğruluklarının korunmasıdır. Bütünlük, bilgi sistemlerinden beklenen hizmetlerin beklendiği gibi olması ve bilgi sisteminde saklanan verilerin bozulmadan muhafaza edilebilmesi olarak da tanımlanabilir [1].

Bütünlük açısından üç temel amaç bulunmaktadır. Bunlardan ilki, yetkisiz kullanıcılar tarafından bilgilerin değiştirilmesini engellemektir [3]. Bu kapsamda, yetkisiz kişiler sisteme girerek kişilerin bilgilerini değiştirmek suretiyle bilgi güvenliği ihlâli ortaya çıkarabilirler. Bilginin bütünlüğü açısından öncelikle o bilginin bütünün korunması, değiştirilmemiş olması gerekmektedir.

İkinci hedef, yetki sahibi kişiler tarafından bilgilerin değiştirilmesini engellemek ya da yetki sahibi olmayan kişilerin bilgilere ulaşmasını engellemektir [3]. Yetki sahibi kişiler dikkatsizlik sonucunda kasıtları olmasa da bilgilerin değişmesine neden olabilirler. Burada özellikle bilgileri koruyan sisteme büyük bir rol düşmektedir. Bilgilerin değiştirileceği zaman sistemin uyarması ve buna kolay kolay izin vermemesi dikkatsizlik sonucu veri kaybını önlemek açısından faydalı olabilir.

Bütünlük açısından son hedef ise, iç ve dış bakımdan istikrarın sağlanmasıdır [3]. İç istikrar, verilerin ve bilgilerin yer aldığı sistemdeki istikrarı ifade eder. Örneğin, yetkili kişinin bilgisayarında yer alan bilgileri korunaklı durumda ise, saldırı gelmiyorsa ya da gelen saldırılara rağmen bu bilgiler ve veriler korunabiliyorsa iç istikrarın var olduğu söylenebilir. Dış istikrar ise kişiler veya Kurumlar bilgi güvenliğinin sağlanması için başka bir Şirketten hizmet alıyorsa ya da bilgilerini bir veritabanında saklıyorsa bu veritabanın gerçek bilgiler ile uyumlu olmasını, veritabanlarının güvenlilik derecesini ifade eder [3].

Erişilebilirlik, bilgiye yetkili kişinin istediği zaman kesintisiz ve sekteye uğratılmadan erişebilmesidir. Bir bilgi sistemine erişebilmek donanım, bilgisayar ağı ve verilen hizmetler bakımından değerlendirilecektir [1]. Sistem güvenliği devrede olup istikrarlı bir biçimde çalışması gerekmektedir. Birçok siber saldırı sonucunda erişilebilirlik unsuru büyük zarar görebilmektedir. Örnek olarak hackerlar tarafından yetkili kişinin bilgisayarı kontrol altına alınarak yetkili kişinin istediği bilgilere erişmesi engellenebilir. Bu durum özellikle Dağıtık Hizmet Engelleme (Distributed Denial of Service (DDoS)) saldırılarında görülmektedir. DDoS saldırıları, bilgi güvenliğinin erişilebilirlik unsurunu hedef alan bir saldırıdır ve sık görülen bir siber saldırı türüdür. Sistemlerin açıklarından faydalanan yetkisiz kişilerin müdahalesi sonucunda erişilebilirlik unsuruna saldırı gerçekleşmektedir. Sistemlerin güncel tutulup her türlü

teknik önlem alınarak dikkatli bir biçimde kullanılmaları erişilebilirlik açısından önem teşkil etmektedir.

Gizlilik, bütünlük ve erişilebilirlik unsurlarına ek olarak izlenebilirlik, inkâr edilemezlik, güvenilirlik de bilgi güvenliğinin bileşenlerinden sayılabilir [1]. İzlenebilirlik, bilgi sisteminde gerçekleşen işlemlerin kim tarafından, ne zaman yapıldığının izlenmesi ve kaydedilmesidir [1]. İzlenebilirlik ile olası saldırıları önlemek, yanlış eylemleri ortaya çıkarmak veya saldırı sonrasında tespit edilmesi açısından önem teşkil etmektedir. İnkâr edilemezlik de özellikle çok kullanıcılı sistemlerde kişilerin gerçekleştirdiği işlemlerin izlenebilmesi, ispatı bakımından söz konusudur [1]. Özellikle internet bankacılığı ile kişilerin gerçekleştirmiş olduğu eylemleri inkâr etmemeleri ve ispat bakımından inkâr edilemezlik kimlik doğrulamalarının sağlanmasında kullanılır [1].

Güvenilirlik de verilerin saklandığı her türlü donanımsal, yazılımsal, vb. sistemlerin yüksek derecede korunması, güvenilirliğinin yüksek olmasıdır [1]. Sistemler güncel tutularak, gerekli periyodik bakımları yapılarak, en yüksek güvenilirlikli yöntemler kullanılmak suretiyle de güvenirlik sağlanmaktadır.

Bilgi güvenliğinin sağlanmasında teknik unsurların yanında fiziki güvenliğin de sağlanması büyük önem taşımaktadır. Fiziksel güvenlik ise bilişim sistemlerini yetkisiz insanların fiziksel erişimi veya doğal afet gibi etkenlerden korunmasını ifade eder [5]. Doğal afetler yangın, fırtına, deprem, volkanik patlama, erozyon, yıldırım gibi olayları içermektedir. Bilişim sistemlerinin korunaklı bir ortamda tutularak dış etkenlerden zarar görmesinin engellenmesi fiziksel güvenlik ile hedeflenmektedir [5].

2.1.2 Kriptolojiye ilişkin temel bilgiler

Kriptoloji, bilgi güvenliğini sağlamaya yarayan temel kavramlardan bir tanesidir. Her ne kadar bilgi güvenliğini artırma çalışmaları günümüzde çok yoğun olsa da, kriptolojinin temeli aslında çok eskilere dayanmaktadır. Örnek vermek gerekirse Rönesans döneminde tacir prensler ticari sırlarını gizli tutmak isterlerdi ve emirlerini şifreli ve gizli bir biçimde göndermeyi tercih ederlerdi [4]. İkinci Dünya Savaşı'nda Naziler tarafından gizli mesajlarını şifreli olarak gönderdikleri bir makine olan Enigma

da yine şifreleme yönteminin eskilere dayandığını göstermektedir. Önemli sırların, gizli mesajların güvenle ulaşabilmesi ve taraflar dışında kimse tarafından anlaşılmayacak biçimde şifreleme yöntemlerini deneme süreçleri kriptografinin de ortaya çıkışını sağlamıştır.

Kriptografi, dijital bir makinede saklanan bilgilerin veyahut taraflar arasında gerçekleşen mesajlaşmaların korunması amacıyla kullanılan matematiksel işlemler bütünü olarak tanımlanabilir [4]. Özellikle 1960'lı yıllarda kriptoloji çalışmalarına ağırlık verilmiştir. Bilgi güvenliğinin üç bileşeni olan gizlilik, bütünlük ve erişilebilirlik kriptolojinin de temelini oluşturmaktadır. Geçmişten günümüze kriptolojiye ilişkin birçok yöntem geliştirilmiş olsa da bu başlık altında simetrik ve simetrik olmayan şifreleme yöntemleri, veri bütünlüğünü sağlama yöntemleri anlatılacaktır.

2.1.2.1 Terminoloji

"Düz metin" (plaintext), orijinal mesajın kendisidir. Şifreleme gerçekleşmeden önce mesajın kişinin dilinde yazılmış, anlaşılır hâline düz metin denilmektedir. Şifreleme, düz metinler üzerinden gerçekleşebilmektedir. Günümüzde düz metinler yazı biçiminde olabileceği gibi ses, görüntü, video veya birkaç veri formatının birleşiminden de oluşabilir [4].

"Kripto analizi" (cryptanalysis) ise içinde gizli mesajları barındıran şifrelenmiş verileri veya kodları deşifre etme yöntemine verilen addır. [5] Bir kriptocu, kendi dilinde yazılmış olan basit bir mesajı veyahut düz metini alarak kripto analizi sayesinde bunları gizli mesaja dönüştürebilir [5].

Verilerin gizlenmesi işlemine "şifreleme" (encipher/encrypt) denilmektedir. Diğer bir deyişle, kriptolama ya da şifreleme (encryption), çeşitli algoritmaların uygulanmasıyla düz metni anlaşılmaz hâle çevirerek onu şifrelenmiş metin (ciphertext) durumuna getirmektir [4]. Bunun bir diğer anlamı da kişinin elinde o şifreyi çözebilecek bir kod, algoritma ya da anahtar bulunmadığı takdirde şifrenin çözülmesi mümkün olamayacaktır [5].

Kripto analizini gerçekleştirecek olan kişiler genellikle istatistiksel teknikleri kullanabilme ve çeşitli göstergeleri, kodları birleştirerek ileri seviyede hesaplayabilme becerisini haiz matematikçiler ya da deneyimli dil bilimciler arasından çıkmaktadır [5].

Şifreleme işleminin tam tersi işleme ise şifrenin çözülmesi denilmektedir. Verinin orijinal hâline geri döndürülmesi, şifrenin çözülmesi ile (decryption) mümkündür. "Kodlama" (cipher), şifreleme ve şifreyi çözme yöntemlerinde kullanılan matematiksel işlemlerin bütünüdür [5].

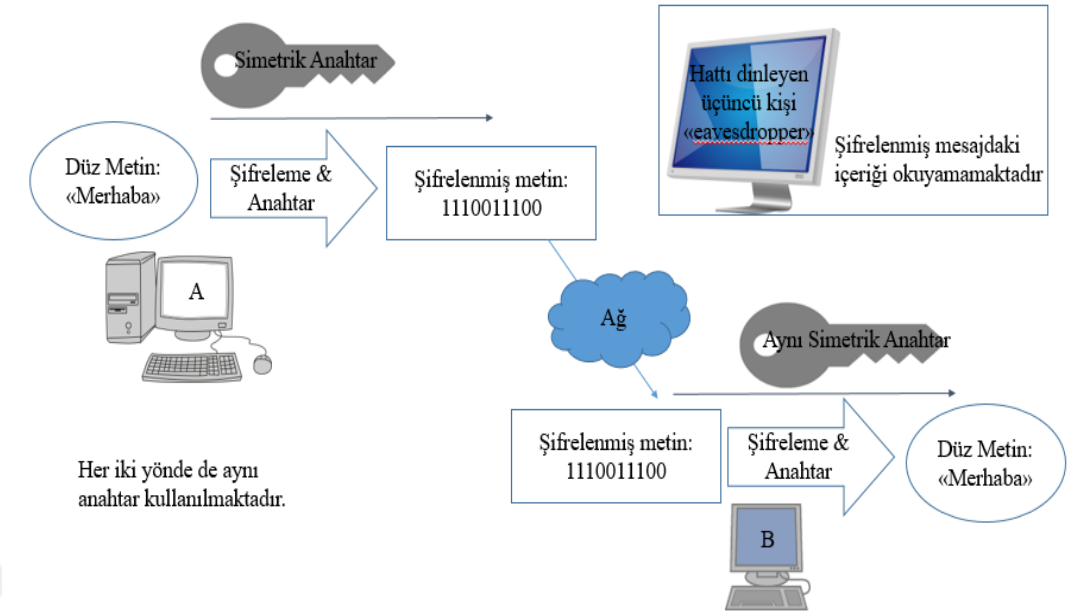
"Anahtar" (key) ise, şifreleme ve şifreyi çözme yöntemlerinde gerekli olan, 40'tan 4000 bit'e kadar (birler ve sıfırlar) rastgele bit dizilerinden oluşmaktadır. Anahtar ne kadar uzunluğu ne kadar fazla ise şifrenin kırılması da o kadar zor olacaktır [4].

Algoritmaların, anahtarların ve şifrelemeye ilişkin standartlar ve protokollerin birleşimi ile şifreleme ve şifreyi çözme yöntemlerinde kabul gören teknik yöntemlerle yürütülen ve uygulanan konsept, kripto sisteminin (cryptosystem) bütününü oluşturmaktadır [5].

2.1.2.2 Simetrik şifreleme yöntemleri

Bilgi güvenliğinin "gizlilik" unsurunu sağlamak amacıyla geliştirilen yöntemlerden bir tanesi simetrik şifreleme yöntemidir. Simetrik şifreleme yönteminde düz metni şifrelemek için kullanılacak anahtar ile şifrelenmiş metni çözmek için kullanılacak anahtar aynı olmalıdır [6]. Hem şifreleme işleminde hem de şifre çözme işleminde kullanılacak anahtarın aynı olması bakımından bu yönteme simetrik denilmektedir.

Simetrik şifrelemede her iki taraf da şifreleme ve şifreyi çözme işlemleri için her iki yönde de tek bir anahtarı kullanmaktadır [4]. Saldırgan şifreyi kırabilmek için doğru olan anahtarı bulabilene kadar kapsamlı bir arama (exhaustive search) yapmaktadır. Bu saldırıyı önleyebilmenin yollarından bir tanesi de anahtarın boyutunu çok uzun tutarak saldırganların doğru anahtarı bulabilme ihtimalini azaltmaktır [4]. Simetrik anahtar şifreleme yöntemi Şekil 2.1'de gösterilmektedir [4].



Şekil 2.1: Simetrik anahtar şifreleme

Eğer anahtarın N bit'ten oluşan uzunluğu varsa, 2^N tane muhtemel anahtar olduğu kabul edilir. Genellikle bir saldırganın şifreyi çözmesi için anahtarların en az yarısını denemesi gerekmektedir; bu da saldırganın bir şifreyi çözebilmesi için en az $2^N/2$ kere deneme yapması anlamına gelecektir [4]. Bit sayısı arttıkça, o şifrenin çözülme ihtimali de azalacaktır ve saldırganın şifreyi kırmak için harcayacağı zaman da bir o kadar artacaktır. Örnek olarak Çizelge 2.1'e bakılabilir [4]:

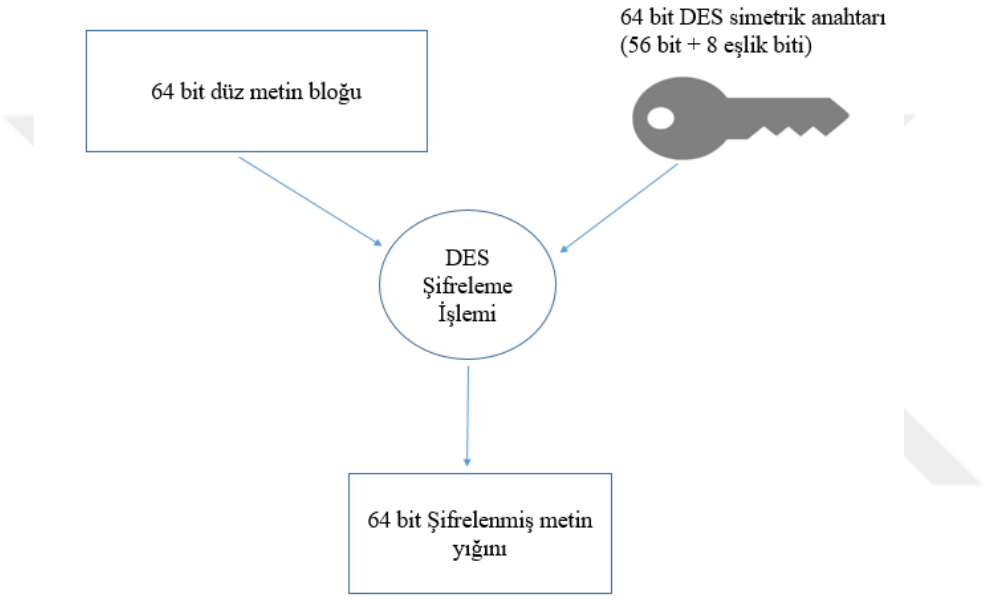
Çizelge 2.1: Anahtar uzunluğu ve sayı ilişkisi

Anahtar Uzunluğu Bit Olarak	Muhtemel Anahtar Sayısı
2	4
16	65.536
112	5.1923E+33
512	1.3408E+154

Simetrik şifreleme yöntemlerine örnek olarak BLOK Şifreleme Yöntemleri (DES, 3DES, AES vb.) ve Akan Şifreleme Yöntemleri (RC4, A5/1, A5/2) gösterilebilir [6].

DES'in açılımı "The Data Encryption Standard" yani Veri Şifreleme Standardı'dır. 1977 yılında şu anki adı Ulusal Teknoloji ve Standartlar Enstitüsü (National Institute

of Standards and Technology “NIST”) olan enstitü DES’i oluşturmuştur. Bu method, daha sonra en fazla kullanılan yöntemlerden bir tanesi olmuştur [4]. DES, 2010’lu yıllarda da kaba kuvvet arama saldırıları hariç olmak üzere çoğu saldırılardan kurtulabildiği ve hala donanım hızlandırıcıları tarafından desteklendiği için yaygın olarak kullanılmaktadır [4]. DES, blok şifreleme yöntemlerinden bir tanesi olup şifreleme anahtarı 64 bitliktir [6]. Anahtarı oluşturan her sekizlik içinde bir bit eşlik biti olarak kullanıldığı için bu anahtarın boyutu 56 bit’e düşmektedir ve bu boyut günümüz için yeterli görünmese de yine de kullanılabilmektedir [4].



Şekil 2.2: DES şifreleme örneği

Üçlü DES (3DES) ise DES şifreleme yöntemlerinin art arda üç kez kullanılmasıyla oluşturulur ve her bir DES için farklı anahtar kullanılabilir [6]. Güçlü bir simetrik şifreleme yapısı bulunmaktadır; ancak DES’in yavaş olması sebebiyle hızlı değildir. Ek olarak, bu yöntemde DES 3 kez tekrarlanmak durumunda olduğu için 3DES pratik bir yöntem değildir [4].

İleri Şifreleme Standardı (Advanced Encryption Standard “AES”) ise DES’in zayıf kalması ve 3DES’in oluşturduğu blok yığınlarının kullanışlı olmaması nedenleri ile NIST’in 2001 yılında geliştirdiği bir başka yöntemdir [3]. AES, 128; 192 ve 256 bit olmak üzere üç çeşit anahtar uzunluğuna sahiptir. AES, işlemci gücü ve RAM gereksinimleri açısından çok çeşitli aygıtlarda - hatta hücresel telefonlarda ve kişisel dijital yardım aygıtlarında kullanılabilmektedir [4].

RC4 ise zayıf şifreleme yöntemlerinden birisidir. Ark Four olarak da adlandırılmaktadır. RC4'ün iki temel avantajı vardır. Bunlardan ilki, RC4'ün oldukça hızlı olması ve çok az miktarda RAM kullanmasıdır. İkinci olarak ise RC4 geniş yelpazede anahtar uzunlukları sunmaktadır. Bir anahtar ne kadar uzunsa şifre de o kadar iyi olacaktır. Bütün bunların yanında, şayet RC4 doğru olarak uygulanamazsa, koruma seviyesi de minimum düzeyde olacaktır [4].

2.1.2.3 Simetrik olmayan şifreleme yöntemleri

Simetrik şifrelemede düz metni şifrelemek ve şifreyi kırmak için aynı anahtar kullanılıyordu. Simetrik sistemde ortaya çıkan problem olarak gönderen ve alan tarafın aynı anahtarı alma zorunluluğu gösterilebilir [6]. İnternet bankacılığı gibi çok sayıda kullanıcısı olan sistemlerde oturum sırasında banka ve kullanıcı bilgisayarı arasında gidip gelen verilerin gizliliğini sağlamak bakımından simetrik şifreleme yöntemini kullanmak zor ve pratik değildir [6]. Bunun doğal bir sonucu olarak da çok kullanıcılı sistemlerde kullanılmak üzere simetrik olmayan şifreleme yöntemleri oluşturulmuştur.

Simetrik olmayan şifreleme yöntemlerinden en fazla kullanılan tekniklerden birisi RSA (Rivest- Shamir- Adleman) şifreleme yöntemidir. RSA, günümüzde yaygın olarak kullanılan açık anahtarlı simetrik olmayan algoritma temelli şifreleme yöntemidir [6]. RSA, dijital imzada ve mesajları şifrelemede kullanılabilir. Büyük asal sayılardaki faktörleri belirleyebilmek açısından karmaşık ve zor bir algoritmadan oluşmaktadır. RSA algoritmasında izlenecek adımlar aşağıdaki gibidir [6]:

- "p" ve "q"olmak üzere iki asal sayı seçilir; ve n=p.q olmak üzere mod alınacak değer hesaplanır.
- Φ(n)= (p-1).(q-1) hesaplanır ve n'den az olacak ve Φ(n) ile en büyük ortak bölenleri 1 olacak bir "e" sayısı seçilir. e ile Φ(n) arasında 1 dışında ortak bölen bir sayı olmayacaktır [6].
- Bu çerçevede, açık anahtar n ve e'den oluşacaktır; özel anahtar olarak d ise

$$\mathbf{d} = \frac{\mathbf{2\Phi(n) + 1}}{\mathbf{e}}$$

hesaplanır. (2.1)

- Düz metin A olsun.
- İşlenmiş metin (ciphertext) C diyelim. $C=A^e \bmod n$
- Şifreyi çözme işlemi ise; Düz metin= $C^d \bmod n$ formülü ile okunacaktır.

Eliptik eğri şifrelemesi (elliptical curve cryptography - ECC) de başka bir simetrik olmayan şifreleme işlemlerindendir. Eliptik bir eğri oval şeklinde bir elips değildir, fakat iki ekseni kesen bir halka çizgisi olarak temsil edilir. ECC, daha hızlı, daha küçük ve daha etkili şifreleme anahtarları oluşturmak için kullanılabilen eliptik eğri teorisine dayanan açık anahtar şifreleme tekniğidir [5]. ECC, çok büyük asal sayıların çarpımı olarak geleneksel üretim yöntemi yerine eliptik eğri denkleminin özellikleri aracılığıyla anahtarlar üretir. RSA gibi diğer açık anahtar sistemleri ile beraber kullanılabilir [5].

Veritabanında saklanan verilerin ve bilgisayarlar arasında iletilen verilerin bütünlüğünü sağlamak amacıyla da geliştirilen birtakım yöntemler bulunmaktadır. Özetleme (hash) yöntemi de güncel olarak kullanılan simetrik olmayan şifreleme yöntemlerindendir. Özetlemeyi basit bir şekilde anlayabilmek açısından mesajın bitlerini çok büyük bir ikili sayı olarak ele alıp daha küçük bir sayıya böleceğimizi düşünelim. Kalan hash olabilir [4]. Özetlemede bir veri kümesi içerisinde doluşabilecek olan bir bitlik veri değişiminin dahi algılanması amaçlanmaktadır [6]. Örnek vermek gerekirse, kişi kredi kart detaylarının kimse tarafından bilinmesini istemez. Mesajdaki metin karakter sayısını sayarak mesajla birlikte bu değeri (örneğin karakter sayısını) gönderir. Mesajın alıcısı kontrol ederek mesajın geldiğinden emin olabilir [5].

Mesaj özetlemesi yani hash hesaplaması, özetleme fonksiyonu içeren matematiksel bir terimdir. Mesaj özeti fonksiyonu hesaplanması kolay; ancak tersini elde edebilmek için ters mühendislik yapması zor bir matematiksel fonksiyondur [5]. Özetleme işleminde giriş verisinin uzunluğu değişken olabilir; ancak çıkış verisinin boyutu sabittir ve beklenti de bu verinin giriş verilerinden daha kısa olmasıdır [6]. Bu süreç esnasında, giriş verisi belli uzunlukta dilimlere ayrılır ve her dilim bu süreçten geçirilir. Günümüzde dilim boyu 128 ile 512 bit arasında değişkenlik göstermektedir [6].

2.2 Kişisel Verilerin Korunması

Kişisel veriler, teknolojinin gelişmesi ve teknoloji çağına girilmesi ile birlikte ivme kazanan bir konudur. "Mahremiyet" kavramının da bir yansıması olan kişisel veriler, uluslararası ve çeşitli ülkelerce ulusal mevzuatları tarafından özellikle 1980 yılından bu yana korunmaktadır.

Bu kavramın tarihçesi, felsefesi ve ana hatlarını aşağıdaki ilgili başlıklar altında açıklanacaktır. Bu çerçevede kavramın özü, tarihçesi, korunmasının nedeni ve amacı, terminolojisi ve genel ilkeler belirtilecektir.

2.2.1 Kişisel verilerin korunması felsefesi ve tarihçe

Kişisel veri kavramı, özellikle son zamanlarda gerek ülkemizde gerek Avrupa Birliği'nde ve çeşitli Avrupa ülkelerinde önem kazanmıştır. Kişisel veri kavramı, öncelikle Avrupa Konseyi tarafından hazırlanan 108 numaralı «Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi» uyarınca gündeme gelmiştir. Bu Sözleşme, 28 Ocak 1981 tarihinde imzaya açılmış ve 1 Ekim 1985 tarihinde yürürlüğe girmiştir [7]. Türkiye de bu Sözleşmeyi 28 Ocak 1981 tarihinde imzalamıştır. 30 Ocak 2016 tarihinde "*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun*" kabul edilmiştir ve 18 Şubat 2016 tarihinde yayımlanarak yürürlüğe girmiştir. Sözleşme'nin resmi Türkçe çevirisi ise 17 Mart 2016 tarihinde Resmi Gazete'de yayımlanmıştır [7]. Sözleşme, her ne kadar 18 Şubat 2016 tarihinde yürürlüğe girmiş olsa da, Sözleşmenin 30 Ocak 2016 tarihinde kabul edilmesinden itibaren evrakların da Avrupa Konseyi'ne gönderilmesi ve ilgili prosedürlerin de tamamlanması süreci nedeniyle, Sözleşmenin 1 Eylül 2016 tarihinden itibaren tam anlamıyla yürürlüğe girmiş olduğunu belirtmek de mümkün olacaktır. Sözleşmenin de bir yansıması olarak 7 Nisan 2016 tarihinde "6698 Sayılı Kişisel Verilerin Korunması Kanunu" Resmi Gazete'de yayımlanarak altı ay sonra 7 Ekim 2016 tarihinde yürürlüğe girmiştir. Sözleşmenin amacı, Sözleşmeyi imzalayan her ülkede kişilerin "*uyruğu veya ikamet yeri neresi olursa olsun gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin işleme tabi tutulması karşısında özel hayata saygı hakkını güvence altına almaktır* [8]."

Kişisel veriler, 2010 yılında yapılan bir değişiklik ile Türkiye Cumhuriyeti Anayasası kapsamında koruma altına alınmıştır ve kişisel verilerin Kanun ile düzenleneceği hüküm altına alınmıştır. "Özel hayatın gizliliği ve korunması hakkı" başlığı altında Anayasa'nın 20. Maddesinde kişisel verilerin korunmasına ilişkin hüküm yer almaktadır. Anayasa'nın 20. Maddesine göre, "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir* [9]." Kişisel veriler konusu Anayasa'da özel hayatın gizliliği başlığı altında düzenlendiği için mahremiyet konusunu da yakından ilgilendirmektedir.

2.2.2 Kişisel veriler terminolojisi

Kişisel veri denildiği zaman önem arz eden birtakım kavramlar vardır. Gerek ulusal mevzuatımızda gerek AB mevzuatında da paralel düzenlenmiş olduğu üzere, kişisel veri terminolojisinde akla gelen ilk tanımlar "kişisel veri, açık rıza, kişisel verilerin işlenmesi, anonimleştirilmesi, silinmesi, yok edilmesi, aktarılması" kavramlarıdır. Aşağıdaki bölümlerde de bu kavramları açıklayarak kişisel veri terminolojisindeki temel kavramlar tanımlanacaktır. Bu kavramlar, kişisel verilerin diğer bir kategorisine giren hassas/özel nitelikli verilerden biyometrik verinin açıklamaları açısından da geçerli olacaktır.

2.2.2.1 Kişisel veri

KVKK üçüncü madde uyarınca kişisel veri "*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmıştır [10]. KVKK madde gerekçeleri uyarınca üçüncü maddenin gerekçesinde kişisel veriye örnek olarak bireyin adı, soyadı, doğum tarihi, doğum yeri gibi kişinin kim olduğunu anlamaya yarayan bilgiler olabileceği gibi kişinin ailevi, fiziki, ekonomik, sosyal ve benzeri özelliklerine ilişkin veriler sayılmıştır [11]. Bir veri neticesinde kişinin kim olduğu tespit edilebiliyorsa, kişi belirlenebiliyorsa ,o verinin kişisel veri niteliğinde olduğu söylenebilir. Tanımdaki "belirlenebilir"den ne anlaşılması gerektiğine ilişkin olarak KVKK gerekçesinde birtakım örnekler verilmiştir. Bu çerçevede, "*verilerin; kişinin fiziksel, ekonomik,*

kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir." [11]

Kişisel verinin tanımına bakılarak bir verinin kişisel veri olmasını sağlayan iki unsur olduğunu söylemek mümkündür. Bunlardan ilki bilginin gerçek bir kişiye ait olması iken ikincisi ise bu kişinin belirli ya da belirlenebilir olmasıdır. KVKK tasarısı üçüncü madde gerekçesinde de görüldüğü üzere, kişisel veriler bir bireyin bireysel, ailevi, fiziki, mesleki özelliklerini ortaya koyan ve o bireyi diğerlerinden ayırt etmeye yarayan o bireye has her türlü bilgidir [11]. Bu veriler o kişinin felsefi düşüncesi, etnik kökeni, sağlık, eğitim, cinsel yaşamı, başkaları ile arasında geçen haberleşmeler, istihdam durumu, fiziksel özellikleri, aile hayatı, kişisel düşünceleri, adres bilgileri, sosyal güvenlik numarası, kimlik numarası, pasaport numarası, telefon numarası, e-posta adresi, dernek ve sendika üyelikleri, kredi kartına ilişkin bilgileri kapsamaktadır [12].

Kanunda yapılan kişisel veri tanımına bakıldığı zaman geniş kapsamlı bir tanım yapıldığı görülmektedir. Diğer bir deyişle, kişisel verilerin unsurları, neleri kişisel veri olarak kabul edeceğimiz gibi hususlar tahdidi olarak Kanunda sayılmamıştır. Tanıma uyan her türlü veri kişisel veri olarak kabul edilebilecektir.

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik ise elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması, korunması amacıyla yürürlüğe bir düzenlemedir. Bu Yönetmelik kapsamında ise kişisel veri "*Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler*" olarak tanımlanmıştır [13]. Burada dikkat edilmesi gereken husus; KVKK uyarnca kişisel verinin "gerçek kişiye ait belirlenebilir" derken bu Yönetmelik kapsamında ise "gerçek ve tüzel kişiye ait" biçiminde düzenlenmesidir. Yani, KVKK uyarınca tüzel kişilere ilişkin bilgiler kişisel veri olarak sayılmazken; Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik uyarınca tüzel kişilere ilişkin veriler kişisel veri niteliğinde sayılmaktadır. AB ülkelerindeki kişisel verilerin işlenmesine yönelik

düzenlemeleri içeren GDPR uyarınca da KVKK'daki tanım ile paralel tanım yapılmıştır. Dolayısıyla, kişisel veri, Elektronik Haberleşme Sektörü'ne ilişkin yönetmelikte düzenlendiğinin aksine gerek KVKK gerek GDPR'da düzenlendiği üzere gerçek kişiye ilişkin kişiyi belirlenebilir kılan her türlü veri olarak ifade edilebilecektir.

2.2.2.2 Özel nitelikli kişisel veri

Kişisel veri tanımının "*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak Kanun'da yapıldığı ve içeriği yukarıdaki başlıkta belirtildi. KVKK uyarınca kişisel veriler iki kategoride toplanabilir. Bunlar genel nitelikli ve özel nitelikli kişisel verilerdir. Genel nitelikli kişisel veriler KVKK'daki genel tanımın kapsamına giren her türlü veri olarak düşünülebilir. Özel nitelikli kişisel veriler de bu tanımın kapsamında olup hangi verilerin özel nitelikli olduğu ayrıca sayılmak suretiyle tanımlanan verilerdir. Özel nitelikli kişisel verilerin önemi, bu verilerin ifşa edilmesi durumunda kişinin sosyal açıdan daha zor duruma düşebilmesi söz konusudur. Dolayısıyla özel nitelikli kişisel verilerin daha fazla korunması gerekmektedir; farklı istisnalar ve kurallar bu bağlamda öngörülebilir.

KVKK altıncı maddesi özel nitelikli kişisel verileri "*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*" biçiminde tasnif etmek suretiyle ifade etmiştir [10].

Tanımda sayılan kişilere ait her türlü veri özel nitelikli kişisel veri olarak kabul edilecektir. Bu veriler tahdidi olarak sayılmıştır. Diğer bir deyişle, sadece özel nitelikli kişisel veri tanımında yer alan veriler özel nitelikli kişisel verilerdir bunlar dışındaki kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi genel nitelikteki kişisel verilerdir. Özel nitelikli kişisel veriler hassas nitelikte olduğu için bu verilerin işlenme şartları ve istisnaları farklı kurallara tabidir. Bu hususa aşağıdaki kişisel verilerin işlenme ilke ve kuralları başlığında değinilecektir.

2.2.2.3 Açık rıza

Açık rıza kavramı, kişisel verilerin işlenmesi bakından şart olan temel kurallardan bir tanesidir. Kişisel verilerin işlenmesi bakımından aranan temel şart, kişisel verisi işlenen ilgili kişilerin kendi verilerinin işlenmesine açık rıza vermesidir. Anayasanın özel hayatın gizliliği ve korunmasına ilişkin yirminci maddesi uyarınca "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*" [10]. Anayasa uyarınca kişilerin kişisel verilerinin korunmasını isteme hakkı temel haklarından birisi olarak belirtilerek, bu hususun ancak Kanunla düzenleneceği belirtilmiştir. Kanun da, kişisel verinin işlenebilmesi için kişinin açık rızasının varlığını şart koşmuştur. Açık rıza kavramı, hem genel hem özel nitelikli kişisel verilerin işlenmesi bakımından hukuka uygunluk sebebi olarak öngörülmüştür [12].

KVKK'nın tanımlara ilişkin 3. Maddesinde açık rıza "*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*" olarak tanımlanmıştır. [9]. KVKK ilgili maddelerinde kişisel verilerin işlenmesi için açık rıza aranmaktadır. Bu kapsamda, öncelikle KVKK'nın beşinci maddesine göre, "*Kişisel veriler ilgili kişinin açık rızası olmadan işlenemez.*" [10] Yine, aynı şekilde altıncı madde uyarınca da özel nitelikli kişisel verilerin işlenmesinde ilgili kişilerin açık rızası aranmaktadır. Kişisel verilerin yurt içinde aktarılması (madde 8) ve yurt dışına aktarılması (madde 9) için de yine ilgili kişinin açık rızası şart olarak konulmuştur.

Rıza kavramı için KVKK üç husus aramaktadır. Bunlar ise belirli bir konuya ilişkin olması, rıza açıklamasının bilgilendirilmeye dayanması ve kişinin herhangi bir etki altında kalmaksızın özgür iradesiyle beyan açıklamasında bulunmasıdır.

Açık rızanın tanımında yer alan ilk kavram "belirli bir konuya ilişkin olmak"tır. Belirli bir konuya ilişkin olmak, ilgili kişinin neye rıza verdiğini bilerek kişisel verisini paylaşmaya rıza göstermesidir. Kişi, hangi amaç için ve hangi kapsamda kişisel verisini paylaşacağını bilmelidir. Kişinin genel bir tabir ile "kişisel verilerimi

işlemenize rıza gösteriyorum" gibi muğlak ve açık uçlu rıza göstermesi KVKK'daki açık rıza kavramı kapsamında değerlendirilemeyecektir [12].

Kişinin birden çok konu için kişisel verisini paylaşması gerekiyorsa, ilgili kişi rızayı hangi verilerin ne amaçla işleneceğini bilerek bunları belirterek rızayı vermiş olması gerekmektedir [12]. Kişi rıza gösterdikten sonra kişisel verisi üçüncü bir kişi ile paylaşılacaksa, yurt dışına aktarılacaksa bu gibi prosedürlerde ilgili kişinin rızasının tekrar alınması gerekecektir.

Açık rıza kavramının tanımında yer alan ikinci unsur ise "bilgilendirme"dir. Bilgilendirme kriterine ilişkin olarak, KVKK'nın onuncu maddesi veri sorumlularının aydınlatma yükümlülüğünü düzenlemiştir. Veri sorumluları, hangi konuya ilişkin kişisel verilerin paylaşılacağı ve rızanın sonuçları hakkında ilgili kişileri bilgilendirmekle yükümlüdür [12]. Bilgilendirme, kişi açık rızasını vermeden önce yapılmalıdır. Bilgilendirme doğru bir şkilde yapılmalıdır ve kişinin vereceği açık rıza da bu bilgilendirmenin sonucunda gerçekleşmelidir. İlgili kişiden alınan açık rızanın kapsamı sadece bilgilendirildiği konuya ilişkindir. Başka bir konuda kişisel verilerinin işlenmesi gerekiyor ise ayrıca bilgilendirme yapılıp ilgili kişinin rızasının alınması gerekmektedir [12].

Açık rızanın tanımlanması için kullanılan son kavram da "özgür iradeyle açıklanması"dır. Özgür iradeyle açıklanması unsuru, ilgili kişilerin belirli bir konu hakkında bilgilendirildikten sonra hiçbir etki altında kalmaksızın bilinçli olarak ve kendi kararı çerçevesinde kişisel verisini paylaşmaya rıza göstermesidir. Örneğin, Borçlar Kanunu'nda da tanımı yapılan iradeyi sakatlayan durumlar (aldatma, yanıltma, korkutma) var ise, özgür bir iradenin varlığından söz edilemez. Rızayı sakatlayan bir durumun mevcudiyeti belirlenirken her durum ayrı ayrı değerlendirilerek rızayı ekilemenin derecesi belirlenmelidir [12].

KVKK'nın oluşturulma sürecinde rol oynayan 95/46 EC Sayılı Avrupa Birliği Direktifi'ne göre de açık rıza için benzer tanım kullanılmıştır. 95/46 Sayılı Direktif, 2016 yılı itibariyle GDPR olarak güncellenmiştir. GDPR çerçevesinde de açık rıza kavramı benzer bir şekilde düzenlenmiştir. Açık rıza, GDPR'da "*ilgili kişinin özgürce, o konuya ilişkin yeterli bilgi sahibi olarak ve belirsizliğe mahal vermeyecek şekilde*

irade beyanını dile getirmesi veyahut kendisine ilişkin kişisel verinin işlenmesini kabul ettiğine ilişkin açık olumlu hareketi" biçiminde tanımlanmıştır [14].

Kişinin sessiz kalması, kişisel verisinin işlenmesine onay verdiği anlamına gelmeyecektir. Kişinin kişisel verisinin işlenmesi için kural olarak açık irade beyanı gerekmektedir. Kanun gereğince kişi, kişisel verisinin işlenmesine kendi isteği üzerine ya da karşı tarafa onay vererek izin vermelidir [12]. Aynı zamanda kişinin yapacağı rıza açıklaması bu kişinin işlenmesine izin verdiği verinin sınırlarını, kapsamını, gerçekleştirilme biçimini ve süresini de kapsayacaktır ve diğer mevzuatlardaki düzenlemeler saklı olmak üzere irade beyanı yazılı olarak alınmak zorunda değildir; elektronik ortamda da ilgili kişinin rızası alınabilir [12]. Elektronik ortamın tanımı tam olarak yapılmamakla birlikte her türlü dijital ortam aracılığıyla gerçekleştirilebilen işlemler gibi kabul edilebilir.

2.2.2.4 Kişisel verilerin işlenmesi

Bilindiği üzere, her Kanunun ilk maddelerinde Kanunda yer alan terimlerin/kavramların tanımları yer almaktadır. Benzer şekilde, KVKK 3. Madde uyarınca kişisel verilerle ilgili tanımlar yer almaktadır. KVKK'daki 3. maddenin e bendinde kişisel verilerin işlenmesi tanımı yapılmaktadır. Buna göre kişisel verilerin işlenmesi, "*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi*" ifade etmektedir [10].

Verinin hangi şekilde korunacağı ve saklanacağı konusu da verinin önemi ve gizliliği kadar önemli bir meseledir. Otomatik işlemeye ilişkin KVKK'da veya başkaca düzenlemelerde herhangi bir tanım yapılmamıştır. Verilere ilişkin olarak önem arz eden husus, bu verilerin veri sicil kayıt sisteminin bir parçası olmasıdır. Bu kapsamda, verilerin otomatik olan veya otomatik olmayan yolla işlenmesi önemli değildir. Otomatik işlemeden kasıt, KVKK gerekçesi ve Ekonomik İşbirliği ve Kalkınma Örgütü tarafından verilen tanım beraber değerlendirilerek çeşitli bilişim sistemleri üzerinden (bilgisayar, her türlü yazılımsal, donanımsal cihazlar ve benzeri) işlenen

veriler olarak belirtilebilir [12]. Otomatik olmayan yollarla veri işlemede ise veriler veri kayıt sisteminin bir parçası olmakla beraber fiziki ortamda tutulan verilerdir.

2.2.2.5 Kişisel verilerin anonimleştirilmesi, silinmesi ve yok edilmesi

Kişisel verilerin silinmesi, anonimleştirilmesi, yok edilmesi esas ve usulleri Kanunla ve Kanuna dayanarak çıkartılacak ikincil düzenlemelerle belirlenecektir. Bu kapsamda, 28 Ekim 2017 tarihinde "Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik" yayımlanmıştır. Bu Yönetmelik hükümler 1 Ocak 2018 tarihi itibariyle yürürlüğe girecektir. KVKK yedinci madde kişisel verilerin silinmesi, yok edilmesi ve anonimleştirilmesi konusuna ilişkindir. Bu düzenlemeye göre, "*Kişisel Verilerin Korunması Hakkında Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş kişisel veri olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler re'sen (doğrudan) veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir*" [15].

Anonim hâle getirmenin tanımı, "*kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi*" olarak yapılmıştır [10]. Anonim hale getirmenin önemi bilimsel çalışmalarda, istatistiksel verilerin belirlenmesi bakımından ortaya çıkmaktadır. Bilimsel çalışmalarda, istatistiksel çalışmalarda kişinin kimliği belirlenmeksizin o veri araştırma ile ilgili belirli bir kritere uyuyorsa ona ilişkin istatistiklerin belirlenmesi açısından söz konusu olmaktadır. Eğer bilimsel çalışma/istatistiksel amaçlı da olsa kişinin kimliği belirlenebiliyorsa, o bilginin anonimleştiğini söylenemek mümkün olmayacaktır.

Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik kapsamında yeni tanımlar yapılmış ve kişisel verilerin anonimleştirilmesi, silinmesi, yok edilmesine ilişkin ilkeler ve prosedürler hüküm altına alınmıştır. Yönetmelik ile düzenlenmiş olan yeni kavramlar "alıcı grubu, ilgili kullanıcı, imha, kayıt ortamı kişisel veri işleme envanteri, kişisel veri saklama ve imha politikası, periyodik imha"dır. Tanımlar, Yönetmeliğin dördüncü maddesinde yer almaktadır.

Alıcı grubu, "*veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel*

kişi kategorisi"dir [15]. Veri sorumluları, işledikleri kişisel verileri ait oldukları kategorilere işleyerek sisteme kaydedecektir. İlgili kullanıcı, "*verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler"*dir [15].

Kişisel verilerin imha edilmesi, o verinin anonimleştirilmesi, silinmesi veya yok edilmesi prosedürlerinin tümünü kapsayan bir kavram olarak ifade edilmiştir. Her ne kadar imha ile yok etmek kavramları lafzi olarak aynı, benzer gibi algılansa da, Yönetmelik uyarınca kişisel verilerin yok edilmesi ile imhası aynı değildir. Kişisel verilerin imhası, kişisel veriilerin anonimleştirilerek, yok edilerek, silinerek artık kayıtlı olmamasını ifade etmektedir.

Kayıt ortamı, "*Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam*"dır [15]. Kişisel veri işleme envanteri, "*Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter*" olarak tanımlanmıştır**.** Kişisel veri saklama ve imha politikası da "*Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politika*" olarak belirtilmiştir [15]. Kişisel verilerin hukuka uygun olarak işlenmesi bakımından kişisel veri veri saklama ve imha politikası kadar veri envanteri de önem teşkil etmektedir. Bu iki hususa ne kadar önem verilir ve titiz çalışmalar yürütülürse, kişisel verilerin hukuka uygun ve minimum problemle işlenmesi mümkün kılınabilecektir.

Kişisel verilerin kayıt sisteminin bir parçası olmaktan çıkması bakımından periyodik imha kavramı söz konusu olmaktadır. Buna göre, "*kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama*

ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi" periyodik imha olarak tanımlanmıştır [15].

Anonimleştirme prosedürüne ilişkin olarak, kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir [12]. Anonim veri ve anonimleştirilmiş veri farklı kavramlardır. Anonim veri belirli bir kişiyle ilişkilendirilmesi imkânsız olan veridir. Anonimleştirilmiş veri daha önce bir kişiyle ilişkilendirilmiş; ancak artık bağlantısı kalmamış veridir [12]. Anonimleştirmede verinin büyüklüğü, çeşitliliği, o veriden sağlanmak istenen fayda ve işleme amacı gibi özellikler göz önünde bulundurularak uygulanacak hususlara karar verilir [12]. Kişisel Verileri Koruma Kurumu'nun KVKK Bilgilendirme kitapçığında anonimleştirme yöntemlerine örnek verilmek suretiyle açıklama yapılmıştır. Bu kapsamda; maskeleme, kümülatif data yaratma, veri türetme, veri karması gibi teknikler anonimleştirme prosedürü olarak kullanılan tekniklere örnektir [12].

Maskeleme, ilgili kişiye ait kişisel verilerin bazı alanlarının gizlenerek (yıldızlanarak) ya da silinerek kişinin belirli hale gelmesini önlemektir [12]. Örneğin, kişinin kimlik numarasının bir kısmının yıldızlanma durumu maskelenme tekniğine örnektir. (908 *** *** 85 gibi)

Toplulaştırma ya da diğer bir adıyla kümülatif data yaratma, verilerin birleştirilerek toplam değerlerin ifade edilmesidir [12]. Örneğin, bir üniversitedeki öğretim üyelerinden erkek olanların sayısının X olması, bunların %20'sinin profesör, % 55'inin doçent, %25'inin de yardımcı doçent olmasına ilişkin veriler toplulaştırma yöntemiyle anonim hale getirilmiştir.

Veri türetme, işlenilen verilerin daha genel karşılıklarıyla yazılmak suretiyle verileri anonim hale getirmektir [12]. Kişinin doğum tarihini gün/ay/yıl şeklinde yazmak yerine kişinin yaşının yazılması durumu veri türetme yöntemine örnektir [12].

Veri karması ise Kişisel Verileri Koruma Kurumu'nun bilgilendirme kitapçığı çerçevesinde "*Veri kümesi içinde değerlerin karıştırılarak toplam faydaya zarar vermeden kişilerin tespit edilebilirlik özelliğinin yok edilmesini ifade eder*." şeklinde tanımlanmıştır. Örnek olarak da yaş ortalaması alınmak istenen bir sınıfta kişilerin yaşlarını gösteren değerlerin birbirleriyle değiştirilmesi durumu gösterilmiştir [12].

Kişisel verilerin silinmesi, yok edilmesi konusuna ilişkin olarak KVKK'da herhangi bir tanım yapılmamıştır; ancak Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik ve KVKK gerekçesi uyarınca birtakım düzenlemeler getirilmiştir. KVKK gerekçesinde kişisel verilerin silinmesi, "*bu verilerin tekrar hiçbir şekilde kullanılamayacak ve geri getirilemeyecek şekilde imhası*" olarak tanımlanmıştır [11]. Bu tanıma göre eğer veriler kayıtlı oldukları ortamlardan (CD, dosya, harddisk gibi) geri dönüştürülemeyecek şekilde tamamen ortadan kaldırılırsa, kişisel veriler silinmiş olacaktır. Yönetmelik uyarınca ise kişisel verilerin silinmesi ve yok edilmesi arasında farklılık olduğu vurgulanmaktadır. Yönetmeliğin sekizinci maddesi kişisel verilerin silinmesini düzenlemektedir. "*Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir*" [15]. Kişisel verilerin silinmesi durumunda ilgili kullanıcılar bu verilere artık erişemeyecektir. Kişisel verilerin yok edilmesini düzenleyen dokuzuncu madde çerçevesinde "*Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir*." [15] Yani, bir kişisel veri yok edildiğinde bu veriye hiç kimse ulaşamayacaktır.

AB'de ise ilgili kişilerin kişisel verilerinin silinmesini talep etme hakları "unutulma hakkı" (right to be forgotten) kapsamında değerlendirilmiştir. Kişisel verilerin silinmesi hususu, AB'de daha detaylı bir biçimde hüküm altına alınmıştır. GDPR on yedinci madde uyarınca, maddede sayılan şartlardan birinin mevcudiyeti durumunda ilgili kişiler veri sorumlularından kişisel verilerinin derhal silinmesini talep edebilir [14]. GDPR uyarınca ilgili kişilerin kişisel verilerinin silinmesini talep edebilmesi için öngörülen şartlar Türkiye'deki mevzuatta düzenlenen şartlarla benzer olup daha detaylı düzenlediği hükümler mevcuttur. Örneğin, kişisel verilerin silinme şartları mevcut olduğu zaman veri sorumlusunun alenileştirdiği kişisel veriyi silebilmesi için

bütün teknolojik gelişmeleri ve bu teknolojilerin uygulanmasına dair masrafları gözeterek; veri sorumlusu, eğer başka veri sorumluları varsa ilgili kişinin silme talebini diğer veri sorumlularına da bildirerek makul tedbirleri almakla yükümlü kılınmıştır [14].

Kişisel verilerin silinme ve yok etme sürelerine ilişkin olarak Yönetmelikte ayrım yapılmıştır. Kişisel verilerin resen veri sorumlusu tarafından silinmesi durumu veya ilgili kişilerin talebi üzerine silinmesi durumu olarak iki kategori oluşturulmuş ve bunlara ilişkin farklı süreler öngörülmüştür. Kişisel verileri resen silme, yok etme veya anonim hale getirme süreleri, Yönetmeliğin on birinci maddesinde yer almaktadır. Kişisel verileri resen silme, yok etme veya anonim hale getirme süreleri, bu yükümlülüğün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde başlamaktadır [15]. Periyodik imha süreçleri de veri sorumlusunun hazırlayacağı kişisel veri saklama ve imha politikasında belirlenecektir ve bu süre her halde altı ayı geçemez. Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu ise yükümlülüğün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri siler, yok eder veya anonim hale getirir.Bu belirlenen süre, telafisi güç veya imkansız zararların doğması ve açıkça hukuka aykırılık olması durumlarında, Kişisel Verileri Koruma Kurulu tarafından kısaltabilir [15].

Kişisel verileri ilgili kişinin talep etmesi durumunda silme ve yok etme süreleri ise üç ihtimal doğrultusunda farklı süreler öngörülerek düzenlenmiştir:

- *Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa*: Veri sorumlusu, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir [15].
- *Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa*: Veri sorumlusu bu durumu üçüncü kişiye bildirir; ve üçüncü kişi nezdinde Yönetmelik kapsamında belirtilen gerekli işlemlerin yapılmasını temin eder [15].
- *Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa*: Bu talep veri sorumlusunca KVKK on üçüncü maddesinin üçüncü fıkrasında yer alan veri sorumlusuna başvuru prosedüründe belirtilen şekilde veri sorumlusu tarafından gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir [15].

KVKK'nın on altıncı maddesi uyarınca, kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce "Veri Sorumluları Sicili"ne kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir ve bu çerçevede sicile kayıt olma zorunluluğu veya kayıt olmama durumu ortaya çıkacaktır [10]. Kanunda veri sorumluları sicili genel hatları ile düzenlenmiş olup henüz uygulamaya geçilmemiştir; ancak Kişisel Verileri Koruma Kurumu Veri Sorumluları Sicili'ne ilişkin yönetmelik taslağı oluşturarak bu taslağı kamuoyu görüşüne açmıştır. Taslakta özet olarak Türkiye Veri Sicil Bilgi Sistemi olarak "VERBİS"in kurulacağı vurgulanmıştır. Kişisel Verileri Koruma Kurulu'nun yükümlü tutacağı veri sorumlularının sicile yükledikleri bilgilerin bir kısmı herkesin erişimine açık olacaktır [16]. Yönetmelik taslağında ayrıca VERBİS sistemine başvuru, kayıt olma ve sistemden silinme prosedürleri, süreler, VERBİS ile yapılabilecek işlemler, sicilin idaresi, denetimi, ilkeler, yaptırımlar, istisnalar gibi başlıklar da düzenlenmiştir. Veri Sorumluları Sicili Yönetmeliği, Türkiye'de ikâmet etmeyen veri sorumluları bakımından da bağlayıcı olacaktır [16].

Kişisel Verileri Koruma Kurumu, web sayfasında Veri Sorumluları Sicili'nin içeriğine ilişkin ayrıca bir bilgilendirme yazısı yayınlamıştır. Kişisel Verileri Koruma Kurumu, Veri Sorumluları Sicilinde gerçek kişiye ilişkin bilgilerin yer almayacağını; aksine veri sorumluları tarafından hangi tür kişisel verilerin ne amaçlarla işlendiği, ne kadar süreyle saklandığı ve alınan veri güvenliği tedbirleri gibi konuların bu sicilde yer alacağını belirtmiştir. Sayılan konularda bir envanter oluşturulacak ve bu envanterde yer alan bilgilerin başlıklar halinde Veri Sorumluları Siciline girişinin yapılması ile sicilin içeriği oluşacaktır [17].

AB'de veri sorumluları dosyalama sistemi (filing system) adı verilen sisteme kişisel verileri kaydetmektedir. GDPR otuzuncu madde uyarınca bu sistemin içeriğinde nelerin kaydedileceği, ne tür teknik önlemler alınması gerektiği gibi konular düzenlenmiştir. Türkiye'de ayrıntılı konular genellikle ikincil düzenlemeler aracılığı ile düzenlenmektedir. GDPR'da AB vatandaşlarının kişisel verilerine ilişkin bilgi güvenliğinin sağlanması için gerekli olan teknik ve hukuki yükümlülükler

açıklanmıştır. GDPR uyarınca dosyalama sisteminin hukuka aykırı tutulması neticesinde on milyon Euro'ya kadar idari para cezası veya şirketin bir önceki mali yılına ilişkin dünya çapındaki yıllık cirosunun yüzde ikisine kadar, kisisinden hangisi yüksekse o miktarda para cezası yaptırımının uygulanacağı belirtilmektedir [14]. KVKK'da genel ilkeler belirtilmekle birlikte, ikincil düzenlemelerle AB mevzuatında olduğu gibi teknik ve hukuki yükümlülükler detaylı bir şekilde anlatılarak yasal korumanın caydırıcılığı yüksek seviyeye erişebilir.

Son olarak, kişisel verilerin anonimleştirilmesi, silinmesi ve yok edilmesi işlemlerinde uyulması gereken ilkeler Yönetmeliğin yedinci maddesinde yer almaktadır. KVKK'da kişisel verilerin işlenmesinde öngörülen ilkeler, şartlar ve alınması gereken teknik ve idari tedbirler kişisel verilerin anonimleştirilmesi, silinmesi ve yok edilmesi işlemlerinde de geçerli olacaktır. Bunlarla beraber ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına da uygun hareket edilmesi zorunludur [15]. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır. Veri sorumlusu bu işlemlere yönelik uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklamakla yükümlüdür ve Kurul tarafından aksine bir karar alınmadıkça bu işlemlere yönelik yöntemlerden en uygun olanını seçmelidir [15]. Şayet ilgili kişi talep ederse, bu uygun yöntemi gerekçeleriyle birlikte açıklayarak seçecektir [15]. Bu düzenlemenin veri sorumlularının aydınlatma yükümlülüğü kapsamında olduğunu söylemek de yanlış olmayacaktır. Veri sorumlusu, bu aydınlatma yükümlülüğü ile yapmış olduğu işlemlerin ve talep ettiği işlemlerin gerekçelerini açıklamakla mükelleftir.

2.2.2.6 Kişisel verilerin aktarılması

KVKK sekizinci maddede kişisel verilerin üçüncü kişilere; dokuzuncu maddede ise kişisel verilerin yurt dışına aktarılmasına yönelik düzenlemeler bulunmaktadır. Bu kapsamda, kişisel verilerin üçüncü kişilere aktarılması için kişisel verilerin işlenmesindeki gibi "açık rıza" gereklidir. Genel nitelikli kişisel verilerin işlenmesine ilişkin istisnai durumlar veya yeterli önlemler alınmak kaydı ile özel nitelikli kişisel verilerin işlenmesine ilişkin maddede yer alan istisnai durumların olması halinde (2.4 numaralı başlıkta değinilecektir) ise kişisel veriler ilgili kişilerin açık rızası olmaksızın aktarılabilir. Kişisel verilerin ülke sınırları içerisinde aktarılması hususu da AB ile

paralel düzenlenmiştir. Açık rıza, GDPR uyarınca kişisel verilerin aktarılmasında temel şart olarak düzenlenmiştir.

Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz. KVKK dokuzuncu maddeye göre kişisel veriler, "*kişisel verilerin ve özel kişisel verilerin işlenmesi ile ilgili maddede düzenlenen istisnalara ilişkin belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede [10];*

- *Yeterli korumanın bulunması,*
- *Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması*",

kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir. Henüz Kişisel Verileri Koruma Kurulu tarafından yeterli korumanın bulunduğu ülkeler ve bu ülkeleri belirlemeye yarayan kriterler belirlenmemiştir. AB ve diğer ülkeler de benzer şekilde kişisel verilerin yurt dışına aktarılabilmesi için yeterli koruma sağlayan ülkeleri ve bu konuya ilişkin kriterleri belirlemektedir. Kurul, yeterli koruma sağlayan ülkeleri henüz belirlemiş olmamakla birlikte, belirlemesi hususunda kullanılacak birtakım şartlar KVKK uyarınca hüküm altına alınmıştır. Bu kapsamda, düzenlemeye göre "*Kurul, yabancı ülkede yeterli koruma bulunup bulunmadığına ve izin verilip verilmeyeceğine [10];*

- *Türkiye'nin taraf olduğu uluslararası sözleşmeleri,*
- *Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,*
- *Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,*
- *Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,*
- *Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak" [10]* suretiyle karar verir.

Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir [10].

2.3 Avrupa Birliği'nde Kişisel Verilerin Korunmasında Uygulanan Kural ve İlkeler

2.3.1 Tarihçe ve amaç

Avrupa Birliği, kişisel verilerin korunması konusunda titiz davranmaktadır. Verilerin serbest dolaşımı ve işlenmesi amacıyla 95/46/EC Avrupa Kişisel Verilerin Korunması Direktifi (The European Data Protection Directive) 24 Ekim 1995 tarihinde yürürlüğe girmiştir. Türkiye'deki 6698 numaralı KVKK da bu Direktiften uyarlanarak hazırlanmıştır, paralel hükümler bulunmaktadır. 22 Haziran 2011 tarihinde Avrupa Kişisel Veri Süpervizörü tarafından Avrupa Komisyonu Tüzüğü ("Communication") hakkında görüş yayımlanmış; 25 Ocak 2012 tarihinde de Komisyon tarafından 1995 tarihli Direktif'in çevrimiçi gizlilik hükümlerinin daha güçlendirilmesi ve Avrupa'nın dijital ekonomisinin geliştirilmesi amacıyla reform yapılması teklif edilmiştir [18]. Belirli prosedürlerden sonra, 12 Mart 2014'te Genel Veri Koruması Regülasyonu taslağı (General Data Protection Regulation - GDPR) Komisyon tarafından kabul görmüştür. Aralık 2015'te GDPR taslağı nihai hale getirilerek AB'nin organları olan Avrupa Parlamentosu, Konsey ve Komisyon tarafından uzlaşma sağlanmıştır ve nihayetinde 4 Mayıs 2016 tarihinde kişisel verilerin korunması hakkında yönetmelik (regulation) ve direktifler (directives) AB Resmi Gazete'de yayımlanmıştır [18].

Yönetmelik, 24 Mayıs 2016'da yürürlüğe girmiş olup AB'ye üye ülkeler tarafından 25 Mayıs 2018'den itibaren uygulanmaya başlayacaktır. Direktif ise 5 Mayıs 2016 tarihinde yürürlüğe girmiş olup AB'ye üye ülkeler tarafından kendi ulusal hukuklarına 6 Mayıs 2018 tarihinden itibaren uyarlanarak uygulanacaklardır. İlgili düzenlemelerin amacı; AB vatandaşlarına kendi kişisel verilerini kontrol edebilme imkânını vermek, işletmeler bakımından düzenlemeler daha da basit hale getirmek ve AB

vatandaşlarının ve işletmelerinin dijital ekonomiden tamamen yararlanabilmesidir [18].

AB Hukuku'na göre kişisel veriler sadece belirtilen koşullar altında yasal amaçla tutulabilir [19]. Kişisel verileri toplayan bireylerin/işletmelerin bu verilerin hukuka aykırı olarak kullanılmasını engelleme ve AB Hukuku çerçevesinde koruma altında olan kişisel veri sahiplerinin birtakım haklarına uyma yükümlülükleri vardır. Bireyler kişisel verilerinin yurtdışına taşınması durumunda yabancı ülkelerin bu verileri koruyabilme potansiyeli hakkında şüpheye düşerek verileri yabancı ülkelere taşımak istemeyebilirler. AB Kişisel Verilerin Korunması Hakkında Direktif kapsamında bireylerin verileri yurt dışına aktarılsa dahi bu verilerin en iyi şekilde korunabilmesi için özel hükümler de yer almaktadır [19].

GDPR'da kişisel verilere ilişkin detaylı birçok düzenleme bulunmaktadır. Kişisel verilerin korunmasında uyarınca başlıca ilkeler ve kavramlar gündeme gelmektedir. Bu konseptleri başlıca; hukuka uygun olma ve dürüstlük kuralları, ön aydınlatma, rıza, veri işleme şartları, veri koruma sorumlusu, unutulma hakkı, ilgili kişinin haklarının genişletilmesi, bilgi toplumu hizmetlerine ilişkin olarak çocuklar yönünden özel kurallar getirilmesi, tüm AB için tek bir yetkili AB otoritesi getirilmesi ve bu otoriteye ilişkin hükümler, şeffaflık, amaca ilişkin sınırlandırma, yeni yaptırımlar, yeni güvenlik ve ihlâl hükümleri, verilerin taşınabilmesi hakkı, risk temelli yaklaşım ve risklerin minimize edilmesi yaklaşımı, istişare ve raporlama olarak sayılabilir. Tez kapsamında sadece kişisel verilerin işlenme ilkeleri ele alınacaktır. Verilerin işlenme ilkeleri ve temel kurallara ise 2.4.2 numaralı başlıkta değinilecektir.

2.3.2 GDPR kapsamındaki tanımlar

Tanımlar, GDPR dördüncü maddede yer almaktadır. Buna göre tanımı yapılan yirmi altı kavram vardır. Bu kavramlardan tez konusu ile ilişkili olan ve en çok kullanılacak olan tanımlara değinilecektir.

İlk olarak kişisel veri (personal data), belirlenmiş ya da belirlenebilir gerçek kişiye (ilgili kişi) ilişkin her türlü bilgiyi; belirlenebilir gerçek kişi doğrudan ya da dolaylı olarak isim, kimlik numarası, yer bilgisi, çevrimiçi belirleyiciler ile ya da fiziksel, psikolojik, genetik, mental, kültürel ya da sosyal kimliği unsurlarından bir veya daha

fazla unsur ile belirlenmiş kişiyi ifade eder [14]. Kişisel veri tanımı, KVKK'daki tanım ile benzer olup örneklendirme yapılmak suretiyle daha detaylı açıklanmıştır. AB uyarınca da kişisel veri gerçek kişiye ilişkindir. Bu gerçek kişiye ilişkin veri belirlenebilir veya belirlenmiş olmalıdır. Kişinin dolaylı ya da doğrudan belirlenmesi önemli değildir; her ne suretle olursa olsun o verinin açığa çıkmasıyla kişinin kim olduğu anlaşılabiliyorsa, o veri kişisel veri niteliğindedir**.**

Veri işlemenin de tanımı dördüncü maddenin ikinci fıkrasında yapılmaktadır. Otomatik araçlarla olsun olmasın; kişisel veri ya da veri topluluğu üzerinde yapılan toplama, kaydetme, organize etme, yapılandırma, depolama, uyarlama veya değiştirme, geri döndürme (kurtarma); verilere ilişkin danışma, kullanma, aktarma veya erişilebilir hale getirme, sıraya getirme veya birleştirme, kısıtlama, silme veya yok etme işlemlerinin bütünü veri işlemedir (processing) [14].

İşlemenin sınırlandırılması (restriction of processing), gelecekte işlenmesi amacıyla depolanmış olan verilerin sınırlandırılması için işaretlenmesidir [14]. Profilleme (profiling), gerçek kişi ile ilgili bazı kişisel verilerinin - özellikle o kişilerin iş performansı, ekonomik durumu, sağlık durumu, kişisel tercihleri, ilgi alanları, güvenirliği, davranışları, yer ve hareket bilgileri gibi kişisel verilerinin değerlendirmek amacıyla kullanılması için herhangi bir biçimde otomatik şekilde işlenmesidir [14].

Sözde anonimleştirme (pseudonymisation), kişisel verilerin korunması amacıyla alınan teknik ve idari önlemlerden ayrı olmak üzere herhangi bir ek bilgi olmadan kişisel verinin ilgili kişiye atfedilemeyecek biçimde veya ilgili kişi belirlenebilir/belirlenmiş olmayacak şekilde işlenmesini ifade eder [14]. Bu kavram, ilk kez GDPR ile düzenlenmiştir, dolayısıyla GDPR ile AB Kişisel Verilerin Korunması Hukuku terminolojisine yeni girmiştir. "Pseudonomysation" terimi yeni bir konsept olduğu için esasen tam olarak bir Türkçe karşılığı yoktur. Mahlaslaştırma, kimliksizleştirme, sözde anonimleştirme gibi kelimelerle karşılığını türetebiliriz. Kavramın özü irdelendiği zaman "pseudo"nun birçok kullanımı olsa da genellikle bilişim alanında "sözde" anlamında gelmektedir. Dolayısıyla bu kavramı "sözde anonimleştirme" olarak uyarlamak daha yerinde olacaktır.

Sözde anonimleştirme ile anonimleştirme her ne kadar benzer gibi gözükse de aslında her ikisi de ayrı kavramlardır. Nitekim, sözde anonimleştirme sözde olduğu için benzer

gibi gözükse de farklı yönlerinin olduğu kavramın kendisinden de çıkartılabilmektedir. Sözde anonimleştirmede ayrıca korunan kişisel verilerden ek bilgi almaksızın, verinin ilgili kişiye atfedilmesi mümkün değildir. Bir veri kümesini kimliksizleştirmek için, ek bilgi ayrı yerde tutulmalıdır ve tanımlanmış veya tanımlanabilir bir kişiye atfetmeyi güvence altına alacak teknik ve organizasyon önlemlerine tabi tutulmalıdır [20].

Anonimleştirme, veri konusunun tanımlanmasının herhangi bir yolunu geri döndüremeyecek şekilde yok eder. Sözde anonimleştirme ise, veri konusunun kimliğini, veri konusunu yeniden belirlemek için ek bilgiye ihtiyaç duyacak şekilde değiştirir [21]. Örnek olarak, yazarı "Anonim" olan şiirlerin, şarkı sözlerinin, kitapların aynı kişi tarafından mı yoksa her birinin farklı kişilerce mi yazıldığını bilmek mümkün değildir. Bu, anonim kavramının da bir gereğidir. Sözde anonimleştirmede ise örnek vermek açısından mahlas kullanarak kitap yazan yazarının gerçek adı ve soyadı bilinmese de, kitabın o takma adını kullanan yazara ait olduğu bilinebilir [21]. Mesela, 20 kitap varsa ve bunların hepsi Halikarnas Balıkçısı tarafından yazılmışsa 20 kitabın da aynı kişi tarafından yazıldığını anlayabilmek mümkündür. Bu yazarın gerçek adı Cevat Şakir Kabaağaçlı olmasına rağmen mahlas kullanarak yazmayı tercih etmiştir. Aynı şekilde, Mark Twain'in yazdığı 10 tane kitap olsun. Mark Twain'in aslında gerçek kimliğinin Sam Clemens olduğu bilinmese bile, 10 kitabın tamamının da aynı kişi tarafından yazıldığı söylenebilecektir. Clemens, takma ad ile yazmıştır, anonim nitelikteki yazılarda ise kimin – kimlerin - kaç kişinin yazdığını anlamak mümkün değildir [21]. Örnek olarak aşağıda yer alan Çizelge 2.2 de incelenebilir [21]:

Çizelge 2.2: Anonimleştirme

Gerçek İsim	Sözde Anonimleştirme	Anonimleştirme
Göksu	8obc2	xxxxx
Ayşe	C1o4	*****
Ali	Ck7	xxx

Dosyalama sistemi ("filing system"), işlevsel veya coğrafi olarak dağınık, merkezileştirilmiş veya merkezileştirilmemiş şekilde belirli kriterler doğrultusunda erişilebilir olan herhangi bir yapılandırılmış veri topluluğudur [14]. KVKK uyarınca

kişisel verilerin işlenmesi bakımından veri sicilinin tutulması öngörülürken GDPR uyarınca dosyalama sistemi öngörülmektedir. Dosyalama sistemlerinin kullanılma şartları, ilkeleri, alınacak önlemler GDPR otuzuncu madde ve devamı madddelerde düzenlenmiştir. Dosyalama sistemi, karşılaştırmalı olarak Türkiye'de kişisel verilerin işlenmesi ile ilgili konu başlıkları anlatılırken de irdelenmiştir.

Veri sorumlusu (data controller), kişisel verilerin işlenme amaçlarını ve araçlarını belirleyen gerçek veya tüzel kişi, kamu kurum ve kuruluşları veya kendi veya başka kişilerle beraber diğer organları; araçları ve amaçları Birlik'in ya da üye devlet hukukunun belirlediği şekilde; Birlik veya Üye Devlet Hukuku tarafından veri sorumlusu olmak için belirlenen özel kriterleri [14] ifade eder.

Veri işleyen (processor), veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu kurum ve kuruluşları ve diğer organlardır [14].

Alıcı (recipient), üçüncü kişi olsun veya olmasın, kişisel verilerin ifşa edildiği gerçek veya tüzel kişi, kamu kurum ve kuruluşları veya başka bir organ anlamına gelir. Bununla birlikte, Birlik veya Üye Devlet hukukuna uygun olarak belirli bir soruşturma çerçevesinde kişisel veriler alan kamu otoriteleri alıcı olarak kabul edilmeyecektir; ve bu kamu yetkilileri tarafından verilerin işlenmesi, kişisel verileri işleme kurallarına uygun bir biçimde yapılacaktır [14].

Üçüncü taraf (third party); ilgili kişi, veri sorumlusu veya işleyen dışında kalan veri sorumlusu veya işleyenin yetkilili olarak kıldığı gerçek veya tüzel kişiler, kamu kurum ve kuruluşları veya diğer organları" olarak tanımlanmıştır. [14]

Rıza (consent), ilgili kişinin özgürce, o konuya ilişkin yeterli bilgi sahibi olarak ve belirsizliğe mahal vermeyecek şekilde irade beyanını dile getirmesi veyahut kendisine ilişkin kişisel verinin işlenmesini kabul ettiğine ilişkin açık olumlu hareketidir [14].

İlgili kişinin rızasının geçerli olabilmesi için tanımda sayılmış olan bütün şartların gerçekleşmesi gerekmektedir. Bir unsuru dahi eksikse, açık rızanın gerçekleşmediğini ifade etmek gerekecektir. KVKK'daki açık rızaya ilişkin tanımla da örtüşen bu tanım, kişisel verilerin ve hassas ntelikteki verilerin işlenmesi bakımından temel kuraldır.

Öncelikle, ilgili kişi ne için rıza gösterecekse o konuda bilgilendirilmesi gerekmektedir. Bilgilendirmenin kapsamı dışında kalan konular hakkında rıza göstermiş sayılmayacaktır. Ne için bilgilendirilmiş ise, o konuya ilişkin rıza gösterdiği kabul edilecektir. Başka bir konuya ilişkin rızası gerekecekse bununla da ilgili ayrıca bilgilendirilip rıza göstermesi gerekecektir.

İrade beyanı, açık olmalıdır. İlgili kişi, hiçbir tereddüte yer bırakmayacak şekilde neye ilişkin rıza gösterdiğini özgür iradesiyle vermelidir. Herhangi bir baskı altında kalmadan bilinçli bir şekilde irade açıklamasını yapmalıdır. İlgili kişini açık rızası, olumlu bir irade açıklamasına dayanmalıdır. Açık rızaya ilişkin mevzuatta herhangi bir bir şekil şartı (yazılı, sözlü vs.) öngörülmemiştir; ancak ispat bakımından rızaların dijital ortamda ya da yazılı olarak rızanın alınması yerinde olacaktır.

GDPR'da birçok tanım yapılmakla beraber, ifade edilmesi önem taşıyan son tanım ise "kişisel verilerin ihlâl edilmesi" kavramıdır. Kişisel veri ihlâli (personal data breach), iletilen, saklanan veya başka şekilde işlenmiş kişisel verilerin kazara veya kanuna aykırı olarak imhası, kaybolması, değiştirilmesi yetkisiz ifşası veya bunların erişimine neden olan bir güvenlik ihlâli anlamına gelir [14]. Bilgi güvenliğinin gizlilik, erişilebilirlik, bütünlük unsurlarını içeren bu tanım uyarınca herhangi bir unsurun güvenliğine zarar gelmesi durumunda kişisel verinin ihlâli söz konusu olmaktadır.

2.3.3 Avrupa Birliği'nde kişisel verilerin işlenmesi

GDPR beşinci maddede kişisel verilerin işlenmesi ilkeleri düzenlenmiştir. Bu kapsamda, öncelikle kişisel verilerin hukuka uygun ve dürüstlük kuralları içerisinde "şeffaf" (transparency) bir şekilde işlenmesi gerekmektedir [14].

Kişisel veriler işlenirken yasal düzenlemelerin öngördüğü çerçevede, doğru (fairness) ve gerektirdiği ölçüde, verisi işlenen ilgili kişinin istediği zaman bu veriye erişebilecek şekilde işlenmesi gerekir. GDPR Başlangıç hükümlerinden 39 numaralı paragrafa göre şeffaflıktan kasıt, ilgili kişilerin verileri toplanılırken, kullanılırken, işlenirken ya da ne ölçüde bu işlemler gerçekleştirilecekse her süreçten haberdar olabilmesidir[14]. Şeffaflık, ayrıca işlenen verilerin açık, anlaşılır ve erişilebilir olmasını da kapsamaktadır. Gerek veriyi toplayan ve işleyen veri sorumlusu gerek verisi işlenen ilgili kişi açısından şeffaflık prensibi geçerli olmaktadır. Kişisel verilerin başka amaçla

kullanılması, aktarılması durumunda ilgili kişileri haberdar etmek, ilgili kişileri sahip oldukları haklarla ilgili bilgilendirmek de bu prensibin kapsamında değerlendirilmiştir [14]. KVKK'nın onuncu maddesinde düzenlenen veri sorumlusunun ilgili kişiyi aydınlatma yükümlülüğü de benzer hükümleri içermektedir. Bu nedenle mevzuatımızdaki aydınlatma yükümlülüğünü AB mevzuatındaki şeffaflık ilkesi açıklamalarıyla bağdaştırarak kavramın özünün daha da kavranması söz konusu olabilir.

Yasallık (Lawfulness) açısından da korunması gereken hukuki yarar kavramı önem arz etmektedir. Yasallık hususu, GDPR altıncı maddede düzenlenmiştir. Bu bakımdan kişisel verilerin işlenmesi bakımından genel kurallar getirilmiş olmakla beraber, kamu yararı, kamu sağlığı ve benzeri gibi toplumun hukuki yararının kişinin kendi hukuki yararından daha önemli olması durumları için de istisnalar getirilmektedir. Kişisel verilerin hukuka uygun işlenebilmesi için, öncelikle ilgili kişilerin açık rızası gerekmektedir. Açık rıza kavramı, verinin hangi amaçla işlendiği meselesi ile yakından bağlantılıdır. Kişi, verinin hangi amaçla işleneceğini bilmelidir; böylelikle bilinçli bir şekilde açık rızasını verdiği kabul edilebilecektir.

GDPR'da açık rıza kavramına getirilen istisnalar da KVKK'da düzenlenen istisnalarla paralel özelliktedir. İstisnalar;

- *Bir sözleşmenin kurulması veya yerine getirilmesi için kişisel verilerin işlenmesi*: Bazı sözleşmelerin doğası gereği kişilerin edimlerini yerine getirebilmeleri için birtakım kişisel verilerini paylaşmaları gerekmektedir. Örneğin, bir satım sözleşmesinde taraflar banka hesap numaralarını, isim soy isimlerini, ikâmetgahlarını, hatta kimlik numaralarını belirtmek zorundadır. Sözleşmenin kurulması açısından bu verilerin işlenme zorunluluğu bulunduğu için ilgili verilerin kişilerin açık rızası olmaksızın işlenmesi söz konusu olacaktır. Ancak, kişisel verilerin işlenmesinin çerçevesini "amaç" çizdiği için; bu verilerin kötüye kullanılmaması, ifşa edilmemesi, o sözleşme amacı doğrultusunda kullanılması gerekmektedir.
- *Yasal bir zorunluluk gereği işlenmesi gerekiyor ise:* AB düzenlemeleri kişisel verilerin işlenmesine cevaz veriyorsa, bu düzenlemeler doğrultusunda kişilerin açık rızası olmadan kişisel veriler işlenebilir. GDPR altıncı maddede

düzenlenen bu hususun uygulanabilmesi için kişisel verileri işleyen veri sorumlusunun (data controller) tabi olduğu hukuk AB Hukuku veyahut üye devletin ulusal hukuku kuralları olmalıdır ve bu hukuk kuralları uyarınca açık rıza olmadan kişisel verilerin işlenebileceği düzenlenmelidir. Bu hukuk kuralları şüphe bırakmayacak şekilde açık ve belirli olmalıdır [22].

- *İlgili kişinin ya da başka bir kişinin rıza verecek durumda olmaması durumunda onun menfaatini korumak için gerekli ise:* GDPR Başlangıç hükümlerinden 46 numaralı paragrafta da bu hükümle ilgili açıklamalara yer verilmiştir. Özellikle salgın hastalıkların izlenmesi gibi insanlıkla ilgili amaçlar bakımından veya insanlık bakımından acil durum teşkil eden durumlarda (afet müdahale durumları vb.) bu hükmün uygulanabileceği açıklanmıştır. Kişisel verilerin ilgili kişiden ziyade başka bir kişinin önemli çıkarları doğrultusunda işlenmesi durumunda, verileri işlemenin dayanağı sadece başka uygulanabilir bir yasal zeminin bulunmamasına bağlıdır [22]. Kamu yararı amacıyla görevin yerine getirilmesi veya veri sorumlusuna kamu otoritesi tarafından bahşedilmiş olan yetkinin kullanılması bakımından gerekli ise
- Kamu yararı amacıyla sürdürülen bir görevin yerine getirilmesi veya veri sorumlusuna kamu otoritesi tarafından bahşedilmiş olan yetkinin kullanılması bakımından gerekli ise
- *Yasal çıkarların (legitimate interests) gerektirdiği durumlarda :* GDPR uyarınca, GDPR'ın çizdiği çerçevede hukuka aykırı olmamamk koşuluyla üye devletler kişisel verilerin işlenmesi ile ilgili başkaca düzenlemeler yapabilirler. Bu husus, yasal çıkarların gerektirdiği durumlara örnek olarak gösterilebilir.

Toplanan verilerin belirli, açık ve meşru amaçlar doğrultusunda toplanması gerekmektedir; ancak GDPR 89. maddede belirtilen kamu yararı, bilimsel, tarihsel veya istatistiksel araştırmalarla ilgili hükümler saklı tutulmaktadır [14]. Bu durum da amaca ilişkin sınırlandırma (purpose limitation) olarak tanımlanmıştır.

Verilerin minimize edilmesi (data minimization) ilkesi ise verilerin yeterli ölçüde, ilgili ve toplandığı amaç doğrultusunda işlenmesini ifade etmektedir [14]. Bunun yanında, verilerin güncel olması da büyük önem taşımaktadır. Doğruluk ilkesi (accuracy) uyarınca, verilerin işlenme amaçları göz önünde bulundurularak güncelliği kontrol edilmelidir. Şayet veriler güncel değil ise verilerin derhal silinmesi ve düzeltilmesi için gerekli her türlü makul ve uygun tedbir alınmalıdır [14].

Saklamanın sınırlandırılması (storage limitation) ilkesine göre de yine GDPR 89. Madde hükümleri saklı kalmak kaydıyla, verilerin işlenme amaçlarının gerektirdiği süre kadar saklanması gerekmektedir; bu süreler dışında ilgili kişinin kimliğinin belirlenmesini sağlayacak biçimde verilerin saklanması yasaklanmıştır [14]. Verilerin gerektiğinden fazla süre tutulması ancak arşivleme, bilimsel ve istatistiksel çalışmalar bakımından GDPR'da düzenlendiği şekilde saklanabilir.

Bilgi güvenliğinin bileşenlerinden olan gizlilik (confidentiality) ve bütünlük (integrity) de kişisel verilerin işlenmesi ilkelerinden sayılmaktadır. Kişisel verilere yetkisiz ve hukuka aykırı erişim, bu verilerin kazara kaybolması, silinmesi veya zarar görmesi de dahil olmak üzere, uygun teknik ve idari tedbirler alınarak bu verilerin korunması sağlanmalıdır [14]. Bu durum da gizlilik ve bütünlük ilkesi olarak düzenlenmiştir.

Bütün ilkelere uygun şekilde kişisel verilerin işlendiğini ve her türlü önlemin alındığını ispatlayacak taraf veri sorumlularıdır, yani bu konulara ilişkin ispat yükü veri sorumlularına aittir. Bu durum ise hesap verilebilirlik (accountability) olarak tanımlanmaktadır.

2.4 Türkiye'de Kişisel Verilerin Korunmasında Uygulanan Kural ve İlkeler

Kişisel verilerin işlenme şartları ve ilkeleri KVKK dördüncü ve beşinci madde kapsamında düzenlenmektedir. Buna göre, aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür [10]:

- *Kanunlarda açıkça öngörülmesi*: Kanunlarda kişisel verilerin işlenmesine cevaz veren hükümler bulunduğu takdirde kişisel veriler işlenebilecektir.
- *Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması:* Kişinin bilinci yerinde değilse ya da temyiz kudreti yerinde olmadığı için hukuk açısından iradesi geçerli sayılmıyorsa veyahut başkasının hayatı, beden bütünlüğü açısından gerekli ise bu durumlarda kişinin açık rızası olmadan kişisel verileri işlenebilir. Ya da kişi fiziksel açıdan rızasını açıklayamayacak durumda ise,

örneğin hürriyeti kısıtlanmış ve kendisine ulaşılamıyor ise bu kişinin yerinin belirlenmesi için kredi kartı, telefon, bilgisayar gibi teknik bir araç üzerinden verilerinin işlenmesi söz konusu olabilir [11].

- *Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması:* Burada, sözleşmenin taraflarının sözleşmenin kurulması açısından paylaşmaları gerekli olan kişisel verileri ifade eder. Sözleşmenin gereği olarak bazı kişisel veriler işlenmektedir. Örneğin, bir satış sözleşmesinde alıcı ve satıcı tarafların isim soyadı, satıcının banka hesap numarası, iki tarafın da ikâmetgah bilgileri yer almaktadır. Kira sözleşmesinde kiracının ve kiralayanın kimlik numaraları, ikâmetgah ve kiralayanın banka hesap numarası bilgileri gibi kişisel veriler yer almaktadır. Görüldüğü üzere, birçok sözleşme türünde kişisel verilerin paylaşılması sözleşmenin kurulması açısından gerekmektedir.
- *Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması:* KVKK gerekçesinde bu hususa örnek olarak bir işverenin çalışanına maaş ödemesi için çalışanın banka hesap numarası, medeni durumu, bakmakla yükümlü olduğu kişiler, sosyal güvenlik numarası gibi bilgilerinin işlenmesi gerekliliğini göstermiştir [11].
- *İlgili kişinin kendisi tarafından alenileştirilmiş olması:* Kişisel verisini ilgili kişi kendisi ifşa ederek açığa çıkartabilir. Örneğin, sosyal medyada telefon numarasını paylaşırsa, bu takdirde kendisi alenen kişisel verisini paylaştıktan sonra artık o veri kişisel veri özelliğini taşımayacaktır; çünkü artık o verinin ifşa olmasıyla sahip olduğu hukuki yarar da mevcut olmayacaktır.
- *Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması:* Bu koşula ilişkin olarak KVKK gerekçesinde temyiz kudreti yerinde olmayan veya kısıtlı birisinin yerine vasisinin ya da kayyımının, o kişinin mali bilgilerini tutması örnek olarak gösterilmiştir [11].
- *İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması:* İşçi-işveren ilişkisinde işçilerin terfisi, sosyal haklarının düzenlenmesi kapsamında veri sorumlusu sıfatına sahip işveren-şirket sahibinin meşru menfaati açısından veri işlemesi bu koşula örnektir [11].

Yukarıda belirtilen koşullar, KVKK'da tahdidi olarak sayılmıştır. Yani, bu sayılan şartlardan başka şartların olması halinde kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemeyecektir.

Özel nitelikli kişisel verilerde ise, özel nitelikli kişisel verilere ilişkin KVKK 6. maddesindeki tanımda yer alan "*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* [10]."

Özetle, sağlık ve cinsel veri dışındaki özel nitelikli kişisel veriler için genel nitelikli kişisel verilerin işlenmesine ilişkin istisnai durumlar aynen uygulanmakta iken sağlık ve cinsel verileri ile ilgili açık rıza olmadan işlenmesi için daha sıkı tutularak başka istisnalar getirilmiştir.

2.5 Diğer Ülkelerdeki Kişisel Verilerin Korunmasında Uygulanan Kural Ve İlkeler

2.5.1 Amerika

Amerika'da kişisel verilerin toplanması ve kullanılmasını düzenleyen tek, kapsamlı bir federal (ulusal) düzenleme mevcut değildir. Genel itibariyle eyaletlerin çıkarttığı düzenlemeler vardır. Bunun yanısıra, her Kongre döneminde yasaların federal düzeyde standartlaştırılması için teklifler yapılmaktadır. ABD'nin federal Kanun ve Yönetmelikleri, bazen birbirlerini kapsayan, birbirleri ile çelişen veya örtüşen yama bir sisteme sahiptir [23]. Bunlara ek olarak, devlet kurumları ve sanayi grupları tarafından geliştirilen hukuken bir üstünlüğü olmamasına rağmen "en iyi uygulamalar" olarak kabul edilen kendi kendini düzenleyici yönergelerin ve çerçevelerin bir parçası olan pek çok düzenleme bulunmaktadır [23]. Bu düzenlemelerin ortak özelliği ise içerik olarak hesap verilebilirlik ve uygulamaya elverişlilik unsurlarını içermesidir.

Amerika'da kamu otoriteleri/federal kuruluşlar için ayrı; özel sektördeki kuruluşlar için ayrı düzenlemeler mevcuttur. Sektörler arası da kişisel verilerin korunmasına ilişkin ayrı ayrı birçok düzenleme bulunmaktadır. Bu düzenlemelerden belli başlı birkaç tanesine değinilerek Amerika'nın kişisel verilerin korunmasında öngördüğü kuralların genel çerçevesi çizilecektir.

Amerika'da dağınık düzenlemelerin olması sebebi ile kişisel verilerin korunması ile ilgili birkaç düzenlemeye değinilecektir. Kişisel veriler özellikle sektörel bazda korunduğu için bu Kuruluşların da rehber ilkeleri büyük önem teşkil etmektedir. 1974 tarihli Gizlilik Yasası (Privacy Act) temel düzenlemelerden bir tanesidir. Gizlilik Yasası'nın amacı, federal kurumlar tarafından kişisel bilgilerin toplanması, bakımı, kullanımı ve kişisel bilgilerin ifşa edilmesinden kaynaklanabilecek mahremiyet ihlâllerinin istismar edilmesine karşı bireylerin korunan hakları ile hükümetin bilgileri muhafaza etme ihtiyaçlarını dengelemektir [24]. 552a numaralı bölüm altında hükümetin ve kurumların kişisel verileri ne şekilde kayıt edebileceği konusuna ilişkin düzenlemeleri içermektedir. Gizlilik Yasası'nda kişisel verileri korunan bireyler Amerika vatandaşları veyahut orada sürekli ikamet eden bireyler olarak belirtilmiştir.

"Kayıt (record) "tan kasıt ise herhangi bir verinin toplanması, kuruluşlar tarafından işlenen verilerin bireylerin eğitim durumu, mali durumu, tıbbi geçmiş, ceza veya istihdam geçmişi de dahil olmak ancak bunlarla sınırlı olmamak üzere kategorize edilen bilgiler ve kişinin adı, parmak izi veya fotoğraf gibi kişinin tanımlanmasını sağlayan tanımlayıcı numara, sembol veya diğer belirleyici belgelerdir. Bu Yasa, kamu kurum ve kuruluşları (federal kuruluşlar) bakımından uygulanmakta olup, özel sektör kuruluşları bakımından da yol gösterici nitelikte kabul edilmektedir.

Gizlilik Yasası, biteylerin kamu otoriteleri tarafından toplanan işlenen, kullanılan kişisel verilerini denetleyebilmeleri ve sorgulayabilmeleri, verilerini sildirme, güncelleme, değiştirme ve benzeri imkânları sunması açısından bir ilk olmuştur. Yasanın temel özellikleri aşağıdaki gibidir [25]:

- Bireylerin kamu otoritelerinde bulunan kişisel verilerine erişebilme, bu verileri düzeltme veya değiştirme imkânı tanınmıştır.

- Kamu otoritelerinin ya da kuruluşlarının kişisel verileri ilgili kişilerin rızası olmaksızın elde etme veya başka bir kuruma aktarma ihtimali önlenmiştir.
- Kamu otoritelerinin sadece meşruluk çerçevesinde işlemesi gerekli olan verileri doğru ve güncel tutması ve bireyler hakkında bilgi içeren tüm veri bankalarının ve dosyaların varlığını ilgili kişilere açıklamaları gerekmektedir.
- Kişilerin önceden rızası veya yazılı talebi olmaksızın kişisel verilerin başka bir kamu kuruluşuna aktarılması yasaklanmıştır.
- Kuruluşların kayıtların saklanması ve başka bir yere aktarılması ile ilgili bilgileri doğru bir biçimde tutmak ve bunları ilgili kişilere erişilebilir hale getirme yükümlülüğü getirilmiştir.
- Kişilerin kamu kuruluşları tarafından tutulan bir kaydı düzeltmek veya değiştirmek için tedbir talep etmesini ve kuruluşların "kasıtlı, istekli" olarak ihmalkar şekilde davranması durumunda uğradıkları zararların tazminini talep etme imkânı tanınmıştır.
- Merkezi İstihbarat Dairesi tarafından tutulan kayıtlar; kolluk kuvveti tarafından tutulan gizle kayıtlar; istatistiksel bilgiler; bir kişinin federal hizmet görevi gereği kişinin niteliklerini belirlemeye yarayan bilgiler; federal test materyalleri ve Ulusal Arşivlerin tarihi kayıtları muaf tutulmaktadır.
- Yasanın ihlâline neden olan kamu görevlisi veya işçi hakkında beş bin dolara kadar para cezasına hükmedileceği düzenlenmiştir.
- Kamu kuruluşlarının ilgili kişilerin adını veya adresini posta listesi kullanımı için satması veya kiralaması yasaklanmalıdır.

Yukarıdaki düzenleme dışında çeşitli sektörel ve kamu otoriteleri düzenlemeleri, eyaletin kendi düzenlemeleri bulunmaktadır. Yine önde gelen düzenlemelere örnek olarak Gıda ve İlaç İdaresi (FDA Privacy Act Regulations - yirmi birinci bölüm altında düzenlenmiştir), Sağlık ve İnsan Hizmetleri Bakanlığı Gizlilik Yasa Düzenlemeleri (HHS Privacy Act Regulations), Gizlilik Yasası Yayınları (Privacy Act Regulations - yirmi birinci bölüm altında düzenlenmiştir), Sağlık ve İnsan Hizmetleri Bakanlığı Gizlilik Yasa Düzenlemeleri (HHS Privacy Act Regulations), Gizlilik Yasası Yayınları (Privacy Act Issuances), Ulusal Arşiv ve Kayıt İdaresi kayıtları (1995 yılından günümüze kadar), Adalet Bakanlığı Gizlilik Yasası Değerlendirmesi (DOJ Privacy Act Overview (2015)) verilebilir [26].

2.5.2 Japonya

Japonya'da da kişisel verilerin korunması için düzenlemeler yapılmaktadır. Japonya'daki kişisel verilerin korunmasına ilişkin düzenleme, Kişisel Verilerin Korunması Yasası (Act on the Protection of Personal Information - APPI)'dır. Bu Yasanın temelleri 2003 yılına dayanmaktadır ve Asya'daki en eski kişisel veri düzenlemelerindenden bir tanesidir. APPI güncellenmiş olup en son hali 30 Mayıs 2017 tarihinden itibaren yürürlüğe girmiştir.

APPI, iş sektöründeki kuruluşların kişisel verilerin işlenmesi hakkında ilkeler ortaya koymaktadır. Japonya'da Kişisel Bilgileri Koruma Komisyonu (Personal Information Protection Commission (PCC)) kurularak yeni yerel gereksinimlerini nasıl uygulanacağı ve sınır ötesi veri aktarımlarını, Asya Pasifik Ekonomik Birliği'ni, yeni teknolojileri sorgulayarak bu sayede dünyanın en büyük ekonomik güce sahip ülkelerinden birisi olmayı sürdürmeyi amaçlamaktadır [27].

Güncellenmiş APPI ile Kişisel Verileri Koruma Komisyonu merkezi kişisel verileri koruma otoritesi olmuştur. Değiştirilen APPI, cezai yaptırımlarla desteklenen yürütme yetkileri olan merkezi ve özel bir düzenleyici otorite olan Kişisel Verileri Koruma Komisyonu'nu kurmuştur. APPI, geçmişte belirli özel sektör kuruluşlarını denetleyen bakanlıklara kişisel verilerin korunmasını uyarlama ve yürütme yetkisini devretmişti; ancak bu özel sektör kuruluşları arasında çelişen uygulamalara neden olmuştur ve yeknesaklık sağlanamamıştır [27].

Japonya'da da özel bakım gerektiren kişisel veriler olarak adlandırılan kategorideki kişisel verilerin kullanılması veya ifşa edilmesi için ilgili kişilerin "rıza"sı gerekmektedir. Bu kategori AB'deki hassas veriler ile; ülkemizdeki özel nitelikli kişisel veriler ile aynı niteliktedir. Dolayısıyla, bu kategoriyi özel nitelikli kişisel veriler olarak belirtmek yerinde olacaktır [28]. APPI uyarınca kişilerin ırkı, soyu, sosyal statüsü, sağlık kayıtları (engellilik durumu, check-up sonuçları, reçetesi, konulan teşhisler ve benzeri veriler), herhangi bir mahkumiyeti olup olmadığına ilişkin cezai geçmişine ilişkin verilerin tümü özel nitelikli kişisel veri olarak sayılmıştır [28].

Anonim olarak işlenen verilerin kullanılmasında veya aktarılmasında kişilerin rızası aranmamaktadır. Anonim olarak verilerin işlenmesi kavramı da APPI'nin son versiyonu ile Japonya'da kişisel verilerin işlenmesine ilişkin hukuk çerçevesinde düzenlenmiştir. Bu husus, özellikle Büyük veri ve meşru finansal analiz çalışmaları açısından faydalı olmuştur. Kişisel veriler kişiyi belirlenebilir kılacak faktörlerden arındırılarak istatistiksel amaçlarla kişilerin rızası olmadan kullanılabilecektir. Türkiye ve AB için beliritilen anonimleştirme prosedürlerinin Japonya açısından da aynı şekilde geçerli olduğunu söylemek mümkündür.

Kişisel verilerin aktarılması konusu da üç kategoriye ayrılarak düzenlenmiştir. İlk grup, kişisel verilerin sınır ötesi aktarılması işlemidir. Kişisel verilerin hukuka uygun bir şekilde sınır ötesi aktarılması için; [28]

- Kişisel Verileri Koruma Komisyonu'nun belirlemiş olduğu yeterli korumayı sağlayabileceği kabul edilen ülkelerden birisi olmalıdır.
- Yabancı bir ülkede üçüncü bir tarafa aktarılacaksa o ülkenin kişisel verileri koruma seviyesi Japonya'daki seviye ile eşdeğer olmalıdır.
- İlgili kişinin rızası olmalıdır.

Japon mevzuatında tam olarak "veri sorumlusu" kavramı bulunmamaktadır. Bununla birlikte, APPI uyarınca "iş yürütücüsü (business operator)" tanımı yapılmıştır, ve bu iş yürütücüsü kişisel verilerin işlenmesi prosedürlerinden sorumlu tutulmuştur.

İş yürütücüleri hem veri sorumlusu hem veri işleyen gibi yükümlülüklere sahiptir ve kişisel verilerin hukuka uygun, ölçülü, doğru, güncel, amacına uygun, meşru tutulmasını sağlamalıdır [28].

Yukarıdaki kısımlarda da açıklandığı üzere, Japonya'daki kişisel verilerin korunması mevzuatı da ülkemizdeki ve AB'deki düzenlemeler ile örtüşmektedir. Japonya, her ne kadar dünyanın en önde gelen ülkelerinden bir tanesi olsa da kişisel verilerin korunması konusunda yetersiz kalmaktaydı. Japonya da kişisel verilerin düzenlenmesi meselesine geç başlamış ülkelerden bir tanesidir; ancak Mayıs 2017'de yapılan güncelleme ile kişisel verilerin korunmasına ilişkin iyileştirmeler yapılmıştır ve daha yeknesak kurallar ortaya konmuştur. Kişisel Verileri Koruma Komisyonu'nun

kurulması ve merkezi bir otorite olarak görevine başlaması IPPA ile getirilen en önemli yeniliklerden bir tanesidir. Japonya da kişisel verilerin korunması konusunda yeni politikalar benimseyerek ve güncellemeler yapmak suretiyle ilerleyen ülkelerden bir tanesi olarak kabul edilebilir.

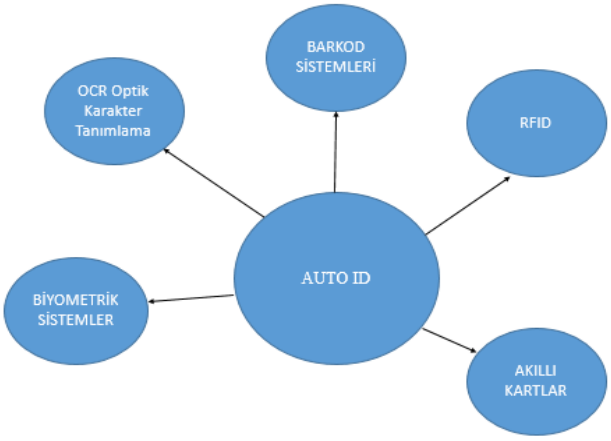
3. BİYOMETRİK VERİLERİN İŞLENMESİ

3.1 Tanımlar ve Örnekler

Teknolojinin de gelişmesiyle birlikte bilişim çağına girilmesi kaçınılmaz olmuştur. Bu çerçevede, yeni konseptler önem kazanmaya başladı; çünkü teknoloji geliştikçe teknolojiye yönelik saldırılar da aynı oranda artmaya başladı. Genel itibariyle, birisinin kimlik doğrulamasını sağlamak amacıyla aşağıda yer alan üç özellik kullanılabilir[29]:

- *Şifre ya da kişiyi tanımlama numarası (PIN) gibi kimlik sahibinin bildiği bir unsur*
- *Akıllı kart ya da jeton gibi kimlik sahibinin sahip olduğu bir unsur*
- *Kimlik sahibinin kendisini oluşturan davranışsal ya da biyolojik özellikler*

Biyometrik verileri kullanmaya yarayan sistemler otomatik tanımlama sistemlerinden bir tanesidir. Otomatik tanımlama sistemler (Auto-ID) aşağıdaki şablondaki gibi gösterilebilir:

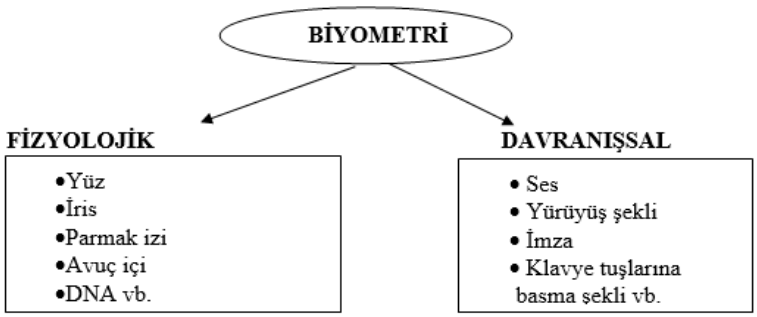


Şekil 3.1: Otomatik Tanımlama Sistemlerinin Diyagramı [30]

Bireylerin kişisel verileri daha çok elektronik ortamda tutulmaya başladıktan sonra bilişim sistemlerine saldırılar da bu doğrultuda artmaya başladı. Saldırıların da çoğalması ile zor şifrelerin bile kırılması daha kolay hale geldi ve bilgi güvenliğini

sağlamak giderek zor hale gelmeye başladı. Biyometrik verinin önemi de bu noktada ortaya çıkmaktadır. Kırılması olası parolalar yerine bilişim sistemlerine sadece o kişilere has olan biyometrik veriler ile girilmesi bilgi güvenliğini sağlamak açısından öncelikli hale getirildi. Gelecekte şifrelerin yerini biyometrik verilerin alacağını söylemek yanlış olmayacaktır.

Biyometrik verilerin tanımına ilişkin olarak birçok tanım yapılmıştır ve çeşitli ülkelerin mevzuatlarında da birbirlerine benzer tanımlar yapılmaktadır. Biyometrik ile insana ait bir özellik ifade edilmektedir. Bu özellikler biyolojik veya davranışsal olabilir. Biyometri, kişilerin kimliklerini doğrulamak amacıyla onların fizyolojik veya davranışsal özelliklerini kullanan bir konsepttir [31]. Biyometrik örnekler her bireyin kendine has ve benzersizdir. Biyometrik veriler, müdahaleci olmadan zahmetsiz bir şekilde elde edilmiş ve herhangi bir özel önlem alınmaksızın genel olarak ömür boyu değişmeden kalan verilerdir [31]. Bu özellikleri dolayısıyla güvenilirlik düzeyi yüksek olarak kabul edilmektedir. Bir bireyin biyometrik verisini değiştirmesi veya unutması mümkün değildir; çünkü ona ait özellikleri kendisi taşımaktadır. Biyometrik veriler, kimlik doğrulamada kişilerin bildiği üzerine değil de kişilerin sahip olduğuna yönelik olduğu için de oldukça pratiktir. Kişilerin irisi, parmak izi, yüzü, avuç içi, eli, sesi, imzası, yürüyüş şekli gibi tüm özellikler biyometrinin kapsamına girmektedir. Biyometrik verilerin Türk mevzuatında tanımı yer almamakla beraber biyometrik verilerin özel nitelikli kişisel veri olduğu KVKK'da belirtilmektedir. Bununla birlikte, Sosyal Güvenlik Kurumu'nun da çıkarmış olduğu "Biyometrik Yöntemlerle Kimlik Doğrulama Sistemlerine Ait Kılavuz" uyarınca sağlık kuruluşlarında avuç içi damar izi, parmak damar izi sistemlerine ilişkin düzenleme yapılmıştır. Biyometrik verileri aşağıda yer alan şekildeki gibi kategorilere ayırabiliriz [32]:



Şekil 3.2: Biyometrik veri kategorileri

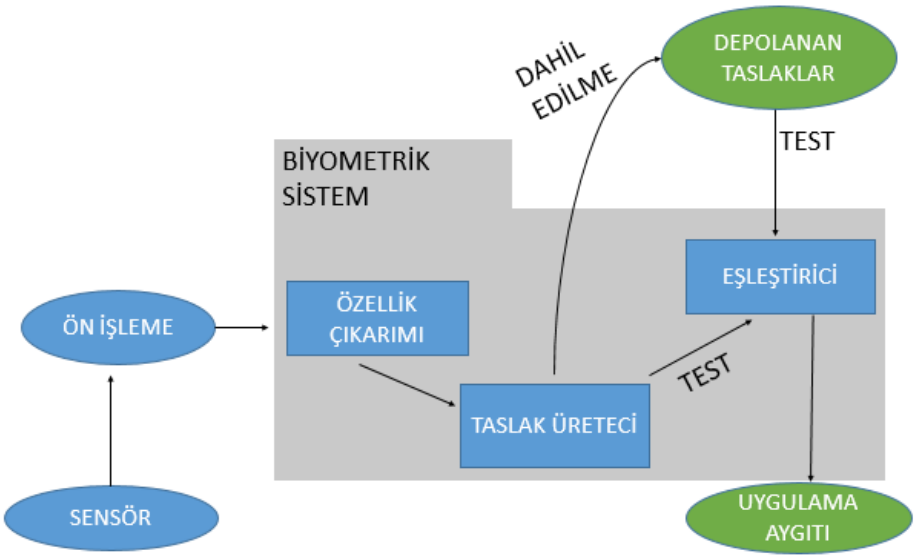
Biyometrik verilerin de kendi aralarında güvenilirlik dereceleri olduğu söylenebilir. Şöyle ki, her gözün iris yapısı farklıdır ve tek yumurta ikizlerinin bile iris dokuları farklı özelliktedir. İrisle ilgili çaşışmalar ve biyometrik veri olarak önemi, 1930'larda yürütülen çalışmalarla ortaya çıkmıştır. İris, en yapısı itibariyle biyometrik verinin en önemli kaynaklarından birisidir [29]. İris tanıma, özellikle yanlış kabul oranları söz konusu olduğunda en doğru biyometrik veri olarak kabul edilmektedir. İris dokuları örneklerinin toplanması pahalı ve karmaşık işlemler gerektirmektedir. İris tanıma, son derece güvenlikli sistem gerektiren yerlerde kullanılmaktadır [29]. İris ve retina tanıma sistemleri oldukça güvenlidir; çünkü kişilerin iki gözündeki retina yapısı bile farklıdır, kişi öldüğünde kan damarları çok hızlı çürümeye başladığı için kişi öldükten sonra da retinası alınmak suretiyle taklit edilemez. Hızlı olmasının yanında net sonuçlar da alınabildiği için hata oranı çok azdır [32].

Yüz tanıma ise bireylerin yüzünde yer alan göz yuvaları, elmacık kemikleri, ağız kenarı gibi özellikleri kullanarak bunların dijital görüntülerini bir referans şablonla karşılaştırarak kullanır [29]. Yüz tanıma da yüksek güvenilirlik derecesine sahip biyometrik verilerden bir tanesidir; ancak yüz tanıma kullanılarak birbirine benzeyen kardeşleri, tek yumurta ikizlerini ayırt etmek mümkün olmayabilir [29]. Yüz yapısı benzeyen insanları aynı insanmış gibi algılayarak her zaman doğru sonuç elde edilmeyebilir.

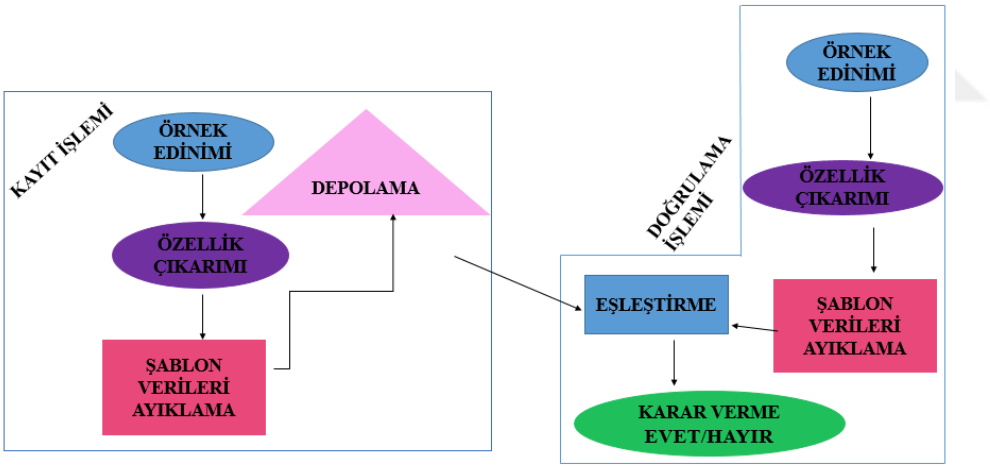
Parmak izi de en fazla kullanılan tekniklerden bir tanesidir. Parmak izi uygulaması, özellikle mobil uygulamalarda en sık kullanılan tekniklerden bir tanesidir. Aynı zamanda, en güvenilir ve doğru sonuçlar veren biyometrik verilerden biri olarak da kabul görmektedir. Otomatik parmak izi eşleştirme sistemlerinin çoğu, ayrıntı ("minutiae") olarak adlandırılan sırt uçları ve sırt ayrımlarına dayanmaktadır. Bir minutiaenin tanımlanması genellikle konumuyla (x, y koordinatları) ve sırtın yönü (θ) ile yapılır. Birleşik Devletler'deki Federal Soruşturma Bürosu'na göre iki kişinin sekizden fazla aynı minutiaeye sahip olamayacağı ifade edilmiştir [29]. Ucuz sistemlerle hızlı bir şekilde güvenilir ve verimli sonuçlar alınabildiği için parmak izi sistemleri daha çok tercih edilmektedir [33].

Ses tanıma da bir diğer biyometrik veridir. Ses, davranışsal özellikli biyometrik veridir. Her bir bireyin sesinde ton, perde, ahenk farklılığı olması nedeniyle ses de

biyometrik veri olarak kullanılabilir. Ses, kişilerin konuşurken ağızlarını hareket ettirme biçimleri ve ses tellerinin şekli nedeniyle eşsiz ve kişiye özgü olarak ifade edilir [34]. Ses tanıma da bireylerin ayırt edilmesinde güvenli, hızlı ve kolay bir yöntem olarak kabul görmektedir [33-35].



Şekil 3.3: Biyometrik kimlik doğrulama sistemi örneği



Şekil 3.4: Biyometrik sistemler ve çalışma şeması

Bunların yanında, biyometrik tanıma sistemlerinin avantajları aşağıdaki gibi sıralanabilir[30]:

- Şifre, PIN kart numarası gibi kaybetme ihtimali bulunmamaktadır. Zira, biyometrik veriler bizzat kişilerin kendileridir, vücutlarının bir parçasıdır.
- En yüksek güvenilirlik derecesine sahip korunma yöntemlerindendir.
- Kullanan kişiler için herhangi bir uzmanlık alanı gerektirmez.

- Biyometrik verisi alınan kişinin bilgileri başka bir kişiye transfer edilemez veya kopyalanamaz.
- Temassızdır; kullanıcının herhangi bir fiziksel etkileşimine ihtiyaç duyulmaz.
- Güvenilirdir; aynı zamanda da birçok sayıda kullanıcının içeriğinin kaydedilmesine ve kimlik belirleme işlemine izin veren bir teknolojidir.

3.2 Türkiye'de Biyometrik Verilerin Korunmasında Hukuki Çerçeve ve Uygulamalar

3.2.1 Biyometrik verilerin işlenmesi politikaları

KVKK'nın altıncı maddesi uyarınca biyometrik verilerin özel nitelikli kişisel veri niteliğini haiz olduğu belirtilmiştir. Özel nitelikli verilerin hassas nitelikte olması sebebiyle daha fazla koruma altında olduğu düşünülürse, biyometrik verilerin işlenmesine ilişkin kural ve ilkelerin de sıkı düzenlemelere tabi olduğunu vurgulamak gerekir. Kişisel Verileri Koruma Kurumu'nun KVKK hakkında bilgilendirme amacıyla yayımladığı "Kişisel Verilerin Korunması Kanunu ve Uygulaması" başlıklı kitapçığında da özel nitelikli kişisel verilerin önemi vurgulanmaktadır. Buna göre, "*özel nitelikli kişisel veriler, işlenmeleri halinde sahipleri hakkında ayrımcılık yapılmasına veya mağduriyete neden olma riski taşıyan verilerdir. Bu nedenle, diğer kişisel verilere göre çok daha sıkı şekilde korunmaları gerekmektedir."* [12]

Özel nitelikli kişisel verileri korumanın sıkı kurallara tabi olmasıyla birlikte, Anayasa'da da düzenlendiği üzere, bu koruma mutlak değildir ve tüm temel hak ve özgürlükler bakımından geçerli olduğu gibi diğer hak ve özgürlükler lehine sınırlanabilir [12]. Anayasa'nın on üçüncü maddesinde temel hak ve özgürlüklerin sınırlandırılmasına ilişkin düzenleme yer almaktadır. Bu kapsamda, "*Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz*" [9].

Yaşam hakkı, ifade özgürlüğü, haberleşme özgürlüğü, gibi birçok temel hak ve özgürlüğün kullanılması, özel nitelikli kişisel verilerin işlenmesini zorunlu hale getirmektedir. Örneğin; tehlikeli ve/veya sağlığa zararlı şartlar altında çalışmakta olan

kimselerin sağlık verilerinin işveren tarafından kaydedilmesi ve gerektiğinde ilgili kurum ve kuruluşlar ile paylaşılması kanuni bir zorunluluktur. Bu bakımdan, özel nitelikli kişisel verilerin işlenmesinin mutlak yasak olduğunu söylemek mümkün değildir [12].

KVKK'nın genel kişisel verilerin işlenme şartları biyometrik veriler için de geçerlidir. Genel işlenme ilkeleri yukarıdaki gibi olmakla beraber, KVKK altıncı maddede biyometrik verilerinin işlenmesini iki kategoriye ayırmıştır. Bunlar; sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler ve bu ikisi dışında kalan altıncı maddede sayılan diğer özel nitelikli kişisel verilerdir. Bu çerçevede, sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir [10]. Yani genel kişisel verilerin işlenmesine ilişkin yukarıda açıklanmış olan ilkeler geçerli olacaktır. Öncelikle, genel nitelikli kişisel verilerde de olduğu gibi ilgili kişilerin açık rızası gereklidir. Buna ek olarak, işlenen biyometrik verilerin hukuka ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekmektedir. Aynı kurallar AB normlarında, Birleşmiş Milletler Rehber İlkeleri'nde ve İngiltere BS 10012 – Kişisel Bilgi Yönetim Sistemi ("Personal Information Management System")'nde de yer almaktadır.

Gerekli olan süre belirlenirken biyometrik verinin alınma amacı da önem arz etmektedir. Biyometrik verilerin işlenme amacının ortadan kalkması ile birlikte o biyometrik verinin saklanmasının da bir anlamı olmayacaktır. Yine Kanunlara uygun bir biçimde ve güncel olarak biyometrik verilerin saklanması gerekmektedir. Tutulan veriler doğru olmalıdır ve meşru amaçlarla gerektiği derecede işlenmelidir. Amacın gerektirdiğinden fazla biyometrik verinin işlenmesi iyiniyet olarak sayılamayacaktır ve dürüstlük kurallarına da aykırılık teşkil edecektir. İşte bu ölçüde de sınırlılık ve meşruluk ilkelerini vurgulamak yerinde olacaktır.

Sağlık ve cinselliğe ilişkin kişisel verilere ilişkin olarak ise, bu veriler "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." [10] Bütün bu ilkelere ek olarak, KVKK uyarınca Kişisel Verileri Koruma Kurulu'nun özel nitelikli kişisel verilerin işlenmesi bakımından yeterli önlemleri alması şartı da düzenlenmiştir.

3.2.2 Bankacılık sektöründe biyometrik verilerin işlenmesi

Bankacılık sektöründe de biyometrik verilerin kullanılması söz konusu olabilmektedir. Bankaların mobil uygulamalarında kişinin belirlemiş olduğu şifre yerine yüz tanımayla, parmak iziyle girmek suretiyle biyometrik veriler kullanılmaktadır. Örneğin, Garanti ve Yapı Kredi Bankaları göz tanıma ile mobil uygulamadan giriş yapılmasına imkân tanırken Türkiye İş Bankası da parmak izi ile mobil uygulamaya giriş imkânı tanımakta idi. Ancak, Türkiye İş Bankası 2016 yılında parmak izi ile mobil uygulama kullanılmasını kaldırarak şifre yöntemine geri dönmüştür. Bu durumu kendi internet siteleri üzerinden de açıklama yaparak müşterilerini bilgilendirmişlerdir. Bu çerçevede, "İşCep'e parmak iziyle (Touch ID) giriş özelliği kaldırılıyor. Ülkemizde uygulanan bankacılık düzenlemeleri çerçevesinde İşCep'e 'Parmak iziyle Giriş' özelliğinin sonlandırılması ihtiyacı doğmuştur. 28 Mart 2016 tarihinden itibaren parmak izi teknolojisinin İşCep'e girişlerde kullanılamayacağını belirtmek isteriz [36]." açıklamasını yapmak suretiyle parmak izi yöntemi kaldırılmıştır. Bu yöntemin kaldırılmasının sebebi, parmak izi bilgileri akıllı cihazlarla paylaşıldığı için biyometrik verilere ilişkin bilgilerin akıllı telefon sunucusuna da gitmesi ve bankacılık uygulamalarında tam güvenliğin sağlanamayacağı durumudur. Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ uyarınca da bankaların bilgi sisteminde sahip olmaları gereken mekanizma ana hatları ile belirtilmiştir. Ayrıca, bilgi sistemleri üzerinde tesis edilen yönetimin etkinliğinin risk yönetimi, iç kontrol sistemi ve iç denetim kapsamında yürütülecek çalışmaların da katkısıyla sağlanacağı vurgulanmıştır [37].

Öncelikle, Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ 4. Maddesine göre biyometrik kavramının tanımı yapılmıştır. Buna göre, biyometrik "*bir kişinin diğer şahıslardan ayrılmasını sağlayan, bu kişiye ait ölçülebilir bir biyolojik veya davranışsal karakteristiği*" olarak tanımlanmaktadır [37]. Yukarıda da biyometrik verinin tanımı yapılırken fizyolojik ve davranışsal özelliklerden oluştuğu belirtilmişti. Bu kapsamda, yapılan tanım biyometrik

kavramının özünü vurgulayan doğru bir tanım olmuştur. İlgili tanım GDPR'daki tanımla da örtüşmektedir.

Banka Bilgi Sistemleri Tebliği'nin 27. Maddesi kimlik doğrulamayı düzenlemektedir. Bu çerçevede, "Müşterilere uygulanan kimlik doğrulama mekanizması birbirinden bağımsız en az iki bileşenden oluşur. Bu iki bileşen; müşterinin "bildiği", müşterinin "sahip olduğu" veya müşterinin "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Müşterinin "bildiği" unsur olarak parola/değişken parola bilgisi gibi bileşenler, "sahip olduğu" unsur olarak tek kullanımlık parola üretim cihazı, kısa mesaj servisi ile sağlanan tek kullanımlık parola gibi bileşenler kullanılabilir. Bileşenler tamamen müşterinin şahsına özgü olmalı ve bunlar sunulmadan kimlik doğrulama gerçekleştirilememeli, hizmetlere erişim sağlanamamalıdır. (…) Kimlik doğrulamada kullanılacak şifreleme anahtarları; bu anahtarların ele geçirilme ihtimallerini en aza indiren, gizliliğini sağlayan, değiştirilmesini ve bozulmasını önleyecek yöntemler barındıracak şekilde müşteri kullanımına sunulur. Şifreleme anahtarları kimlik doğrulama için kullanılmak istendiklerinde parola, PIN (Kişisel Tanımlama Numarası) veya biyometrik bir bileşen bilgisi ile erişilebilir olmalıdır [37]."

Türkiye'de, 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 23. Maddesi uyarınca, "*Kart çıkaran kuruluşlar, edindikleri kişisel bilgileri 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* [38]." Burada, Kanun uyarınca bankaların kişisel bilgileri tutarken yeterli önlemleri almaları gerektiği belirtilmiştir. Bu çerçevede, kişisel verileri işleyen bankaların kişisel verileri korumak için KVKK'daki düzenlemelere uyma zorunluluğu vardır. Kişisel verilerin korunması kadar, sistemlerinin güvenliğine de önem vermeleri gerekmektedir. Bu çerçevede, hem mevzuatsal hem de teknik önlemleri alarak kişisel verilerin korunmasını sağlamalıdır.

Yine, Bankaların İç Sistemleri Ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik'te yer alan 11. maddeye göre bankalar müşterilerden aldıkları bilgilerin korunması için Kanunlarda ve ikincil mevzuatlarda belirtilen asgari standartlara uymakla yükümlü kılınmıştır. Aynı maddede, bankaların yerine

getirmekle yükümlü ve sorumlu olduğu faaliyetler bakımından kendi bilgi sistemlerinde "*gerekli olan bütün bilgilerin, elektronik ortamda güvenli ve istenildiği an erişime olanak sağlayacak şekilde kaydedilmesi ve kullanılması*" gerekmektedir [39]. Bilgi güvenliğinin sağlanması ve düzenli olarak güncellenmesi de önem arz etmektedir. Bilgilerin doğru ve güncel tutulması kişisel verilerin işlenmesi hukuka uygun olarak işlenebilmesi için öngörülen ilkelerden bir tanesini oluşturmaktadır. Düzenlemede yer alan "her an erişime olanak sağlayacak şekilde" ibaresi ile bilgi güvenliğinin unsurlarından erişilebilirlik faktörüne vurgu yapılmaktadır. Verilere yetkili kişiler tarafından yetkileri doğrultusunda kullanılmak suretiyle erişilebilirlik sağlanmalıdır. Güncellik, bilgilerin doğru olabilmesi ile de doğru orantılı olduğu için her bilginin güncel ve doğru olması gerekmektedir.

Yurt dışında da bankaların çoğu biyometrik verileri uygulamada kullanmaktadır. Örnek olarak, Lloyds Banking Group bünyesindeki Halifax, dijital finansal hizmetlere erişimde kimlik doğrulamada müşterisinin kalp atışlarını temel alan bir teknoloji denemiştir. Bir Finlandiya şirketi olan Uniqul, ödeme yapmak isteyen müşterilere yüz tanıma sistemini kullandırtmaktadır [40]. Japon Telekom şirketi NTT DOCOMO ve Fujitsu'nun hayata geçirdiği akıllı telefon da, mobil ödeme yapmak isteyen kullanıcılarını iris tarama olanağını sunmaktadır [40].

Kişisel veri düzenlemelerinin Türkiye'de yürürlüğe girmesiyle birlikte özellikle bankaların uyum sürecinde gerekli çalışmaları yaparak önlem sağlamaları önem teşkil etmektedir. Dünya genelindeki sektörlere bakıldığı zaman kişisel verileri en fazla işleyen sektörlerden birisi olarak bankacılığı göstermek yanlış olmayacaktır. Türkiye'de bankacılık sektöründe yer alan düzenlemeler özetle yukarıda belirtildiği gibi olmakla beraber daha ayrıntılı düzenlemelere ihtiyaç duyulduğunu söylemek yerinde olacaktır. Özellikle ileride şifrelerin yerine biyometrik verilerin kullanılacağını düşünürsek bankalar için özel sistemler geliştirilmeli ve biyometrik verilerin toplanması hakkında detaylı düzenlemelerle desteklenmesi gerekecektir.

3.2.3 Sağlık sektöründe biyometrik verilerin işlenmesi

Türkiye'de, kişisel verilerin işlenmesi konusundaki en geniş düzenleme sağlık sektöründe görülmektedir. Sağlık sektöründe hastaların özel nitelikli kişisel veri niteliğindeki verileri tutulduğu için kişisel veri düzenlemeleri önemli yer

kaplamaktadır. Özellikle ikincil düzenlemelerle kişisel verilerin korunmasına yasal dayanaklar hazırlanmıştır. Yasal olarak korumayı sağlamanın yanında, güvenilir teknoloji ile verileri tutabilmek için veritabanları, elektronik sistemler de mevcuttur. Bu elektronik sistemlerin bir kısmı hali hazırda uygulanmakta olup, bir kısmı da iyileştirme ve güncelleme çalışmaları kapsamında pilot olarak uygulanmaktadır.

"Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelik" 20 Kasım 2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Yönetmeliğin amacı, "*kişisel verilerin korunması ve veri mahremiyetinin sağlanmasına, kişisel sağlık verilerini toplama, işleme, aktarma, bu verilere erişim için kurulacak sisteme, kişisel sağlık verisi kaydı tutulan sistemlerin güvenliği ve denetimi ile sağlık hizmeti sunumundaki personel hareketlerinin Bakanlığa bildirilmesine ilişkin işlemlerde uyulacak usul ve esasları düzenlemektir*" [41]. Yönetmelikte anonim hale getirme, kişisel veri, kişisel sağlık verisi, kişisel sağlık verisinin işlenmesi gibi kavramların tanımları yapılmıştır. Anonim hale getirme, veri işleyen, veri sorumlusu, kişisel sağlık verilerinin işlenmesi kavramları KVKK'daki gibi tanımlanmıştır. Kişisel sağlık verisi de kişisel verinin tanımı ile neredeyse birebir olarak "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü sağlık verisi*"; merkezi sağlık veri sistemi ise "*Bakanlık tarafından oluşturulan kişisel sağlık verilerinin toplandığı sistem*" olarak tanımlanmıştır [41].

Sağlık sektöründe kişisel verilerin işlenme ilkeleri KVKK'da belirtilen kişisel verilerin işlenme ilkeleri ile aynıdır. Kişilerin sağlık verilerinin işlenmesi için kişilerin açık rızası gerekmektedir. Sağlık hizmet sunucularında görevli kişiler ilgili kişinin sağlık verilerine ancak verilecek olan sağlık hizmetinin gereği ile sınırlı olmak kaydıyla işleyebilir ve erişebilir [41]. Bu husus, ölçülülük ilkesinin de bir uzantısı olup verilerin işlendiği amaçla yetkililerin verileri işleyip bu verilere erişebileceklerini vurgulamaktadır. Kişisel sağlık verilerini işleyen veya görevi gereği kişisel sağlık verilerine erişen herkes, bu verilerle ilgili olarak sır saklama yükümlülüğü altındadır [41].

Sağlık hizmet sunucularında veri işleyen kişiler, kişisel sağlık verilerini sağlık hizmet sunucularının tamamen veya kısmen otomatik olan ya da otomatik olmayan her türlü sistemleri ile Bakanlığın ülke genelinde hizmet vermek amaçlı kurulan sistemleri

dışında hiçbir yere kopyalayamaz veya kaydedemez [41]. Aynı zamanda, hukuka ve standartlara uygun elektronik kayıt sistemlerinin kurulmasından ve işletilmesinden, güvenlik ve mahremiyetinin sağlanmasından, ayrıca elektronik sağlık kayıtlarının merkezi sağlık veri sistemine aktarılmasından da sorumlu tutulacaklardır.

Sağlık Verilerinin İşlenmesi Yönetmeliği'ne göre işlenen veriler istatistiksel veya bilimsel çalışmalarda kullanılmak kaydıyla verilerin anonimleştirilmesi prosedürleri gerçekleştirilebilir. Bu durum, KVKK hükümleri çerçevesinde gerçekleştirilecek olup özellikle istatistiksel verilerin sağlık sektöndeki önemi de göz önünde bulundurulduğunda dikkatli bir şekilde gerçekleştirilmesi gereken prosedürlerden birisidir.

İlgili kişinin ayrıntılı bir şekilde bilgilendirilmesi, yazılı rızasının alınması ve bu rızanın muhafaza edilmesi hâlinde ilgili kişiye ait sağlık verileri, rıza doğrultusunda işlenebilir ve aktarılabilir [41]. Sağlık verilerinin korunması için Sağlık Bakanlığı ve Kişisel Verileri Koruma Kurulu ilkeler ve standartlar belirleyebilirler. Sağlık hizmet sunucuları bu ilke ve kurallara uymakla ve gerekli bütün tedbirleri almakla yükümlü kılınmıştır. Kişisel veri ihlâli yaşandığı takdirde izlenecek usul ve esaslar, verilerin işlenmesi, aktarılması, silinmesi, veri sorumlusu ve veri işleyene yönelik hükümler de bu Yönetmelik kapsamında düzenlenmektedir.

Sağlık verileri özel nitelikli kişisel veri olduğu için bu verilerin açık rıza olmadan işlenebilme şartları KVKK'da hüküm altına alınmıştı. Yönetmelikte de aynı şekilde "*Kişisel sağlık verileri; 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*" [41] hükmü ile sağlık verilerinin işlenebilme şartları sayılmıştır. Kişisel verilerin aktarılması için de keza aynı şartlar öngörülmektedir.

İlgili kişinin rızasını geri alabilmesi de mümkündür. Yönetmeliğe göre, "İlgili kişi, aksi yönde bir hukukî düzenleme veya yargı kararı bulunmaması halinde verilerinin işlenmesi ve aktarılması için vermiş olduğu rızayı istediği zaman geri alabilir [41]. Rızanın geri alınması, o tarihe kadar yapılmış bulunan işlemler bakımından etkili

olmaz.” Rıza geri alındığı takdirde geçmişte yapılan işlemleri de kapsamayacak; ileriye yönelik etkili olacaktır.

Sağlık Verilerinin Korunması Yönetmeliği’nde de adı geçen Bilgi Güvenliği Politikaları Yönergesi, 663 Sayılı “Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname” ve 5651 Sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun”a dayanılarak çıkarılmıştır. Bu Yönerge ilkeleri sağlık sektöründe de uygulanacaktır. Bu Yönergenin amacı, Sağlık Bakanlığı’nın görevleri kapsamında; bilgilerin toplanması, raporlanması, değerlendirilmesi ve paylaşılması süreçlerine ilişkin gerekli tedbirleri almak; bilgi güvenliğinin unsurları olan gizlilik, bütünlük ve erişilebilirlik çerçevesinde değerlendirilerek içeriden ve/ya dışarıdan kasıtlı veya kazara oluşabilecek tüm tehditlerden korunmasını sağlamak ve yürütülen faaliyetlerin etkin, hızlı, güvenli ve doğru olarak gerçekleştirilmesinde bilgi güvenliğinin sağlanması için usul ve esasları göstermektir [42].

Yönergede de veri, bilginin işlenmemiş halini ifade etmektedir [42]. Terminolojik olarak da kabul gördüğü üzere, bilgi ve veri aynı kavramlar olmayıp işlenmiş veriler bilgiyi oluşturacaktır. Yani, girdiler veri iken çıktılar bilgiyi oluşturmaktadır. Yönergede bilgi güvenliği ilkeleri ve politikaları genel bir çerçeve çizilerek düzenlenmiştir. Sağlık Bakanlığı ve Genel Müdürlükler tarafından ayrıntılı bir Kılavuz oluşturularak bilgi güvenliğine ilşkin yetki ve sorumlulukların burada paylaştırılacağı, tüm sağlık personellerinin de bu Kılavuzdan bilgi sahibi olmalarının sağlanacağı belirtilmektedir. İlgili Kılavuz oluşturulmuş olup Sağlık Bakanlığı’nın web sitesinde de yer almaktadır. Kılavuz uyarınca bilgi güvenliği politikaları, Bilgi Güvenliği Yönetim Sistemi (“BGYS”) yer almaktadır. Kılavuzda hukuki yükümlülükler, bilgi güvenliği politikaları gibi yasal nitelikli bilgiler bulunduğu kadar teknik konular da bulunmaktadır. Kriptolama yöntemleri, yazılımsal özellikler, bilgi güvenliği testleri, veritabanı özellikleri vb. hususlar Kılavuz kapsamında açıklanmaktadır.

5510 Sayılı Sosyal Sigortalar Ve Genel Sağlık Sigortası Kanunu’nda yer alan altmış yedinci madde uyarınca “genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden ve diğer haklardan yararlanabilmeleri için sağlık hizmet sunucularına başvurduklarında acil haller hariç olmak üzere (acil hallerde ise acil halin

sona ermesinden sonra); biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya Kurum tarafından verilen resimli sağlık kartı belgelerinden birinin gösterilmesi zorunludur [43].” düzenlenerek sağlık hizmetlerinde biyometrik verinin kullanılabilmesine cevaz verilmiştir. Bu maddeden hareketle, SGK tarafından pilot uygulaması yapılan ve başarı ile sonuçlanan Biyometrik Kimlik Doğrulama Yöntemlerine ait düzenlemeler yapılmıştır. Bu düzenleme uyarınca avuç içi tanımlama sistemi tanımlanarak detaylı bir şekilde anlatılmıştır. SGK'nın hazırlamış olduğu kılavuz, hem avuç içi taramam sisteminin güvenlikli teknik yapısını anlatmakta, hem de gerekli yasal zorunlulukları belirtmektedir.

Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliği'nde de benzer düzenleme yer alarak sağlık hizmetlerinde biyometrik verinin kullanılabileceği ifade edilmiştir. “Kimlik tespiti” başlıklı madde 1.6'da ve “Biyometrik kimlik doğrulama işlemi” başlıklı madde 1.6.1 kapsamında biyometrik veriye ilişkin düzenlemeler hüküm altına alınmıştır.

SUT 1.6'ya göre “Sağlık kurum ve kuruluşlarınca, kişilerin müracaatı aşamasında, acil hallerde ise acil halin sona ermesinden sonra, nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya verilmiş ise Kurum sağlık kartı belgelerinden biri ile kimlik tespiti ve biyometrik yöntemlerle kimlik doğrulaması yapılması zorunludur. Kimlik tespiti, biyometrik kayıt işlemi veya biyometrik kimlik doğrulama işlemini usulüne uygun yapmayan ve bu nedenle bir başka kişiye sağlık hizmeti sunulması nedeniyle Kurumun zarara uğramasına sebebiyet veren sağlık hizmeti sunucularından ödenen tutar geri alınır [44].” 5510 Sayılı Kanun'daki düzenleme ile paralel olarak SUT ile kişilerin sağlık kuruluşlarına müracaat aşamasında biyometrik verilerinin alınabileceği bu suretle belirtilmiştir. Biyometrik kayıt işlemi ve biyometrik kimlik doğrulama işleminin usulüne uygun yapılması zorunluluğuna dikkat çekilmiştir. İlgili düzenleme ile ayrıca kişisel verilerin hukuka uygun olarak saklanabilmesi için getirilen ilkelerden “doğru olması, güncel olması” unsurlarını vurguladığını da söylemek yerinde olacaktır.

SUT 1.6.1 uyarınca, “Kimlik doğrulamada kullanılacak olan biyometrik sistem ve uygulamaya geçilecek sağlık hizmeti sunucuları, uygulama tarihi ile uygulamaya

ilişkin usul ve esaslar Kurum (SGK) tarafından belirlenir [44].” Nitekim, bu doğrultuda SGK Biyometrik Yöntemlerle Kimlik Doğrulama Sistemlerine Ait Kılavuz çıkarmıştır. Aynı maddenin ikinci fıkrasında ise “Kişinin sağlık hizmeti sunucusuna müracaatı sırasında ilk biyometrik verinin Kurum veri tabanına kayıt işlemi, sağlık hizmeti sunucusu tarafından yapılacaktır [45].” hüküm altına alınmıştır. Burada, veri sorumluları olarak Sağlık kuruluşları, veri işleyen olarak da sağlık kuruluşlarının yetkilendirmiş olduğu kişiler anlaşılacaktır. Biyometrik verisi alınmayacak durumlar da aynı Kılavuz'da belirtilmektedir. Bu doğrultuda [45];

- 12 yaş ve altı çocuklara, 75 yaş ve üstü kişilere,
- Acil hastalara(yeşil alan muayenesi hariç)
- Organ, doku ve kök hücre nakli tedavilerinde alıcının üzerinden donör takibinin alındığı durumlarda
- Yenidoğan için anne T.C. kimlik numarası üzerinden takip alınan durumlarda
- Tedavi türü günübirlik veya yatan ise
- Provizyon tipi “acil” veya branşı “acil-4400” ise (yeşil alan muayenesi hariç)

biyometrik veri alınmayacaktır.

Kimlik Doğrulama Kılavuzu'nda kimlik doğrulama işlemi tanımı yapılmıştır. “Genel sağlık sigortalısının, ilk kayıt işlemi sonrasındaki biyometrik verisi ile sağlık hizmet sunucusuna başvuru aşamasında alınması gereken sağ veya sol eline ait avuç içi damar izi veya sağ ve sol eline ait işaret ve orta parmaklardan herhangi birisinin biyometrik verisinin karşılaştırılması sonrasında kimlik tespitinin doğrulamasını ifade eden ve sistem tarafından üretilen onaylama kodu” [45] kimlik doğrulama işlemidir. Yapılan tanım uyarınca avuç içi ve parmak izi gibi biyometrik verilerin kullanıldığını söylemek mümkün olacaktır. Biyometrik sistem ise SGK KDK Ek- 1'de yer alan “teknik özellikleri ayrı ayrı belirtilen biyometrik kimlik doğrulama ünitelerinin bileşenleri”dir. [45] SGK KDK Ek-1'de ise üç çeşit parmak damar izi sistemi en ince detaylarına kadar anlatılmaktadır. Bu kılavuzda bahsedilen biyometrik veriler avuç içi ve parmak izi verileridir. SGK KDK ilk çıktığı zamanlar biyometrik verisini veren kişinin açık rıza vermesi için rıza formu imzalama gerekliliği düzenlenmişti. 13 Temmuz 2016 tarihinde SGK web sitesinde yaptığı duyuru ile bu zorunluluğun ortadan kalktığını duyurmuştur. KVKK uyarınca açık rıza kavramı için yazılı şekil şartı öngörülmediği

için rıza için yazılı şekil şartı öngören düzenlemenin kaldırılması yerinde olmuştur. Yine de ispat hukuku uyarınca açık rızanın dijital ortamda veyahut yazılı bir biçimde alınması veri sorumluları bakımından önem teşkil edecektir. Dolayısıyla böyle bir zorunluluk ortadan kalkmış olsa da kişilerin açık rızasının yazılı ya da dijital ortamdan alınması veri sorumluları ve veri işleyenler bakımından faydalı olacaktır.

MEDULA sistemi Sağlık Bakanlığı tarafından oluşturulan ve yürürlüğe konan merkezi bir programdır. İnternet üzerinden erişilebilen MEDULA sistemi sayesinde hastaneler, doktorlar, eczacılar ve optisyenler tıbbi cihaz, ilaç, sağlık malzemeleri, teşhis, tanı vb. kayıtlaSrı sisteme girer veya sistem üzerinde takip ederler [46]. Hastaların kabul işlemleri, fatura takip işlemleri vb. bilgiler bu sistemden takip edilebilmektedir. MEDULA'da Eczacı, optik, doktor ve hastane olmak üzere dört çeşit sistem bulunmaktadır. MEDULA tarafından biyometrik doğrulama ile alınan veya biyometrik kimlik doğrulamaya gerek olmayan durumlarda da takip hasta kabul kimlik doğrulama metodu kullanılarak hastalar takip numaralarını alabileceklerdir [47].

Yukarıda anlatılan sistemler dışında, Sağlık Bakanlığı'nın denemekte olduğu pilot uygulamalar da bulunmaktadır. Kişisel verilerin ve biyometrik verilerin güvenle muhafazası için gerekli bütün çalışmaların yürütüldüğünü söylemek yerinde olacaktır. SGK'nın biyometrik verilerin alınmasına yönelik çıkarmış olduğu kılavuz da biyometrik veri işleyen veri sorumlularına örnek teşkil edecek nitelikte bir kılavuzdur. Bu kılavuzun veri sorumlularına yol gösterdiğini söylemek mümkün olacaktır.

3.2.4 Haberleşme sektöründe biyometrik verilerin işlenmesi

Biyometrik veriler ulaşım, haberleşme, güvenlik gibi sektörlerde kullanılmaktadır. Bankacılık ve sağlık sektöründen sonra biyometrik verilerin en fazla haberleşme sektöründe kullanıldığını söylemek yerinde olacaktır. Haberleşme sektöründe de kişisel ve biyometrik verilerin işlenmesi söz konusu olabilmektedir. Şu an yüzde olarak kişisel verilerin kullanımı biyometrik verilerin kullanımına göre fazla olsa da teknolojinin gelişmesi ile ileride haberleşme sektöründe de biyometrik verilerin büyük önemi olacağını söyleyebiliriz. Biyometrik veriler haberleşme sektörü için de önem arz etse de, bu sektörde bütün veri türlerini kapsayan genel kişisel verilerin işlenmesi ile ilgili düzenlemeler yer almaktadır.

İster bankacılık ister haberleşme olsun bütün sektörler kişisel verilerin işlenmesinde KVKK'yı esas alacaklardır. KVKK yürürlüğe girmeden önce haberleşme sektöründe "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik" 7 Temmuz 2012 tarihinde Resmi Gazete'de yayımlanmıştır. Bu Yönetmelik, dördüncü maddesinin ikinci fıkrası hariç olmak üzere (ilgili madde 1 Ocak 2014 tarihinde yürürlüğe girmiştir) 24 Temmuz 2013 tarihinden itibaren geçerli olmak üzere yürülüğe girmiştir. Elektronik Haberleşme Sektörüne İlişkin Kişisel Verilerin Korunması Hakkında Yönetmelik, 5809 Sayılı Elektronik Haberleşme Kanunu'na dayanılarak hazırlanmıştır.

Yönetmeliğin amacı, "elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması için elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenlemektir [13]." Diğer bir deyişle, elektronik haberleşme sektöründeki veri sorumluları ve veri işleyenlerin uymaları gereken prosedürler bu Yönetmelik kapsamında düzenlenmektedir. Haberleşmenin içeriğine ilişkin verilerin saklanması bu Yönetmeliğin kapsamına dâhil değildir. Zira Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hâle Getirilmesi Hakkında Yönetmelik'te veri sorumlularının verileri saklama süreleri, hazırlamaları gerekli olan imha politikaları vb. konular düzenlenmiştir; başkaca ikincil düzenlemelerin de çıkması planlanmaktadır.

Elektronik Haberleşme Sektörüne İlişkin Kişisel Verilerin Korunması Hakkında Yönetmelik uyarınca kişisel veri kavramı, "*Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler*" olarak tanımlanmıştır [13]. KVKK uyarınca kişisel veri belirli veya kimliği belirlenebilir gerçek kişiye ilişkin tüm bilgiler olarak tanımlanmıştı. Elektronik haberleşme sektöründe kişisel verilerin korunmasını düzenleyen yönetmelik hükümleri uyarınca tüzel kişilerin de verilerinin kişisel veri niteliğini haiz olduğu belirtilmektedir. KVKK'daki kişisel veri tanımı ile çelişen bu durumun düzeltilmesi gerekmektedir. Zira, sadece ülkemizde değil AB ve diğer ülkelerin kişisel veri düzenlemelerinde de tüzel kişi verileri kişisel veri olarak kabul edilmemektedir; ilgili ceza hukuku, idare hukuku, ticaret hukuku gibi mevzuatlar tarafından korunmaktadırlar. Bu tartışmalı husus içtihat hukuku ile de açığa kavuşturulabilir; ancak bu tanımın değiştirilmesi mevzuat terminolojisinde bütünlük sağlanması ve uygulamada sorun teşkil etmemesi açısından faydalı olacaktır.

Aynı Yönetmelikte kişisel verilerin ihlâli, "İstem dışı, yetki dışı ya da yasa dışı olarak; kişisel verilerin tahrip edilmesine, kaybolmasına, iletilmesine, değiştirilmesine, depolanmasına veya başka bir ortama kaydedilmesine, işlenmesine, ifşa edilmesine ve söz konusu verilere erişilmesine neden olan güvenlik ihlâli" olarak tanımlanmıştır [13]. Tanımdan da görüldüğü üzere, kişisel verilerin ihlâlinin gerçekleşmesi için kasıt şart değildir; istem dışı kişisel verilerin silinmesi, kaybolması, tahrip edilmesi ve benzeri sonuçlar meydana gelirse yine kişisel verilerin ihlâl edildiği sonucuna ulaşılacaktır. Elektronik haberleşme sektöründe hizmet veren tüm kuruluşların kişisel verilerin işlenmesi ve saklanması konusunda titiz çalışmalar yürütmesi önem teşkil etmektedir. Bu konuda gerekli stratejileri ve politikaları belirlemeli, aynı zamanda veri güvenliğini teknik açıdan da sağlamak için fiziksel ve teknik güvenliğe de önem vermelidir.

Kişisel verilerin işlenmesi kavramı, KVKK'da yapılan tanımla paralel düzenlenmiştir. Bu kapsamda, "Kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi, tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen işlem ya da işlemler bütünü" kişisel verilerin işlenmesi olarak hüküm altına alınmıştır [13]. Yukarıda kişisel verilerin işlenmesi kavramı için yapmış olduğum açıklamalar, bu kısım için de geçerli olacaktır.
Veri kavramı da "*Abone ya da kullanıcıyı teşhis etmek için yararlanılan trafik verisi, konum verisi ya da ilgili diğer bilgiler*" şeklinde tanımlanmıştır [13]. Elektronik haberleşme sektöründeki veriler, kişilerin mobil cihazlarını veya internette yaptığı etylemlerin trafik verisi, konum verisi ya da bunlara benzer ilgili veriler olarak ifade edilmiştir. Bu verilerin de esasen kişisel veri olarak nitelendirilebileceğini söylemek yanlış olmayacaktır. Bu veriklerin de kişilerin mahremiyetini ihlâl edecek şekilde ifşası halinde hukuka aykırı olarak verilerin ifşa edildiğini kabul etmek gerekecektir.

Kişisel verilerin işlenmesine ilişkin ilkeler de Elektronik Haberleşme Sektörüne İlişkin Kişisel Verilerin Korunması Hakkında Yönetmelik'te dördüncü maddede düzenlenmektedir. Bu ilkeler de KVKK'daki kişisel verilerin işlenme ilkeleri ile aynı

şekilde düzenlenmiştir. Yine hukuka ve dürüstlük kurallarına uygun, ilgili kişinin rızası, işlendiği amaç ile ilgili ve ölçülülük prensibi çerçevesinde, gerektiği süre kadar muhafaza edilecek şekilde kişisel veriler işlenmelidir. Yönetmelikte kişisel verilerin yurt dışına çıkarılamayacağı düzenlenmiştir; ancak kişisel verilerin yurt dışına aktarılması şartları KVKK'da hüküm altına alınmıştır. Dolayısıyla, yurt dışına veri aktarılabilmesi için KVKK'da sayılan şartların sağlanması gerekli ve yeterli olacaktır; bu hüküm de güncellenerek yönetmelik ile KVKK arasındaki çelişiyor gibi gözüken bu durum ortadan kaldırılmalıdır.

İlgili kişinin rızasının kapsamı ile ilgili olarak da yönetmelikte bir düzenleme mevcuttur. Buna göre, "Kişisel verilerin işlenmesi kapsamında abone tarafından işletmeciye verilen rıza, sadece alınan hizmete özgü olmak koşuluyla, kişisel verilerin işletmeci tarafından yetkilendirilen taraflar marifetiyle işlenebilmesini de kapsar" [13]. Veri sorumlusu olarak işletmeciler söz konusu iken veri işleyen olarak da işletmecilerin yetkilendireceği taraflar (tüzel kişi veya gerçek kişi olabilir) anlaşılacaktır. Yine veri işleyenlerin eylemleri dolayısıyla kişisel verilerin ihlâli söz konusu olursa, işletmeci de bu durumdan sorumlu olacaktır. İşletmeci, yönetmelik hükümlerinin ihlâl edilmesi de dâhil olmak üzere kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda kullanılmasının temininden işletmeci sorumludur.

İşletmeciler, kişisel verilerin işlenmesine ilişkin olarak güvenlik politikası belirlemekle yükümlü kılınmıştır. Bu güvenlik politikasının içinde Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik'te de bahsedilen imha politikasını belirlemek de dahil olacaktır. İşletmeciler, şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri almak zorundadır ve güvenlik tedbirlerini alırken teknolojik imkânları da göz önünde bulundurarak muhtemel riske uygun bir düzeyde güvenliği sağlamalıdır [13]. İşletmeciler, kişisel verilere sadece yetkili kişiler tarafından erişilebilmesini sağlamalıdır ve erişimi sağlayan uygulamaların güvenliğini sağlamak için de bütün gerekli tedbirleri almak zorundadır [13].

Kişisel veri ihlâlinin gerçekleşmesi durumunda işletmeciler, bu risk hakkında BTK'yı ve BTK tarafından gerekli görülmesi halinde abonelerini/kullanıcılarını etkin ve hızlı bir şekilde bilgilendirmekle yükümlüdür [13]. İşletmecilerin kişisel veri ihlâlini tespit etmeleri hâlinde izleyecekleri prosedürler detaylı olarak yönetmeliğin beşinci maddesinde düzenlenmiştir. Yine aynı yönetmelikte trafik ve konum verilerinin işlenmesi, bu verilerin güvenliğinin sağlanması, sağlanan imkânlar gibi konular da hüküm altına alınmıştır.

İşletmeciler, kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtlarını saklamakla yükümlüdür ve Bilgi Teknolojileri ve İletişim Kurumu'nun gerekli gördüğü hallerde kişisel verilerin saklandığı sistemlere ve alınan güvenlik tedbirlerine ilişkin tüm bilgi ve belgelerini temin etme ve Kurumun söz konusu güvenlik tedbirlerinde değişiklik talep etmesi durumunda bu doğrultuda hareket etmekle mükelleftir [13].

Haberleşme sektöründe kişisel verilerin hukuka uygun olarak işlenmesi bakımından düzenlemeler olsa da biyometrik verilerin işlenmesini belirten ayrıca bir mevzuat bulunmamaktadır, bu konuda KVKK hükümlerine tabiidir. Biyometrik verilerin gelecekteki konumu düşünüldüğü zaman haberleşme sektöründe de önemli bir rolü olacağını kabul etmek gerekir. Biyometrik verilerin işlenmesiyle ilgili ayrıca düzenlemeler yapılmasına ihtiyaç duyulabilir.

3.2.5 Diğer sektörlerde biyometrik verilerin işlenmesi

Biyometrik veriler hayatımızın her alanında kullanılmaktadır. Güvenlik sektöründe biyometrik veriler çok sık kullanılmaktadır. Şifreler veya kilitler kolayca kırılabildiği için biyometrik veriler güvenlik sistemlerinde yer almaktadır. Bazı iş yerlerine giriş ve çıkışlarda çalışanların biyometrik verisi alınmak suretiyle parmak izi ya da retina tarama ile giriş çıkış yapılabilmektedir. Yine aynı şekilde, birçok kişinin yaşadığı rezidans ve site gibi yerlerde kişilerin giriş ve çıkışları da parmak izi okutma, yüz tanıma, iris tarama gibi sistemlerle gerçekleşebilmektedir. Özellikle güvenilirlik açısından yüksek seviyede olduğu için kişişler evlerine ve işlerine kurduracakları güvenlik sistemlerini biyometrik verileri aracılığıyla kullanmayı arzu etmektedir.

Güvenlik sektöründe biyometrik verilerin işlenmesi de KVKK ve ikincil düzenlemelerin hükümlerine tabiidir; ayrıca bir mevzuat düzenlenmemiştir. Parmak izi okuma, yüz tanıma sistemleri, iris tarama, retina tarama, ses tanıma, el geometrisi tanıma sistemleri gibi biyometrik veri sistemlerinin tümü güvenlik sektöründe kullanılmaktadır.

Biyometrik veriler artık pasaportlarımızda, kimliklerimizde, sürücü belgelerimizde de yer almaya başlamıştır. Biyometrik verilere geçiş süreci başlatılmakla birlikte, Türkiye'de biyometrik verilerimizi barındıran kimlik kartları çıkartılmaktadır. Bu kapsamda, kişiler Nüfus Müdürlüğü'ne müracaat ederek kimlik çıkarma işlemi esnasında parmak izleri ve avuç içleri taranmak suretiyle bu biyometrik verilerini vermektedir. 5490 Sayılı Nüfus Hizmetleri Kanunu güncellenerek Kanun kapsamına biyometrik veri kavramı girmiştir. Kanunun üçüncü maddesinin ff bendi uyarınca biyometrik veri "*elektronik sistemler aracılığı ile kimlik tespit ve kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla alınan parmak izi, damar izi ve el ayasından elde edilen kişiye özgü veriler*" olarak tanımlanmıştır [48]. Tanımda genel olarak biyometrik verinin tanımının yapılmasından ziyade "parmak izi, damar izi ve el ayasından elde edilen kişiye özgü veriler" belirtilerek kişilerin kimlik kartları için biyometrik verilerinden bu üç kategorideki verilerinin alınacağı vurgusu yapılmıştır.

Nüfus Hizmetleri Kanunu uyarınca aile kütüklerinde biyometrik veri bulundurma zorunluluğu getirilmiştir. Kanunun kimlik kartını düzenleyen 41. Maddesine göre "*Kimlik kartında yer alacak biyometrik verinin türü, niteliği ve alınma yaşı Bakanlıkça belirlenir [48].*" Sağlık sektöründe biyometrik verilerin paylaşılmasında da yaş sınırları belirlendiğini belirtmiştik. Benzer düzenlemenin burada da söz konusu olduğunu söyleyebilmek mümkün olacaktır. Yine aynı madde uyarınca "*Biyometrik verisi alınacak kişilerin şahsen müracaatı esastır. Biyometrik verisi alınmayacak çocukların kimlik kartı müracaatı veli veya vasileri ile Kanunun ilgili maddelerinde yer alan bildirim yükümlülüğü bulunan kişiler tarafından yapılır [47].*" Son olarak, merkezî veri tabanında tutulan biyometrik veriler kimlik doğrulama işlemleri dışında kullanılamayacaktır; aksi takdirde biyometrik verilerin işlenme amacını ve ölçüsünü aşacaktır.

Kişiler, biyometrik verilerini çeşitli kamu kurum ve kuruluşlarıyla, büyükelçiliklerle paylaşmak durumunda da kalmaktadır. Vize başvurularında kişilerin parmak izi alınabilmektedir. Ya da kişiler sürücü belgelerini almak için ve pasaport başvurularında Emniyet Genel Müdürlüğü tarafından parmak izi alınmaktadır. Bu tür örnekler daha da çoğaltılabilir; ancak unutulmaması gereken husus biyometrik verilerin özel nitelikli kişisel veri olduğunu göz önünde bulundurarak bu verilerin korunması bakımından gereken her türlü teknik ve yasal önlemlerin alınması gerekmektedir.

3.3 Avrupa Birliği'nde Biyometrik Verilerin Korunması

Avrupa Birliği, kişisel verilerin korunması konusunda en titiz çalışan topluluklardan bir tanesidir. GDPR'da da biyometrik verilerin işlenmesine ilişkin hükümler bulunmaktadır.

GDPR 9. Maddede hassas verilerin işlenme ilkeleri yer almaktadır. Biyometrik veriler de hassas veri niteliğinde olduğu için biyometrik verilerin işlenmesi ilkeleri hassas nitelikteki verilerin işlenmesi şartına bağlıdır. Bu kapsamda, biyometrik verilerin mevzuatta sayılan haller dışında işlenmesi yasaklanmıştır. Mevzuat uyarınca, "*Kişilerin ırk veya etnik kökeni, dini veya felsefi düşünceleri veya sendika üyeliğini ifşa eden veriler, ve genetik verileri, gerçek kişinin kimliğini ortaya çıkartmak amacıyla biyometrik veri, sağlık veya kişinin cinsel hayatına ilişkin verilerin işlenmesi yasaktır*" [14].

Rızanın geçerliliğinin Avrupa Birliği mevzuatı ya da ulusal mevzuat uyarınca yasaklanmamış olduğu hallerde, kişinin açık rızası olması halinde biyometrik veriler işlenebilir. Açık rıza olmadan hassas nitelikli verilerin işlenmesi için istisnaların çoğu genel ilkelerdeki istisnalarla da paralel olup aşağıdaki durumlarda öngörülmüştür [14]:

- İş Hukuku, veya Sosyal Güvenlik Hukuku kuralları uyarınca, veyahut kollektif sözleşmeler uyarıca verilerin işlenmesi gerekli ise;
- İlgili kişinin (verisi işlenecek olan kişi) rıza vermeye mental veya fiziksel olarak imkânı olmadığı hallerde, verilerin işlenmesi kamu yararı veya kamu sağlığı için gerekli ise;
- İlgili kişi, bir veya birden fazla belirlenmiş amaç için rıza göstermişse,

- Genel kamu sağlığı yararı için gerekli olması durumunda
- Mahkemelerin yargılama sürecinde ve hukuki iddiaların gerektirdiği takdirde, hakların kurulması, yürütülmesi ve kullanılması için zorunlu ise,
- Kişinin işlenecek hassas verisini anonim hale getirmiş olması durumunda açık rızası aranmaz.
- Kamu yararı için veya bilimsel ya da tarihi araştırmaların amaçları uyarınca ya da istatistiksel amaçların gerektirmesi halinde
- Koruyucu hekimlik veya tıbbi hekimlik gereği, çalışanlara sağlık teşhisinde bulunmak, çalışanın çalışma kapasitesini belirleme, sağlık veya sosyal güvenlik hizmetleri temelli nedenler çerçevesinde gereklilik arz ediyor ise biyometrik veriler ilgili kişilerin açık rızası olmaksızın işlenebilir.
- Kendilerine üye olan ya da eskiden üye olmuş kişilerin rızası olmaksızın; üçüncü kişilere ifşa edilmemesi şartıyla, politik, felsefi, dini veya ticaret topluluğu niteliğindeki kâr amacı gütmeyen kuruluşlar amaçları çerçevesinde veri işleyebilirler.
- Sağlık alanı ile ilgili olarak kamu yararını gerektiriyorsa biyometrik veriler işlenebilir. Kamu yararı kavramının kapsamı geniş olup üye ülkelerin ulusal hukukları uyarınca veyahut AB hukuku kuralları uyarınca kamu yararını ilgilendiren durumların vuku bulması durumunda biyometrik veriler kişilerin rızası olmaksızın işlenebilir.

AB'ye üye ülkeler GDPR'de yer alan düzenlemeler çerçevesinde, mevzuata aykırı olmamak koşuluyla, genetik, sağlık veyahut biyometrik verilerin işlenmesine ilişkin olarak birtakım yeni düzenlemeler getirebilir; bu konuları geliştirebilmek amacıyla yeni düzenlemeler ve kısıtlamalar yapabilir. GDPR çerçevesini aşacak surette getirilecek düzenlemeler yasaklanmıştır. Üye ülkelerin yapacakları düzenlemelerin aynı zamanda temel hak ve özgürlüklere aykırı olmaması gerekir.

3.4 Diğer Ülkelerde Özel Nitelikli Verilerin Korunması

Biyometrik veriler, neredeyse dünya genelinde özel ya da hassas nitelikli veri olarak kabul görmektedir. Fransa da kişisel verilerin korunmasında çeşitli düzenlemeler yapmıştır ve hassas veriler arasından da en çok sağlık verilerinin korunmasına önem vermiştir. Fransa'da kişisel verilerin korunması için Veri Koruma Komisyonu

(Commission Nationale de l'Informatique et des Libértes – CNIL) kurulmuştur. 1978 yılında kişisel verilerin korunması amacıyla düzenlemeler ilk kez yapılmaya başlanmıştır. Günümüze kadar ulaşan bu yasa, Kişisel Verilerin Korunması Yasası'dır (Loi Informatique et Libértes - LIL). Kişisel Verilerin Korunması Yasası'nda sağlık verisine ilişkin herhangi bir tanım yapılmamıştır. Veri Koruma Komisyonu olarak görev yapan CNIL ise sağlık verilerini genel hatları ile "*insan doğasına ilişkin herhangi bir hastalığın, özrün, eksikliğin teşhisine ilişkin veriler*" olarak tanımlamaktadır [49].

Fransa'da sağlık verilerinin yasada düzenlenen istisnalar dışında işlenmesi yasaktır. Bu istisnalardan ilki, ilgili kişilerin "açık rızasıdır". Açık rıza kavramı, hangi ülkede olursa olsun kişisel verilerin işlenmesi için temel kuraldır. Kişilerin açık rızası ile sağlık verileri işlenebilir. Yine sağlık verileri koruyucu hekimlik, tıbbi teşhis, sağlık bakım veya tedavisinin sağlanması veya bir tıp mesleğinin bir üyesi tarafından gerçekleştirilen sağlık hizmetlerinin sürdürülmesi için gerekli ise; Ulusal İstatistik ve Ekonomik Araştırmalar Enstitüsü (INSEE) tarafından yapılan istatistiksel işlemler veya tıbbi araştırmalar bakımından sağlık verileri işlenebilir [49].

Veri sorumluları, sağlık verileri, genetik ve biyometrik verileri, kişilerin tespit edilmesine ilişkin (sosyal güvenlik numarası, kimlik numarası gibi bilgiler) veya işlemek için CNIL ve Devlet tarafından yetkilendirilmelidir. CNIL, Haziran 2016'da veri sorumlularına ilişkin yeni AB düzenlemeleri hakkında kişilerin uygulamada zorluk yaşamamaları ve çeşitli sektörde çalışan kişilerin de görüşlerini almak için aşağıdaki dört konuyu kamuoyu görüşüne sunmuşlardır [50]:

- Yüksek risk kavramının içeriği, Veri Koruma Etki Değerlemesi (Data Protection Impact Assessment - DPIA)
- Yeni haklar
- Sertifikasyon, veri sorumlusu

Alınan görüşler doğrultusunda özetleri içeren yayını CNIL Mart 2017 tarihinde yayımlayarak vatandaşların bilgisine sunmuştur [50].

Hollanda'da da "Kişisel Verilerin Korunması Yasası" vardır. Kişisel verilerin korunmasına ilişkin Kişisel Verileri Koruma Kurumu (Autoriteit Persoonsgegevens - AP) kurulmuştur.Hollanda'da şirketlerin kişisel veri regülasyonları uyum sürecinde zorluk yaşamamaları için Kurum kendilerine telefonla veya e-posta aracılığı ile yöneltilen soruların tümünü cevaplamaktadır [50]. GDPR hükümleri en güncel haliyle üye ülkelerden biri olan Hollanda'da yürürlüğe girerek uygulanmaya devam edilecektir. Hollanda'nın ayrıca "İhlal Bildirimi Kanunu (Breach Notification Law)" mevcuttur. Bu Kanun'da GDPR ile aynı hükümler yer almakla birlikte verilerin işlenmesi ihlal durumlarında izlenecek prosedürleri düzenlemektedir [50].

Amerika'da derli toplu bir düzenlemeden ziyade sektörler ve eyaletler tarafından kişisel verilerin korunması amacıyla düzenlenmiş farklı yasalar, rehber ilkeler vb. düzenlemelerin olduğunu belirtmiştik. Temmuz 2017'den itibaren yazılımların kamuya açık yerlerde kişilerin görüntülerini rızaları olmaksızın alınması ve kişileri tanımlayabilmesi yasal hale gelmiştir. Illinois ve Chicago'da kişilerden alınan görüntülerin ticari amaçlı kullanılması yasaklanmıştır [50].

Haziran 2017'den sonra Washington eyalet biyometrik yasasını yürürlüğe sokan üçüncü şehir olmuştur. Bu düzenleme, ticari toplulukların ticari amaçlarla kişilerin biyometrik verilerini toplamalarına ilişkindir. Temel kural, kişilerin açık rızalarının bulunmasıdır [50]. Washington, biyometrik verilerin hassas nitelikli veri olduğunu ve bu veriyi toplayacak kuruluşların uyması gereken kuralları düzenlemiştir. Ulusal Teknoloji ve Standartlar Enstitüsü biyometrik teknolojilerin değerlendirilmesi bakımından kurulmuştur. Federal Ticaret Komisyonu (Federal Trade Commission) da tüketicilerin kişisel verileri bakımından ilkeler ve kurallar getirmiştir. Sağlık ve İnsan Hizmetleri Departmanı (Health and Human Services Department) da sağlık verilerinin işlenmesi bakımından Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (Health Insurance Portability and Accountability Act) çıkartmıştır. Amerika, biyometrik verilerin işlenmesi hususuna son derece önem vermektedir ve bu konuda çalışmalar yürütmektedir [50].

4. KİŞİSEL VE BİYOMETRİK VERİLERİN İŞLENMESİNE YÖNELİK SAHA ARAŞTIRMASI

Tez kapsamında kişisel ve biyometrik veriler hakkında yasal düzenlemeler ve bunların hukuki ve teknik korunması bakımından yöntemler, uygulamadaki hâli incelendi. Bu kapsamda, getirilecek önerilere zemin hazırlamak üzere bir anket hazırlanmıştır.

4.1 Yöntem

Anketin hedef grubu olarak öncelikle veri sorumluları belirlenmişti. Ancak; veri sorumluları kadar ilgili kişilerin de bu konuya ilişkin görüşlerini ve kişisel verilerin önemi ve düzenlemeleri ile ilgili ne kadar bilgi sahibi olduklarını ölçmek adına karma olarak hem ilgili kişilere; hem de veri sorumlularına yönelik bir anket oluşturuldu. Çeşitli sektörlerde çalışılan kişilere kişisel veriler ve biyometrik verilere ilişkin sorular yöneltildi. Kişilerin de görüşleri alınarak tezin ana sorularından birisi olan "Biyometrik verilerin ideal olarak işlenmesi mümkün müdür?" sorusuna cevap aranmaya çalışılmıştır.

Anket, Bölüm 0, Bölüm 1, Bölüm 2 ve Bölüm 3 olmak üzere 4 kısımdan oluşmaktadır. Ankete başlamadan önce giriş kısmına kişisel verilerin ve biyometrik verilerin sahip olduğu önem, anketin içeriği, ve amacı vurgulanmıştır. Bu verilerin hayatımızda çok önemli bir yer kapladığı, ekonomik ve sosyal hayatı büyük derecede etkileyen veriler olduğu hakkında açıklamalar yapılmıştır.

Sorular, genel olarak kişilerin eğer haberdar değiller ise kişisel verilerinin öneminden haberdar olmalarını sağlamak ve verileri güvenli işlenmiyor ise niye güvenli işlenmediğine yönelik sorular yöneltilmesi amacıyla oluşturulmuştur. Anket sonucunda verilerin güvenle işlenmesi ihlâline sebep olabilecek durumlar ve kişisel verilerin işlenmesine ilişkin kişilerin görüşleri alınmış; daha sonra bu konuya ilişkin öneriler oluşturulmuştur. Anketten elde edilen veriler sonucunda çıktı olarak

biyometrik verilerin korunmasına yönelik sahadaki açıklıkların giderilmesi hedeflenmiştir.

Bölüm 0'da ankete katılan kişilerin ("katılımcılar") hangi yaş grubunda olduğu, cinsiyeti, öğrenim durumu gibi onları tanımak amaçlı sorular sorulmuştur. Anketi çözen kişi ilgili kişi ise hangi sektörde çalıştığı; veri sorumlusu ya da çalıştığı yerde kişisel verilerin işlenmesi için çalışmalar yürüten kişi ise çalıştığı firmayı tanıma amaçlı sorular yer almıştır. Kuruluşların türü (özel-kamu vb.), kuruluşların kaç kişiyi bünyesinde barındırdığı gibi tanıma soruları yöneltilmiştir.

Bölüm 1'de katılımcılara farkındalık soruları sorulmuştur. Bu çerçevede, katılımcıların kişisel ve biyometrik verilerin işlenmesine ilişkin farkındalık derecelerinin ölçülmesi hedeflenmiştir. Ek olarak, katılımcıların kişisel verilerin korunmasına ilişkin mevzuattan haberdar olup olmadıkları ölçülerek eğer haberdar iseler mevzuatta herhangi bir eksiklik görüyorlarsa konuya ilişkin önerilerini dile getirmeleri sağlanmıştır.

Bölüm 2'de güvenlik ile ilgili sorular yöneltilmiştir. Katrılımcıların çalıştıkları kuruluşta bilgi güvenliğini sağlamak amacıyla ne tür güvenlik ürünleri kullandıkları, veri ihlâlinin yaşanıp yaşanmadığı, yaşanıyor ise ne sıklıkta yaşandığı gibi sorular bu bölümde yer almıştır. Veri ihlâli olması durumunda olay öncesi ve sonrası ne yapıldığına dair katılımcılardan bilgi toplamak hedeflenmiştir.

Bölüm 3'te ise biyometrik verilerin kullanımı, bu konuya yönelik yürütülen çalışmalar ve önerileri toplamak amaçlanmıştır. Yapılacak ikincil düzenlemelere ilişkin olarak:

- Katılımcılar veri işlemekten sorumlu ise bu konuda ne yapmayı düşündükleri, ne tür politikalar izleyecekleri;
- Katılımcılar ilgili kişi ise hangi konuda (Verilerin işlenmesi, silinmesi, aydınlatma yükümlülüğü vb.) mevzuatta eksiklik gördükleri sorulmuştur.

Sorular, genel itibariyle iki kategoride toplanmıştır:

- Teknik Dönüşüm: "Veri güvenliği için ne yapıyorlar, ne kullanıyorlar? Güvenlik ürünü olarak ne kullanılıyor? Fiziksel bağlamda ne tür önlemler alınıyor?" gibi sorular yöneltilmiştir.

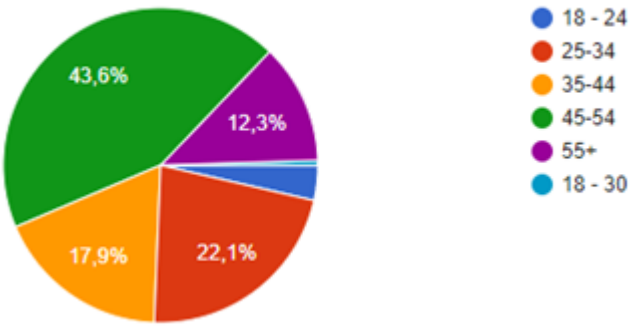
- Kültürel Dönüşüm: Kanun düzenlemeleri hakkında uyum süreci ne şekilde gerçekleşiyor gibi konulara ilişkin bilgilerin toplanması amaçlanmıştır.

4.2 Bulgular

Anket, 18 Eylül 2017 tarihinde oluşturulmuştur. Ankete katılım ise 1 Kasım 2017 tarihi itibariyle sona erdirilmiştir. Çeşitli sektörlerdeki ilgili kişi ve veri sorumluları olan kişilere gönderilmiştir; toplam yüz doksan beş kişi ile ankete katılım gerçekleşmiştir. Bulgular başlığı altında anket sonuçları, yoruma dayalı olan sorular bakımından verilen yanıtlar irdelenmektedir. Anketten sağlanan kazanımlarla uygulamaya ilişkin önerilere ve değerlendirmelere de esas olarak sonuç başlığı altında yer verilecektir.

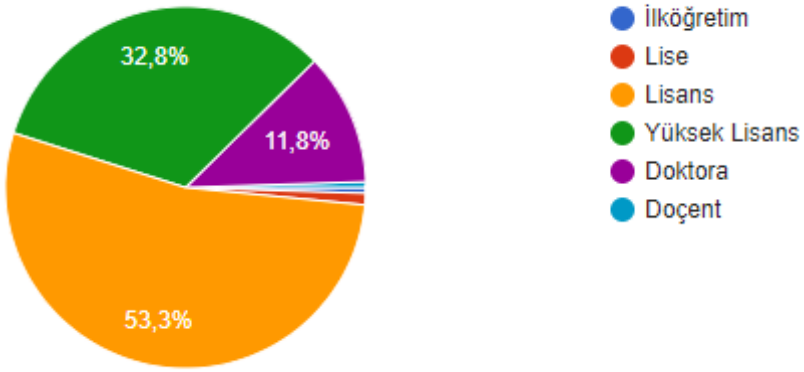
Bölüm 0'da katılımcıları tanımak amaçlı sorular yöneltilmiştir. Bu çerçevede, anketi cevaplayan 195 kişinin:

- % 4.1'i 18-24;
- % 22.1'i 25-34;
- % 17.9'u 35-44;
- % 43.6'sı 45-54
- % 12.3'ü 55 yaş ve üzeridir.



Şekil 4.1: Yaş Dağılımı

Ankete katılanların % 58.2'si kadın olup % 41.8'i ise erkektir. Öğrenim durumu olarak; 0.5'i ilköğretim, %1.6'sı lise, %53.3'ü lisans, %32.8'i yüksek lisans, % 11.8'i ise doktora-doçent olarak yanıtlanmıştır.

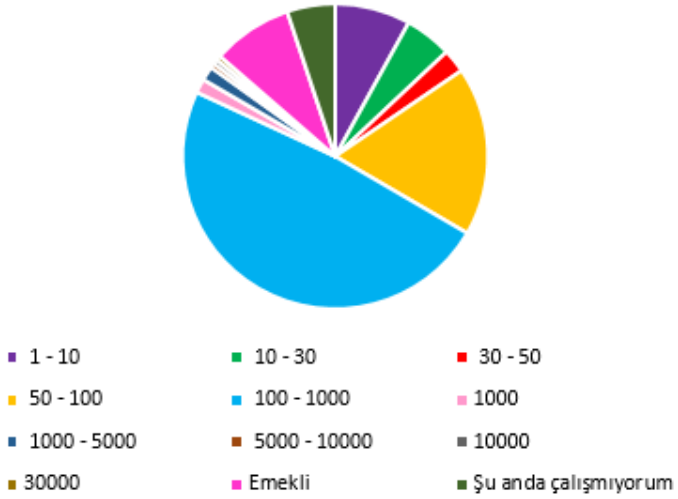


Şekil 4.2: Öğrenim Durumu

ÖN Anketi çözenlerin çalışıyorlar ise çalıştıkları Kuruluşun bünyesinde kaç kişinin istihdam ettiğine ilişkin soru yöneltilmiştir. Bu kapsamda,

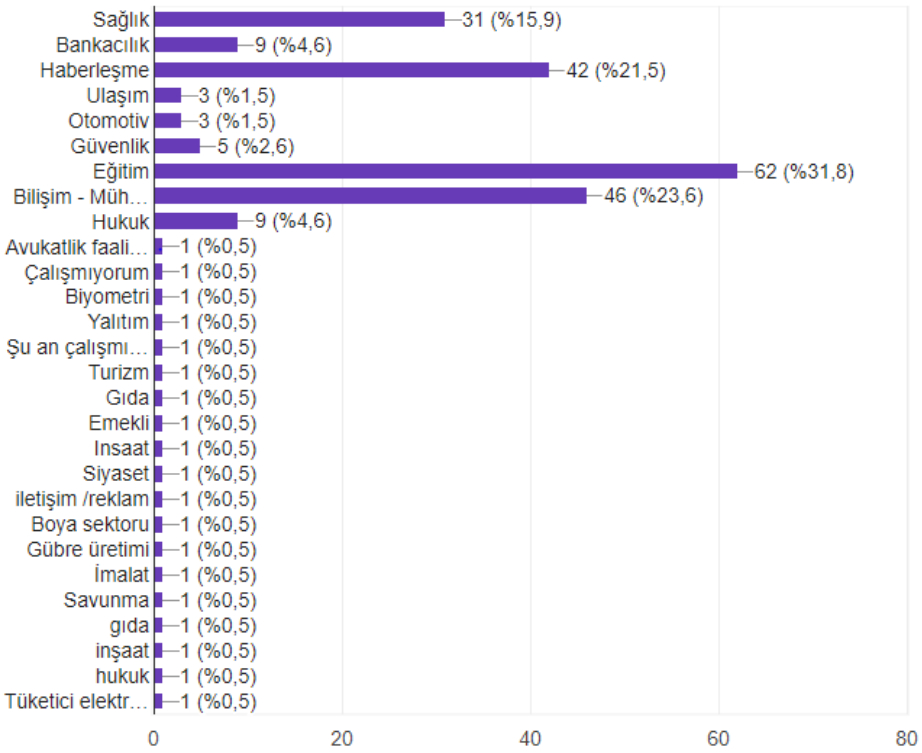
- 1-10 arası %8;
- 10 – 30 arası %5;
- 30 – 50 arası % 2.5;
- 50 – 100 arası %17.9;
- 100 – 1000 arası %48.5;
- 1000 kişi %1.5;
- 1000 – 5000 arası %1.5;
- 5000 – 10000 arası %0.5;
- 10000 kişi %0.5;
- 30000 kişi %0.5
- Emekli olduğunu belirten %8.5;
- Şu anda çalışmadığını belirten %5.1

olarak belirtilmiştir.



Şekil 4.3: İstihdam Durumu

Katılımcıları tanıma amaçlı olarak kişilerin hangi sektörde çalıştığına ilişkin sorular da yöneltilmiştir. Bu kapsamda, anketi yirmi altı farklı sektörden kişi çözmüştür. Eğitimden sağlığa, tüketici elektroniğine; haberleşme- bilişim sektörüne kadar geniş yelpazede faaliyet gösteren kişiler ankete katılım göstermiştir. Ayrıca birden fazla sektörde faaliyet gösteren kişiler var ise bunlar için birden fazla seçenek işaretleme imkânı tanınmıştır. Kişilerin faaliyet göstermiş olduğu sektörler Şekil 4.4 çerçevesinde gösterilmiştir.



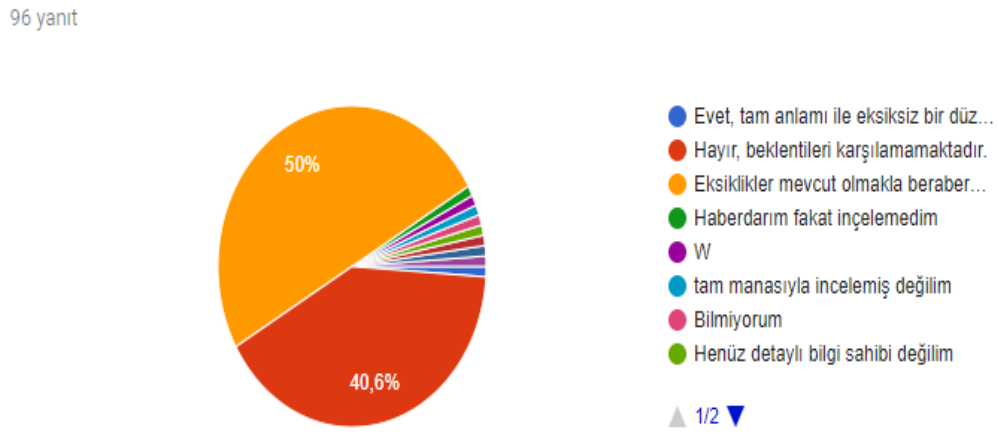
Şekil 4.4: Ankete katılanların faaliyet gösterdiği sektörler

Ankete henüz çalışmayan veya emekli olmuş kişilerle beraber yirmi altı sektörden cevap gelmiştir. Katılımcıların çoğunluğu sırasıyla bilişim – haberleşme - mühendislik, eğitim, sağlık, hukuk, bankacılık, güvenlik vb. sektörlerden oluşmuştur.

Katılımcıların farkındalığını ölçmek amacıyla oluşturulan Bölüm 1'de yer alan ilk soru, KVKK hakkında katılımcıların herhangi bir bilgisi olup olmadığını ölçmeye yöneliktir. Bu kapsamda; kişilerin %59.3'ü düzenlemeyi duyduklarını ancak içeriğini bilmediklerini, %17.5'i düzenlemeyi duymadığını ve içerik hakkında herhangi bir bilgileri bulunmadığını; %23.2'si ise düzenlemeyi duyduğunu ve içeriğini yeterince bildiklerini ifade etmiştir. Burada vurgulanması gereken husus, %76.8 oranı gibi yüksek oranda katılımcının kişisel verilere ilişkin mevzuat içeriğini bilmediklerini ifade etmeleridir. Kişisel veriler, kişisel verileri işleyen veri sorumluları kadar verisi işlenen ilgili kişileri de ilgilendirmektedir. İlgili kişilerin bu konuya dair farkındalığı ve bilgileri arttıkça kişisel verilerinin hukuka uygun işlenip işlenmediğini ayırt edebilmeleri ve kişisel verilerini kolayca paylaşmamaları sağlanabilir. Kişiler sorgusuz sualsiz kimlik numaralarına kadar kişisel verilerini kolaylıkla paylaşabilmektedir ve farkındalık meselesi de yasal düzenlemeler ve bilgi güvenliğini sağlamaya yönelik önlemler kadar önem arz etmektedir.

Mevzuattan haberdar olanlar için KVKK'da yer alan düzenlemelerin beklentilerini karşılama derecesi sorulmuştur. Bu kapsamda, 195 kişiden 96 tanesi bu soruya ilişkin görüşlerini bildirmiştir.

- Bu kişilerden %50'si "Eksiklikler mevcut olmakla beraber, beklentileri karşılamaktadır." yanıtını vermiştir.
- %1'i KVKK düzenlemelerinin tam anlamı ile eksiksiz olduğunu, beklentileri karşıladığını ifade etmiştir.
- %40.6'sı beklentileri karşılamadığını belirtmektedir.
- %8.4'ü ise KVKK düzenlemesinden haberdar olmakla birlikte Kanunu tam anlamıyla inceleyemediğini, içeriğini kapsamlı bilmediğini, detaylı bilgi sahibi olmadığını belirterek çekimser kalmıştır.

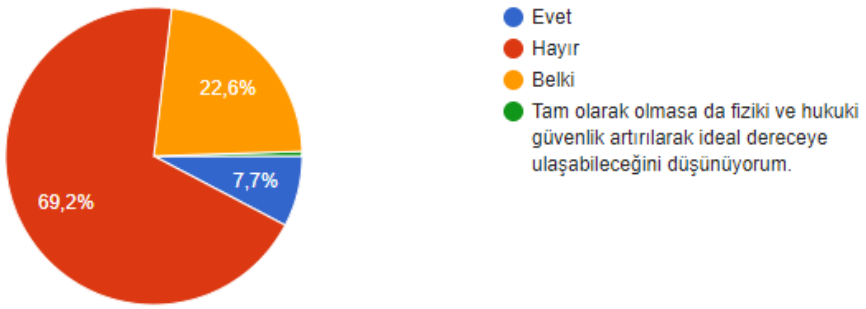


Şekil 4.5: KVKK'ya ilişkin görüşler

Bölüm 1'de yer alan ikinci soruya göre kişisel verilerin korunmasında "Yalnızca yasal düzenlemenin yeterli olacağını düşünüyor musunuz?" sorusu sorulmuştur. Bu soru ile kişilerin KVKK içeriği hakkında bir bilgisi olmasa dahi görüşlerinin alınması hedeflenmiştir. Bu doğrultuda, yasal düzenlemelerle kişisel verilerin korunması konusunda herhangi bir caydırıcılık sağlanabilir mi, yasal düzenleme yeterli görülebilir mi sorularına ilişkin katılımcıların görüşleri alınmıştır. Sonuç olarak, 195 kişinin %7.7'si "evet" diyerek kişisel verilerin korunmasında yasal düzenlemelerin yeterli olacağını ifade etmektedir. Kişilerin %22.6'sı ise "belki" diyerek yasal düzenlemelerin kişisel verilerin korunmasında azımsanmayacak bir rolü olduğunu düşünmektedir. %69.2 oranında ise "hayır" cevabı çıkmıştır; yani anketi çözen kişilerin büyük bir çoğunluğu kişisel verilerin korunması açısından sadece yasal düzenlemelerin yeterli olmayacağını vurgulamaktadır. %0.5'lik ufak bir kesim de "tam olarak olmasa da fiziki ve hukuki güvenlik artırılarak ideal dereceye ulaşılabileceğini düşünüyorum" yorumunu yapmıştır.

Yasal düzenlemelerin kişisel verilerin hukuka uygun olarak işlenebilmesi için ilkeler, şartlar düzenlemesi bu konuda genel bir çerçeve çizilmesine yardımcı olmaktadır. Yasalar uyarınca ağır yaptırımlar öngörülmesi de hukuki düzenlemelere caydırıcı nitelik kazandırabilecektir. Yasal düzenlemelerin sağladığı korumanın önemi, kişisel verilerin yurt dışına aktarılması bakımından da söz konusu olmaktadır. Sadece Türkiye'de değil; gerek AB'de gerek diğer Avrupa ülkelerinde kişisel verilerin başka bir ülkeye aktarılabilmesi için verilerin aktarılacağı ülkenin sağladığı yasal koruma

öncelikle değerlendirilmektedir. Yasal korumalar kadar bilgi güvenliğini sağlamaya yönelik alınacak teknik önlemler de önemlidir. Verilerin tutulduğu sistem ne kadar korunaklı ise verilerin gizliliği ve bütünlüğü de bu suretle sağlanabilecek ve yetkisiz kişiler tarafından bu verilere erişilmesi engellenebilecektir. Yasal düzenlemeler ve fiziki güvenliğin (hem fiziki hem teknik önlemler) sağlanması için gerekli önlemlerin alınması ile hem asgari düzeyde kişisel veri ihlâlleri yaşanacağı hem de maksimum düzeyde korumanın sağlanabileceği yorumunu yapmak yerinde olacaktır.



Şekil 4.6: Kişisel verilerin korunmasına ilişkin görüşler

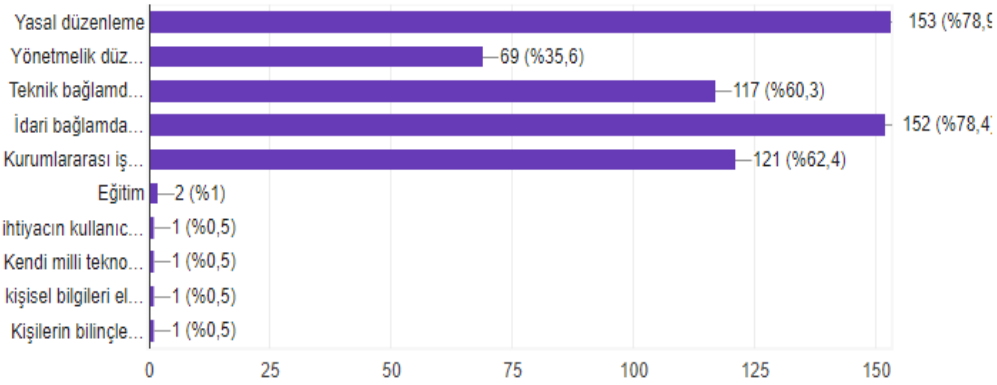
Üçüncü olarak katılımcılara seçenekler sunularak kişisel verilerin korunması için bu seçeneklerden hangisi veya hangilerinin gerekli olduğunu belirtmeleri istenmiştir. Kişiler bu seçeneklerden bir veya birden fazlasını işaretleyebilmektedir.

- Sunulan seçenekler arasından en fazla işaretlenen seçenek "*Yasal Düzenleme*"dir. Katılımcılar, özellikle yasal düzenlemeler aracılığıyla kişisel verilerin korunmasının sağlanabileceğini düşünmektedir. Yasal düzenleme seçeneğini işaretleyen 153 katılımcı bulunmaktadır.
- İkinci sırada ise 152 oyla "*İdari bağlamda hukuki olarak ağır yaptırımlar getirilmesi ve bu kapsamda veri sorumlularının titizlikle çalışması*" gelmektedir. Yine üstteki sonuçla paralel olarak yasal düzenlemeler sonucunda ağır idari yaptırımlar getirilerek caydırıcılık oluşturabileceği düşünülmektedir. Bu ağır yaptırımlar doğrultusunda kişisel verileri işleyecek ve bünyesinde saklayacak olan veri sorumluları ve veri işleyenlerin daha titizlikle kişisel verilerin korunması hususuna yaklaşım sergileyecekleri düşünülmektedir.
- Üçüncü sırada, 121 oyla "*Kurumlararası işbirliği ile politikalar benimsenmesi ve kişisel verilerin korunması hususunda yeknesaklık sağlanması*" yer

almaktadır. Kişisel verilerin korunmasına ilişkin kurumlararası işbirliği sağlanarak çeşitli politikalar benimsenmesinin önemi, uygulamada oluşabilecek çelişkiler, boşlukların giderilmesi açısından önemi göz ardı edilemeyecektir.

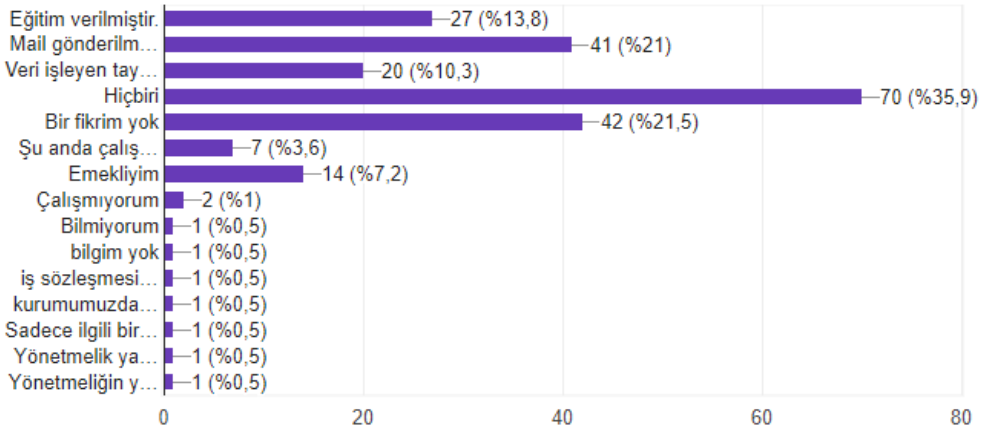
- Dördüncü sırada da 117 oyla "*Teknik bağlamda fiziksel güvenliğin sağlanması*" seçilmiştir. Yasal düzenlemelerle kişisel verilerin hukuka aykırı bir biçimde işlenmesinin önüne geçilmek istense de, teknik önlemlerin de alınması önem arz etmektedir. Teknik önlemlerle yetkisiz kişilerin bu verilere erişebilmesi, değiştirilmesi, silinmesi önlenebilir.
- Beşinci sırada 69 oyla "*Yönetmelik düzenlenmesi*" vardır. İkincil düzenlemeler, Kanun'da tanımı yer alan kavramların daha ayrıntılı düzenlenmesi suretiyle kurallar ortaya koyar; bu bakımdan da her ne kadar hiyerarşik olarak Kanun ile eşdeğer olmasa da en az Kanun kadar önemli düzenlemeler içermektedir. Kanun ile detaylı düzenlenemeyen, soru işareti bırakan hususlar Yönetmelikler ile düzenlenmek suretiyle uygulamadaki sorunları giderebilir.
- Altıncı sırada ise 2 oyla "*Eğitim*" yer almaktadır. Eğitim, aslında bilinçlendirmenin temel faktörlerinden birisi olup; en az yasal ve teknik önlemler kadar önem teşkil etmektedir. Ancak diğer hususlar daha çok katılımcılar tarafından tercih edilmiştir ve altıncı sırada yerini almıştır.
- *Diğer*" şıkkı ile kişilerin başkaca önerileri varsa bunu belirtmeleri imkânı verilmiştir; bu kapsamda da 4 kişi teker teker farklı önerilerini sunmuşlardır. İlk öneri "*ihtiyacın kullanıcılar tarafından benimsenmesi*"dir. Yani, kişisel verilerin korunmasının önemi kişiler tarafından (gerek ilgili kişiler gerek veri sorumluları) benimsenmelidir ki buna göre kişisel verilerin korunması için stratejiler, ilkeler, politikalar geliştirebilir ve korumak için titiz çalışmalar yürütebilir. İkinci öneri, "*Kendi milli teknolojimizi üretmemizin gerekli olduğu*" olarak yer almıştır. Tezin öneriler kısmında da değinilecek bu husus, özellikle yabancı ülkelerde de zaruri olarak kişisel verilerimizi ilettiğimiz ve yabancı ülkelerde de kişisel verilerimizin saklandığı durumlar olduğu için bunun önüne geçebilmek açısından gerekli görülmeltedir. Öncelikle kendi milli teknolojimizi üreterek bu sistemler aracılığı ile güvenli olarak milli sınırlar içerisinde kişisel verilerimizin tutulmasını sağlayarak daha sonra

korunmasına yönelik yasal düzenlemelere ağırlık verilebilecektir. Üçüncü öneri "*kişisel bilgileri ele geçirip kendi amaçları doğrultusunda işleyen ve fayda görenlerin cezalandırılması*"dır. Bu öneri de yasal düzenlemlerin caydırıcılığı görüşü ile örtüşmektedir. Son olarak ise "*Kişilerin bilinçlendirilmesi, kişisel verisinin kıymetini bilmesi ve koruması*" önerisi yer almaktadır. Bu öneri de eğitim unsuru ile örtüşen bir görüştür. Kişiler bilinçlendirilmek suretiyle kişisel verilerini paylaşırken daha dikkatli olacaklar, daha sorgulayıcı bir noktaya ulaşabileceklerdir. Sonuçlar Şekil 4.7'de yer almaktadır:



Şekil 4.7: Görüşler – I

Bölüm 1'de yer alan beşinci soru ise "*Kurumunuzda Kişisel verilerin korunması mevzuatına uyum sağlamak için hangi çalışmalar yapılmaktadır?*" olarak yer almıştır. Bu soru kapsamında da katılımcılara birden fazla seçenek işareyetlebilme imkânı sunulmuştur. Sonuçlar Şekil 4.8'de yer almaktadır:



Şekil 4.8: Kuruluşların uyum sürecine ilişkin yürüttükleri çalışmalar

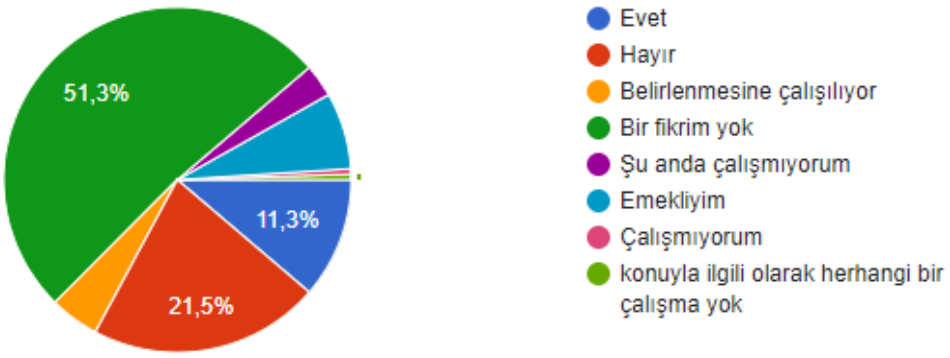
Şekil 4.8'deki sonuçları değerlendirmek gerekirse, ilk değinilmesi önem arz eden husus, katılımcıların büyük bir çoğunluğunun hiçbir çalışma yürütülmediğini ifade etmesidir. 70 oyla "Hiçbiri" seçeneği en fazla işaretlenen seçenek olmuştur. İkinci sırada 42 oyla "Bir fikrim yok" işaretlenmiştir. Bu şıkka ek olarak "Kurumumuzdaki ilgili başkanlığın çalışmaları hakkında detaylı bir bilgim yok; bilgim yok; bilmiyorum" ifadelerini dile getiren 3 tane daha katılımcı vardır. Bu geri dönüşlerin de değerlendirilmesiyle birbirine yakın cevaplar olmaları sebebiyle aslında toplamda 45 kişinin bu konuya ilişkin bir fikri bulunmadığını söylemek doğru olacaktır. En çok oy alan ilk iki sırada yer alan seçenekler incelendiği zaman kişisel verilerin korunması bakımından KVKK'ya geçiş sürecinde henüz Kuruluşlar ve ilgili kişilerin de bilinçlendirilmesi nezdinde hazır olunmadığı yorumu yapılabilir. Bilinçlendirmenin önemi, bu noktada da karşımıza çıkmaktadır. Bazı Kuruluşlar hazırlıklarını tamamlamış olsa da, henüz hazır olmayan Kuruluşların da gerekli önlemleri alması ve hazırlıkları yapması gerekmektedir.

Üçüncü sırada 41 oyla "Mail gönderilmek suretiyle vb. bilgilendirme yapılmıştır." yer almıştır. Çeşitli Kuruluşların çalışanlarına mail atmak suretiyle kişisel verilerin korunması çalışmalarına ilişkin çalışanlarını bilinçlendirme ve bilgilendirme yoluna gidildiği bu suretle görülebilmektedir. 20 oyla dördüncü sırada "Veri işleyen tayin edilerek kişisel verileri korumak için gereken stratejiler belirlenmiştir" cevabı yer almaktadır. Burada da hazırlıkları tamamlama noktasına gelen, kişisel verilerin korunması uyum sürecinde gerekli çalışmaları yürüten Kuruluşların da olduğu çıkarımı yapılmaktadır.

"*Diğer*" şıkkını işaretleyen beş kişi ise uyum sürecine ilişkin yürütülen çalışmalara seçeneklerde yer almayan ancak yapılan çalışmaları eklemişlerdir. Bunlardan ilki, " iş sözleşmesi güncellemesi, veri temsilcisi ataması, her sözleşmeye ek protokol ile ilgili hükümlerin eklenmesi"dir. Kuruluşlardan bir tanesinin sözleşmelerini revize etmek ve veri sorumlusu ve işleyen atamak suretiyle uyum sürecinde gerekli adımları attığı bu çalışma ile görülmektedir. "Sadece ilgili birim içerisinde tedbir alındığını sanıyorum" diğer yanıtlardan bir tanesidir. Bu çerçevede de ilgili birimlerin kendi içerilerinde ilgili çalışmaları yürüttükleri; ancak Kuruluşun genelinin henüz bu konuda bilgi sahibi olmadığı anlaşılmaktadır. Son olarak "*Yönetmeliğin yayınlanması beklenmektedir – Yönetmelik yayınlanmıştır*" cevapları verilmiştir. Anketin hazırlanma süreci ve

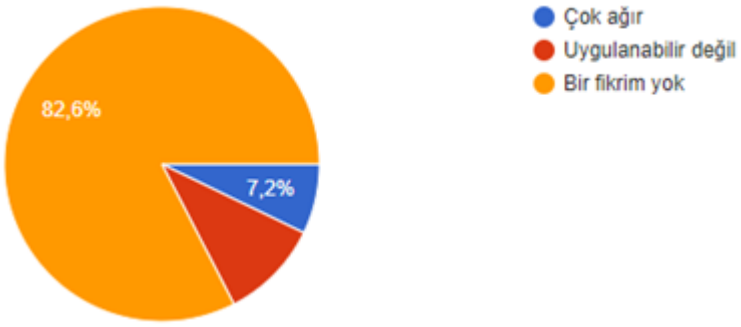
cevaplara açılma tarihi Eylül ortalarına denk geldiği için henüz 28 Ekim 2017 tarihinde Resmi Gazete'de yayımlanan "Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hâle Getirilmesi Hakkında Yönetmelik" yoktu. Dolayısıyla çıkarılması beklenen Yönetmeliklerden bir tanesi olması sebebiyle katılımcılardan bir tanesi Yönetmeliğin yayımlandığını belirtirken; diğer bir katılımcı da gerekli önlemlerin alınabilmesi ve çalışmaların yürütülebilmesi için ilgili Yönetmeliklerin çıkmasını beklediklerini ifade etmiştir.

Altıncı soru olarak, "*Mevzuata uyum süreci kapsamında, kurumunuzda veri sorumlusu (veri sorumlusu, kişisel verilerin işlenme araçlarını ve amaçlarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumludur ve gerçek veya tüzel kişi olabilirler) ve veri işleyen (veri sorumlusunun verdiği yetki ile kişilerin kişisel verilerini işleyecek gerçek kişi veya tüzel kişi/ler) belirlenebildi mi?"* sorusu katılımcılara yöneltilmiştir. Yanıtların %51.3'ü "*bir fikrim yok*"; %21.5'i "*hayır*"; %4.6'sı "*belirlenmesine çalışılıyor*"; %11.3'ü "evet" olarak yer almıştır. 1 kişi de "konuyla ilgili herhangi bir çalışma yok" yazmıştır; bu cevap da hayır olarak değerlendirilebileceği için hayır cevabına verilen oran %22 olacaktır. Diğer kalanlar ise emekli oldukları veya çalışmadıkları için bu soruya herhangi bir yanıt veremeyeceklerini belirtmiştir.



Şekil 4.9: Veri sorumlusu ve/ya işleyen atama

Yedinci soru kapsamında, katılımcılara mevzuat uyarınca veri sorumlularının yükümlülüklerini nasıl değerlendirdikleri sorusu yöneltilmiştir. Bu kapsamda, %82.6 oranında "*Bir fikrim yok*"; %10.3 oranında "*Uygulanabilir değil*"; %7.2 oranında da "*Çok ağır*" yanıtları verilmiştir. Yanıtlar bu şekilde olmakla beraber, uygulanabilir olduğuna ilişkin notlar da iliştirilmiştir.



Şekil 4.10: Görüşler – II

Sekizinci soru olarak "*Yukarıdaki soruya verdiğiniz yanıt "çok ağır" veya "uygulanabilir değil" ise nedenlerini açıklayabilir misiniz?"* sorulmuştur ve bu soru kapsamında 18 adet yanıt gelmiştir. İlgili yanıtlar aşağıda yer almaktadır:

1) "Veri sorumluları verilerin kendi adlarına bir gerçek veya tüzel kişi gtarafından işlenmesi durumunda gerekli tedbirlerin alınması konusunda bu kişilerle beraber müştereken sorumlu olacaklardır. Kişisel verilerle ilgili çeşitli eğitimlerin düzenlenmesi ve Kurum çalışanlarını bilgilendirmek, bilinçlendirmek büyük önem arz etmektedir. Dolayısıyla, veri sorumlularının sadece teknik korumaya yetkili ya da sadece hukuki bilgiye sahip birinin yetkili kılınması durumunda sorunlar oluşabilecektir. Veri sorumlusunun belirleyeceği veri işleyenler hukuki ve teknik bilgiye sahip kişilerden oluşmalıdır ve ağır sorumluluklardan bu şekilde zarar görmeden kişisel veriler işlenmelidir."
2) "Yükümlülükler paylaştırılmalıdır."
3) "Türkiye'de yer alan şirketlerin büyük çoğunluğunda üst yönetim kadrosunun tarzı ve tavrından dolayı veri sorumlusuna verilen sorumlulukların hakkıyla yapılması engellenebilir."
4) "Çok kalabalık ve kapsamlı şirketlerde tüm sorumluluğun bir kişiye yüklenmesi çok ağır."
5) "Bilgiden önce bilinçlenme ve özümseme gerekir. Bu husus yeterince olgunlaşmamıştır."
6) "İş sadece database temizlemekle veya querrylrri filtrelemekle bitmiyor. Bu işi düzgün bir mimarla aşamalandırmak ve yeniden tasarlamak gerekli."

7) "Yasanın kişisel veri korunması ile kullanımı dengesi yok. Koruma sert, bu nedenle uygulanabilir değil. Yarın bu anket bile yasaya aykırı görülebilir."

8) "Bilgi sahibi değilim/Bilgim yok/ Bir fikrim yok şeklinde yanıt veren dört kişi olmuştur."

9) "İdari yapılar liyakat ve sorumluluk üzerine yapılandırılmamıştır."

10) "Beklenti büyük, yükü ağır, kendi işini de yapması beklendiği için zaman yetersiz."

11) "Sorumlu kişinin yeterince bilgisi olduğunu sanmıyorum."

12) "Kişisel sorumluluk değil kurumsal sorumluluk daha uygulanabilir."

13) "Veri ihlâllerinin tespiti konusunda yeterli bir hukuki ve teknik bir altyapı bulunmamaktadır. Sadece şikâyete bağlı olarak kişisel veri koruma mevzuatının uygulanmasının, yeterli koruma sağlayabileceğini düşünmüyorum."

14) "Soru iki uç arasında cevap verilmesine imkan sağlamıyor."

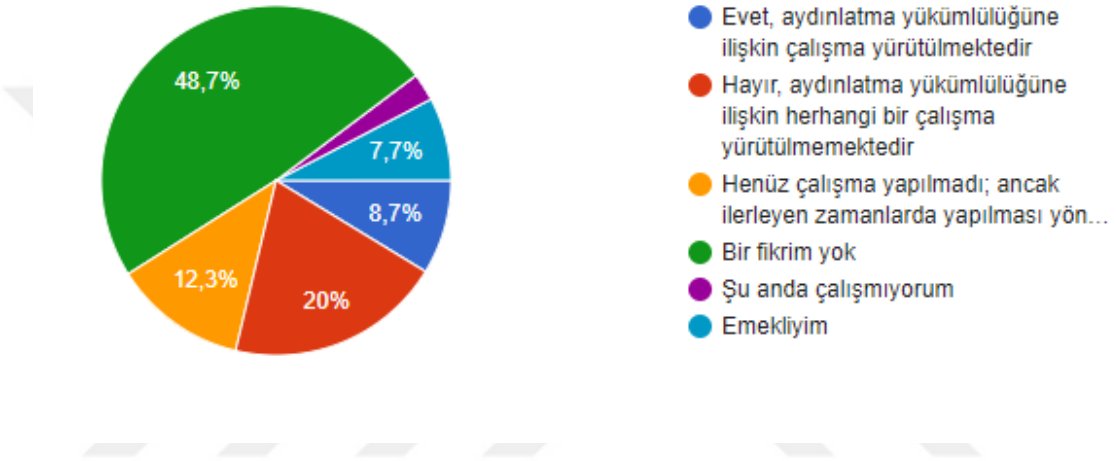
15) "İkincil mevzuatla daha net biçimde tanımlanmadığı sürece görüş bildirmek doğru olmayacaktır."

Dokuzuncu soru olarak kurumlarda veri işleyenlerin ne şekilde belirlenebileceği sorulmuştur. Bu soruya verilen yanıtların büyük bir çoğunluğu %88.2 oran ile "*Hukuk ve Teknik kişilerden oluşan bir grup olmalı*" seçeneğini işaretlemiştir. Bu seçenek dışında %8.2 "*sadece bilgi işlemci olmalı*" seçmiştir. 1 kişi bir fikri olmadığını belirtmiştir. Diğer seçeneğini işaretleyen kalan 6 kişi ise farklı görüşlerini cevap olarak belirtmişlerdir. Buna göre eklenen 6 görüş aşağıdadır:

1) "Hukuk Teknik ve Bilgi İşlem konularında deneyimli kişilerden oluşmalıdır."
2) "Eğitilecek herhangi bir öğrenimi olanlar olabilir."
3) "Mesela bizim hastanede bu işi sadece it departmanına bırakıyorlar fakat bahsedilen data pek çok etik sorunları da beraberinde getirmekte. Bu nedenle etik hukuk bilgi işlem beraber çalışmalı."
4) "Hukuk bilen teknik kişi olmalı."

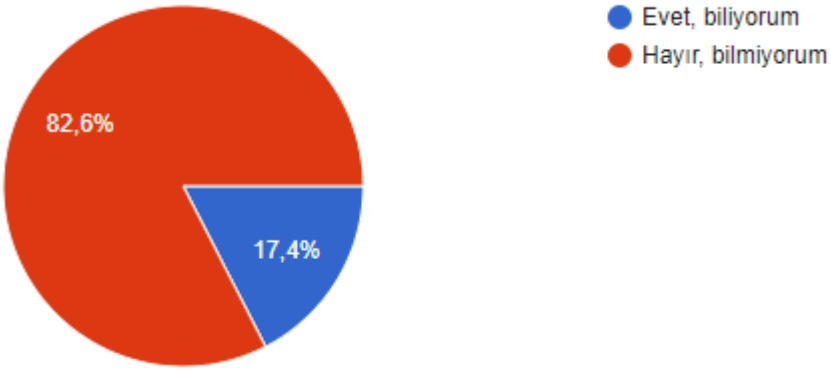
5) “Hukuk teknik ve bilgi işlemci komisyon olabilir.”
6) “Hukuk ve ilgili teknik eğitimlerden geçmiş bilgi işlemciler olmalıdır.”

Onuncu soru olarak “*Veri sorumlusunun ve veri işleyenin kişisel verileri işlenen kişileri (ilgili kişi) aydınlatma yükümlülüğü bulunmaktadır. Bu kapsamda, aydınlatma yükümlülüğü ile ilgili hangi seçenek kuruluşunuzun mevcut uygulamasını en iyi açıklamaktadır?*” yöneltilmiştir. Bu doğrultuda verilen cevaplar Şekil 4.11’de yer aldığı gibidir:



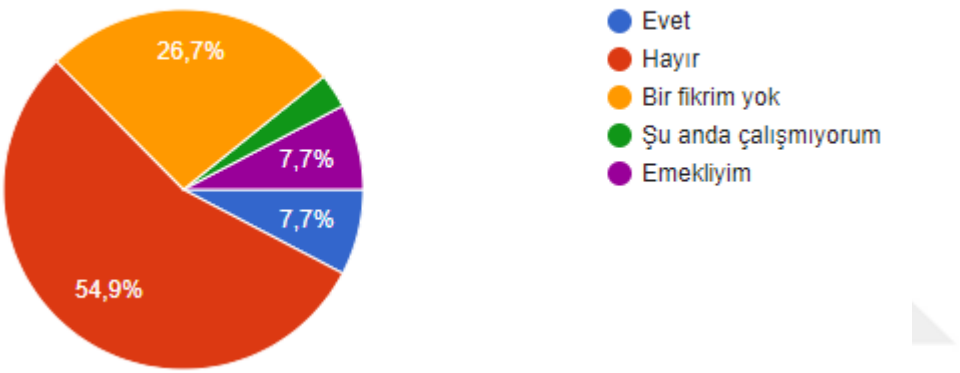
Şekil 4.11: Yürütülen çalışmalar

On birinci soru olarak “*Kişisel verilerinin hukuka aykırı işlenmesi durumunda ilgili kişinin haklarından olan veri sorumlusuna başvuru kavramı ile ilgili bilginiz var mı?*” sorulmuştur. %82.6 “*Hayır, bilmiyorum*” seçeneğini işaretlerken kalan %17.4 ise “*Evet, biliyorum*” seçeneğini işaretlemiştir.



Şekil 4.12: Şikâyet kavramı farkındalık

On ikinci soru olarak "*Kişisel verilerin işlenmesi ile ilgili hukuka aykırı bir durum oluştuğunda veri sorumluları bakımından ağır idari ve mali yaptırımlar söz konusudur. Bu konuda herhangi bir bilgilendirme yapıldı mı?"* sorulmuştur. Bu kapsamda verilen cevaplara göre %26.7 "*Bir fikrim yok*"; %7.7 "*Evet*"; %54.9 "*Hayır*" seçeneğini işaretlemiştir. Sonuç itibariyle, katılımcıların %92.3'ünün veri sorumlularına uygulanan ağır yaptırımdan haberdar olmadıkları çıkarımı yapılabilecektir. Bu sonuçlar, anketin işk kısmında yer alan farkındalık soruları sonuçlarında ortaya çıkan KVKK içeriğinden tam anlamıyla haberdar olmama oranı ile de örtüşmektedir. Kişilerin kişisel verilerin işlenmesi hususunda bilinçlendirilmesinin gerekliliği buradan alınan sonuçlarla da ortaya çıkmaktadır.



Şekil 4.13: Veri sorumluları yaptırımlara ilişkin farkındalık

Bölüm 1'in sonuncu sorusu ise "*Yukarıdaki soruya "Evet" işaretlediyseniz veya konu hakkında bilgi sahibi iseniz, (Yukarıdaki soruya evet dışında işaretleyenler bu soruyu pas geçebilir) kişisel verilerin işlenmesi ile ilgili hukuka aykırı bir durum oluştuğunda öngörülen ağır idari ve mali yaptırımlar hakkında görüşleriniz ve önerileriniz nelerdir?*" olarak yer almıştır. Bu doğrultuda, 21 adet yanıt bulunmaktadır.

1) "Kişisel verilerin korunması önemli bir konudur; dolayısıyla ağır yaptırımların öngörülmesinin bunun doğal bir sonucu olduğunu düşünüyorum. Ancak, veri sorumlularının kişisel veri işleme politikalarını değerlendirerek stratejiler belirlemeli, buna göre kurallar ve ilkeler belirleyerek verileri işlemelidir."
2) "Ağırlaştırılmalı."
3) "Hapis cezası ve para cezası"

4) “Ağır yaptırımların olması güzel ancak bu sürecin yürütülebilmesi için şirketlerin ve kurumların ana sorumluluğu üstleneceği ek cezai yaptırımlar da eklenmeli.”
5) “Yaptırımlar her ne koşulda olursa olsun yeterli denetim olmadıktan sonra anlamsızlaşmaktadır. Bu sebeple denetim mekanizması da yeterli düzeyde oluşturulmalıdır. Bunun yanında, hukuki sistemde kaçak noktalar bırakılmamalı ve sağlam temeller üzerine oturtulmalıdır.”
6) “Para ve hapis cezası olabilir.”
7) “Düzenleme sade, açık ve uygulamanın yaygın ve yeknesak olması gerekir. Denetimin etkili olması uygulamada aksayan her hususun fark edilmesi ve sürekli iyileştirme yapılmasını sağlayacağından önemlidir. Bunların olabilmesi için kişisel bilincin, eğitimin, bilişim teknolojileri kullanım becerisini desteklemeye yeterli bilgi birikiminin toplum genelinde ve kişisel bilgileri kullanılan/kişisel bilgileri oluşturan/kullanan/analitiğini yapma ölçülerine uygun seviyelerde verilmesi gerekir. Yaptırımın yapabildiğinden fazlası için bu gereklidir.”
8) “Uygulama neticesinde yaptırımlarda bazı güncellemeler yapılabilir.”
9) “Bu konuda çalıştırılmak istenenlerin çekinmesine ve gönüllü olarak bu konuda çalışmak istememesine yol açabilir.”
10) “Açıkçası bu ceza bazen sistemlerin yeterince uygun tasarlanmamasından da oluşmakta; sisteme giriş ve veri tabanlarını masraftan kısmak için hala aynı makinelerde çalıştıran pek çok kurum var. En basitinden bunları ayırmak standartlara uygun şifreleme entegrasyonu bile kullanılmazken bir bilişim mühendisine sadece yönetici (db admini) yetkisi verilerek bütün bu adli ve idari işleri de bu kişiye yıkmak bana göre etik değil. Sonuçta adamın tasarlamadığı sistem ve sadece yürütücü; tabi kişinin etkinliği ve yetkinliği de tartışılır.”
11) “Yaptırımların caydırıcı niteliğinin olması gerekiyor. Sadece idari para cezasının yeterli olduğunu düşünmüyorum.”
12) “Biraz daha yaptırımın ağır olması ve bunun deklare edilerek caydırıcı etkisinin sağlanması gerekir.”
13) “Yaptırımlar hakkında bilgim olmadığı için öneride bulunamıyorum.”
14) “Yaptırımların uygulanması denetlenmesi çok önemli.”
15) “Etkili bir düzenleme sağır duzenleme değildir.”

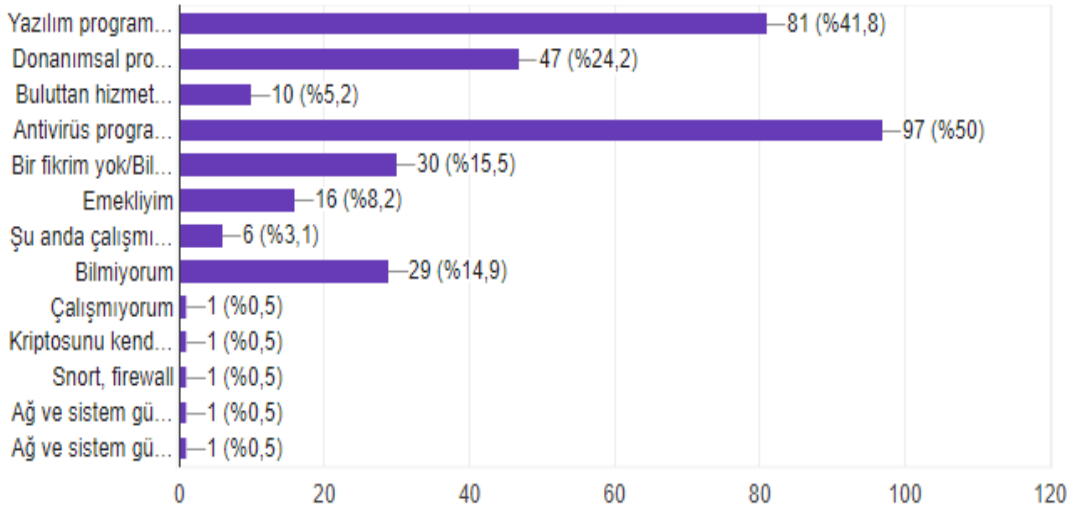
16) “Uygun bir düzenleme olduğunu düşünüyorum.”
17) “Ağır cezalar verilmeli.”
18) “Para cezası aralığı çok açık; uygulanamaz gibi görülüyor.”
19) “Yerinde ve kişileri güvende hissetiriyor.”
20) “Fikrim yok.”
21) “Öncelikle kurumlar muhatap alınmalı.”

Kişilerden alınan görüşler doğrultusunda iki yönlü değerlendirme yapılabilecektir. İlk değerlendirme, ilgili kişilerin bakış açısından kişisel verilerin korunması meselesidir. İkinci değerlendirme ise veri sorumlularının bakış açısından KVKK uyarınca kendilerine ait olan yükümlülükler ve yaptırımlara ilişkindir. İlk değerlendirme çerçevesinde, ilgili kişilerin kişisel verilerin korunması konusunda endişeli olduğu ve yasal düzenlemeler kadar bu düzenlemelerin uygulanması konusuna da önem verdikleri görülmektedir. Yasal düzenlemede yer alan yaptırımların daha da ağırlaştırılarak caydırıcılık sağlanabileceği görüşleri yer almıştır. Yasal düzenlemelerle caydırıcılık sağlanmasının yanında denetimin de önemi vurgulanmaktadır. Denetim ne kadar sık yapılırsa, kuruluşlar da o derece kişisel verilerin korunması mevzuatına uyum sağlamak amacıyla çalışmalar yürütecektir. Düzenleme ile birlikte uygulamada yeknesaklık sağlanması gerekliliği de vurgulanmaktadır. Son olarak farkındalık konusunun da önemi ifade edilerek tüm kişilerde kişisel verilerin işlenmesine ilişkin bilincin olması gerekliliği açıklanmıştır. Bir ülkede mevzuat ne kadar katı düzenlenmiş olursa olsun, kişilerin bilgi sahibi olmaması sonucunda katı düzenleme bir anlam ifade etmeyecektir. Dolayısıyla, kişilerin eğitimi ve bilinçlendirmenin kişisel verilerin korunmasında en temel faktörlerden birisi olduğunu söylemek yerinde olacaktır.

İkinci değerlendirmede ise veri sorumlularının temel sorunu kurumsal ilkeler, kuruluşların yeterli önlemleri almayarak veri sorumlularından ve/ya işleyenlerden hali hazırda olan sistemler ile yükümlülüklerini gerçekleştirmelerini beklemesidir. Masraflı olması dolayısıyla kuruluşlarda yeterli güvenlik önlemlerinin alınamadığı, yöneticilerin kararı doğrultusunda çalışan personellerin bu konuda bilinçli olsalar dahi kurumsal ilkelere bağlı kalma zorunlulukları veri sorumlularını ve/ya işleyenleri zor durumda bırakmaktadır. Yine kişisel verilerin işlenmesi kapsamında tanımlanan

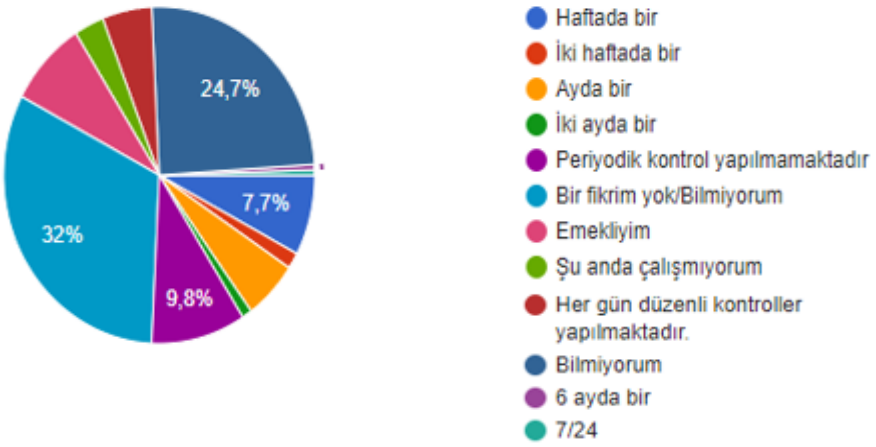
teknik ve hukuki yükümlülüklerin teknik personeller tarafından yerine getirilmesini beklemek de veri işleyenleri zor durumda bırakan bir başka husustur.

Bölüm 2'de kişisel verilerin ihlâl edilmesi durumu ve alınan önlemlere yönelik sorular yöneltilmiştir. İkinci bölümdeki ilk soru "*Kuruluşunuzda veri güvenliğini sağlamak için ne tür güvenlik ürünleri kullanılmaktadır?*" şeklindedir. Bu soru ile teknik açıdan bilgi güvenliğini sağlamak için ne şekilde önlemlerin alındığı tespit edilmek istenmiştir. Bu çerçevede, katılımcıların %50'si antivirüs programı ile veri güvenliğini sağladığını beyan etmiştir. İkinci sırada ise %41.8 ile yazılım programları gelmektedir. Üçüncü sırada %34.4 ile bu konuda bir bilgisi olmadığını söyleyenler gelmektedir. Dördüncü sırada %24.2 ile donanımsal programlar yer almaktadır. %5.2'lik kesim ise buluttan hizmet alarak veri güvenliğini sağladıkalrını belirtmiştir. Bunlar dışında ankete katılanların %1'i ağ ve sistem güvenlik uygulamalarını; %0.5'i snort, firewall uygulamalarını; %0.5'i de kriptosunu kendi oluşturdukları veriler ve sistemler aracılığı ile koruduklarını belirtmiştir.

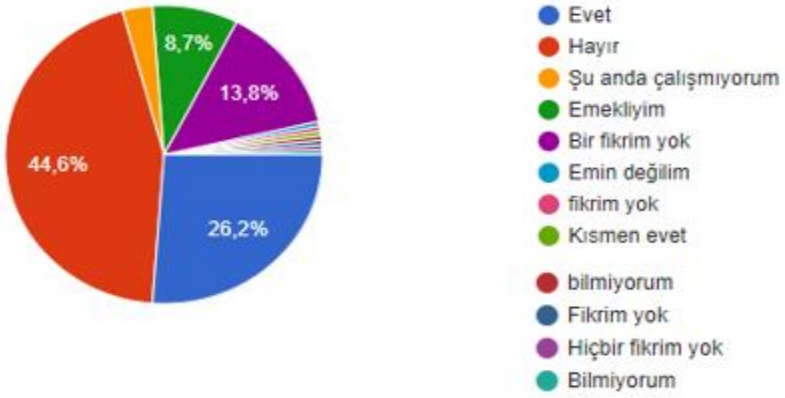


Şekil 4.14: Kullanılan güvenlik yöntemleri

Bölüm 2'de ikinci soru olarak veri güvenliğini sağlamak için kullanılan sistemlerde periyodik kontrolün ne kadar sıklıkta yapıldığı sorulmuştur. Bu soruya da farklı cevaplar verilerek çeşitli zaman dilimleri belirtilmiştir. En fazla verilen yanıt, %56.7'lik oranla "*bilmiyorum/bir fikrim yok vb.*" olmuştur. %9.8'i "*periyodik kontrol yapılmamaktadır*"; %7.7'si "*haftada bir*"; %5.7'si "*ayda bir*"; %5.7'si "*her gün – 7/24 düzenli kontroller yapılmaktadır*"; %1.5'i "*iki haftada bir*"; %1'i "*iki ayda bir*"; %0.5'i "*altı ayda bir*" seçeneklerini işaretlemişlerdir.



Şekil 4.15: Kontrol süreçleri



Şekil 4.16: Görüşler – III

Üçüncü soru olarak "*Kuruluşunuzda veri güvenliğinin korunması için yeterli önlemlerin alındığına inanıyor musunuz?*" sorulmuştur. Katılımcıların %44.6'sı "*Hayır*" seçeneğini işaretlemiştir ve en fazla da bu seçenek işaretlenmiştir. %26.2 "*evet*"; %16.8 "*bir fikrim yok - bilmiyorum - emin değilim vb.*"; %0.5 "*kısmen evet*" seçeneklerini işaretlemiştir. Katılımcıların yaklaşık %60.4'ünün kuruluşlarında ne tür

teknik önlemler alındığını bilmemeleri yine farkındalığın önemini ortaya koymaktadır. Kuruluşlarda yürütülen bu tür çalışmalar şeffaf olmalıdır ve tüm çalışanların bu konuda bilgilendirilmesi gerekmektedir. Bu sonuç, çalışan kişilerin de bilgi güvenliğinin korunması açısından çalıştıkları kuruluşa güvenmemeleri sonucuna da yol açabilecektir.

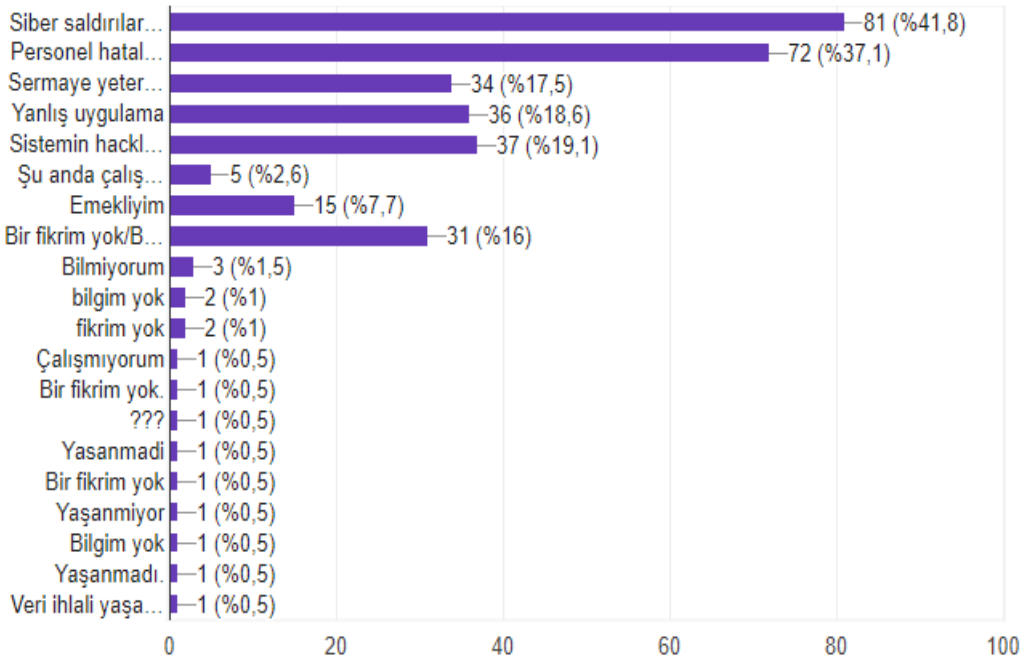
Diğer soru ise katılımcıların eğer çalışıyorlar ise çalıştıkları kuruluşta veri güvenliği ihlâlinin yaşanma sıklığı sorulmuştur. Çoğunluk %48.5 ile "*bilmiyorum – bir fikrim yok*" yanıtını vermiştir. Katılımcıların %21.1'i "*bazen*"; %15.5'i "*hiç yaşanmadı*"; %2.6'sı "*sık sık*"; %1'i "*bir kez*"; %0.5'i "*Virüslü mail açılması ile bilgisayar içindeki dosyaların kullanım dışı hale gelmesi ile yaşandı*" yanıtlamışlardır.

Şekil 4.17: Veri güvenliği ihlâlleri

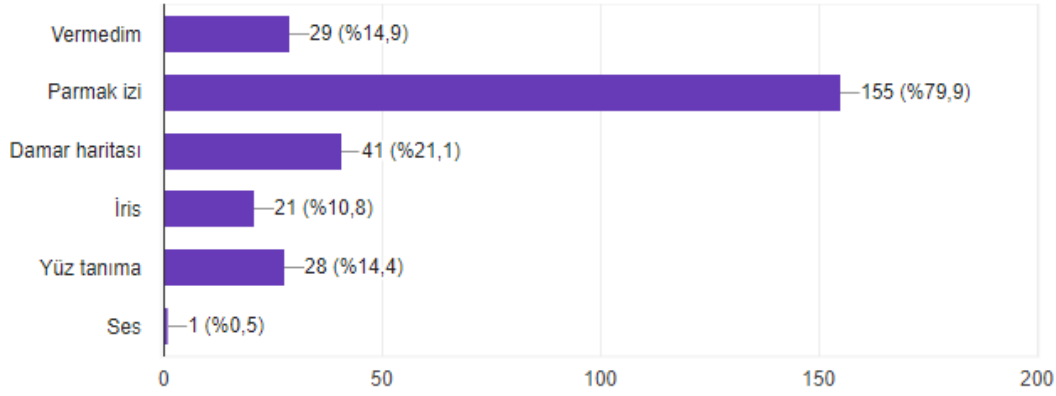
Beşinci soru olarak "*Veri ihlâlleri yaşanıyor ise bu ihlâller ne gibi sebeplerden ötürü yaşanmaktadır?*" sorulmuştur. Katılımcılara birden fazla seçenek işaretleyebilme imkânı tanınmıştır. Bu çerçevede, en fazla işaretlenen seçenek %41.8 ile "*Siber saldırılar (DDoS, DoS, Truva atı, vb)*" olmuştur. İkinci olarak ise %37.1 "*personel hataları ve kusurları*" oylanmıştır. Diğer oylamalar ise sırasıyla %19.1 ile "*sistemin hacklenmesi suretiyle verilerin elde edilmesi*"; %18.6 ile "*yanlış uygulama*"; %17.5 "*sermaye yetersizliği sebebiyle sistemlerin korunması için yeterli teknik donanımın sağlanmaması*"; %21.5 "bilmiyorum – bir fikrim yok vb."; %2 "veri ihlâli hiç yaşanmadı" olarak sonuçlanmıştır.

Bölüm 3 çerçevesinde biyometrik verilerin kullanım alanları ve izlenen politikalar, görüşler alınması hedeflenmektedir. Bölüm 3'teki ilk soru "*Herhangi bir kişi ya da*

kuruma ne tür biyometrik veri verdiniz?" olarak sorulmuştur. Katılımcıların birden fazla seçeneği işaretleyebileceği de belirtilmiştir. Ankete katılanların %79.9'u "*parmak izi*"; %21.1'i "damar haritası"; %10.8'i "iris"; %14.4'ü "yüz tanıma"; %0.5'i "ses" olarak oylamıştır. Ayrıca, katılımcıların %14.4'ü ise biyometrik veri vermediklerini ifade etmiştir.



Şekil 4.18: İhlâl nedenleri



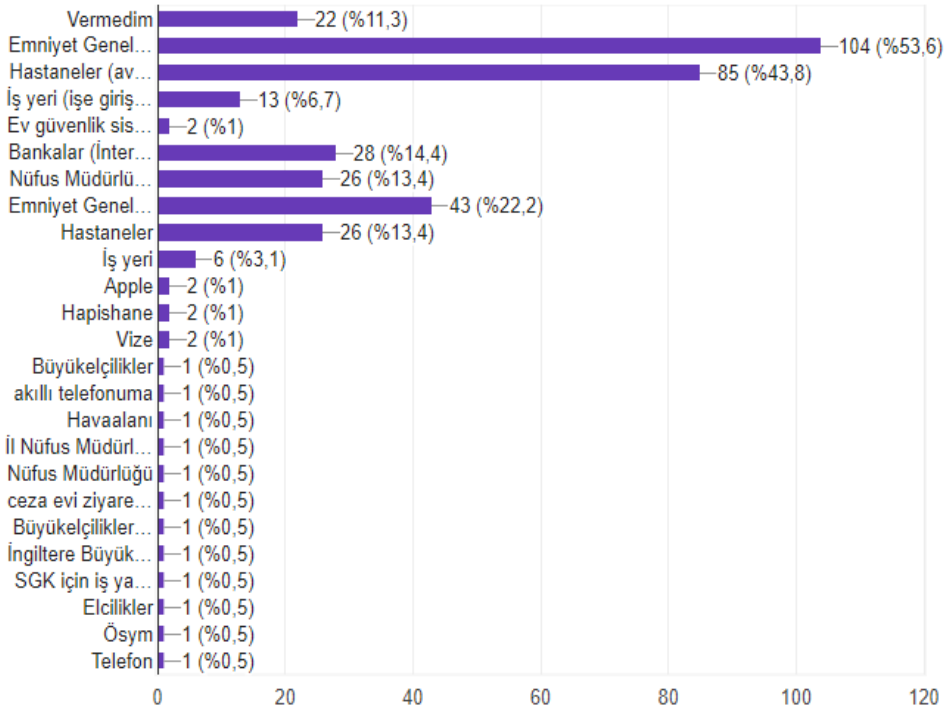
Şekil 4.19: Katılımcılardan örnek alınan biyometrik veri türleri

İkinci soru uyarınca katılımcılara biyometrik verilerini hangi Kurumlara verdikleri sorulmuştur. Yine birden fazla seçebilme ve yeni seçenekler ekleyebilme imkânı tanınmıştır.

Katılımcıların;

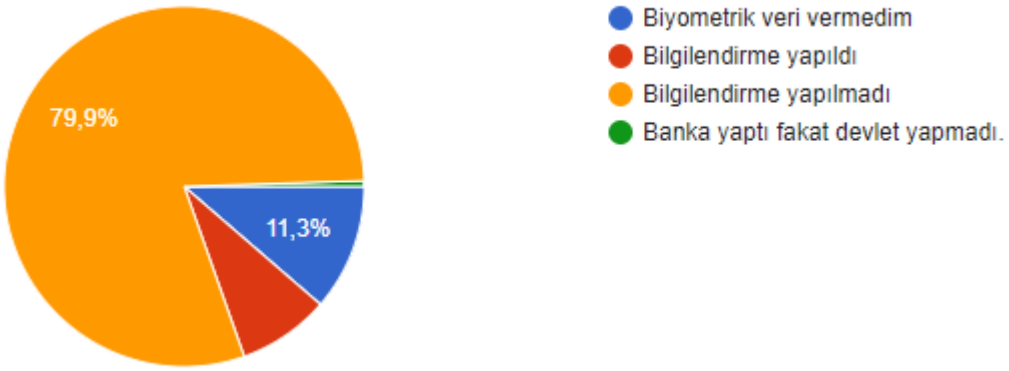
- %11.3'ü "*vermedim*"
- %75.8 "*Emniyet Genel Müdürlüğü (pasaport, yeni sürücü belgeleri vb.)*"
- %57.2 "*Hastaneler (avuç içi tarama vb.)*"
- %12.7 "*İş yeri (işe giriş-çıkışlarda parmak izi okutma vb)*"
- %1 "*Ev güvenlik sistemi*"
- %14.4 "*Bankalar (internet bankacılığı vb.)*"
- %14.4 "*Nüfus Müdürlüğü*"
- %2 "Akıllı telefon"
- %3 "Büyükelçilikler"
- %0.5 "Ösym"
- %0.5 "*SGK için iş yapan ve bilişim sektöründe çalışan firma standında cihaz tanıtımında*"
- %0.5 "*Havaalanında*"
- %1.5 "*Ceza evi (ziyaretçi girişinde göz okutma vb.)*"

şeklinde cevaplamak suretiyle soruya yanıt vermişlerdir.



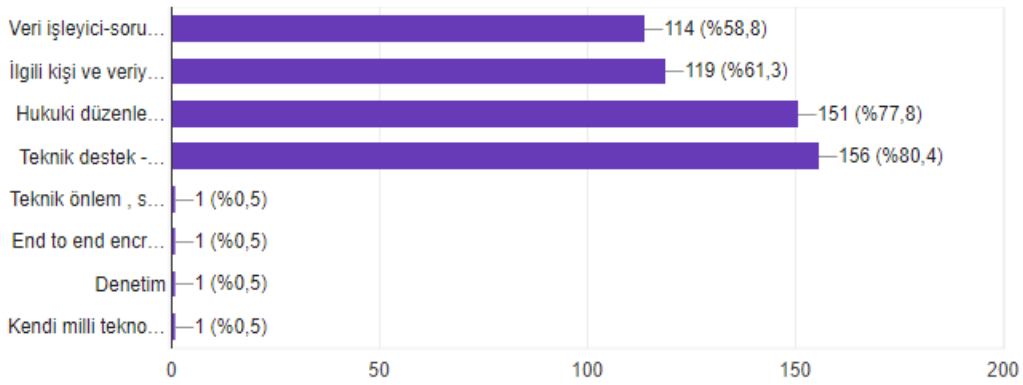
Şekil 4.20: Katılımcıların biyometrik verisini işleyen kuruluşlar

Üçüncü soru olarak "*Biyometrik verilerinizin işlenmesi ve sahip olduğunuz haklarınız ile ilgili tarafınıza herhangi bir bilgilendirme yapıldı mı?*" sorusu yöneltilmiştir. Katılımcıların %79.9'u "*bilgilendirme yapılmadı*"; %11.3'ü "*biyometrik veri vermedim*"; %8.2'si "*bilgilendirme yapıldı*"; %0.5'i "*banka yaptı; fakat Devlet kurumları yapmadı*" cevaplamıştır.



Şekil 4.21: Katılımcıların biyometrik verilerini paylaşmadan önce bilgilendirilme oranları

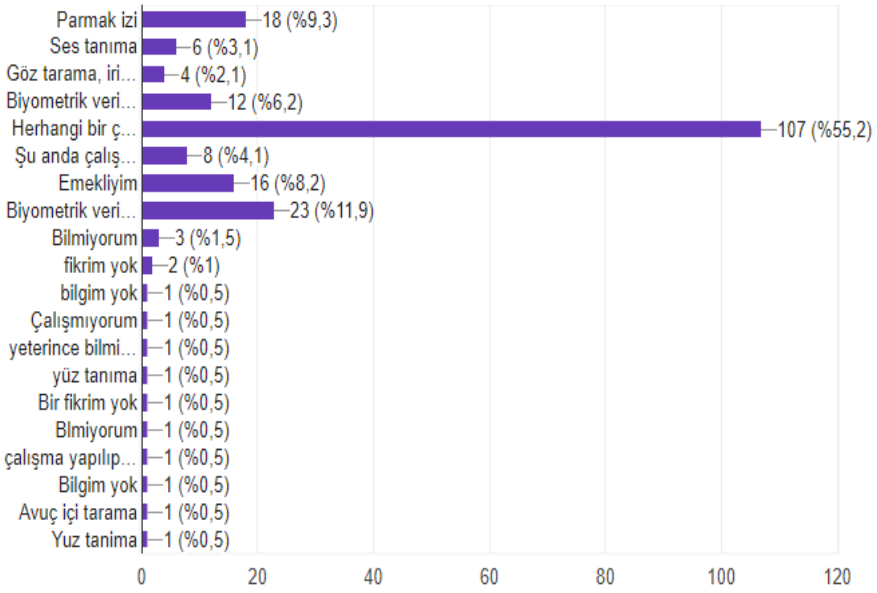
Diğer soru ise biyometrik verilerin korunması için ne gibi önlemlerin alınması gerektiğine ilişkindir. Bu soru kapsamında da katılımcılar birden fazla seçenek işaretleyebilir; yeni seçenekler ekleyebilmektedir. Bu soruya da %80.4 "*Teknik destek - önlemlerin alınması ve bu suretle en üst düzey korumanın sağlanması*"; %77.8 "*Hukuki düzenlemeler ile*"; %61.3 "*İlgili kişi ve veriye ulaşma yetkisi olanların farkındalığının artırılması*"; %58.8 "*veri sorumlusunun – işleyenin eğitimi*"; %0.5 "*Teknik önlem ,sürekli güncellenen ve denetlenen bir yapıyı içen önlemden oluşmalıdır.*"; %0.5 "*End to end encryption uygun standartta*"; %0.5 "*denetim*"; %0.5 "*kendi milli teknolojisi ile üretim*" yanıtları alınmıştır. Milli teknolojinin geliştirilmesi, bir ülkenin kalkınması açısından da gerekli olan temel unsurlardan bir tanesidir. Milli yazılımlarla bu yazılımı tasarlayan kişiler korumanın en iyi ne şekilde gerçekleşebileceğini bilirler ve verilerin yurt dışı sınırlarına kaçak olarak aktarılması ihtimali de asgari düzeye indirgenebilir. Kişiler, yabancı sistemlerden ziyade milli yazılımlara daha çok güveneceklerdir.



Şekil 4.22: Veri koruma önlemleri

Beşinci soruda "*Biyometrik verilerle ilgili Kuruluşunuzun yürütmüş olduğu çalışmalar var mı? Varsa bunlar nelerdir?"* sorulmuştur. Katılımcılar birden fazla seçenek işaretleyebilir; yeni seçenekler ekleyebilmektedir. Bu kapsamda verilen yanıtlar aşağıdaki gibidir:

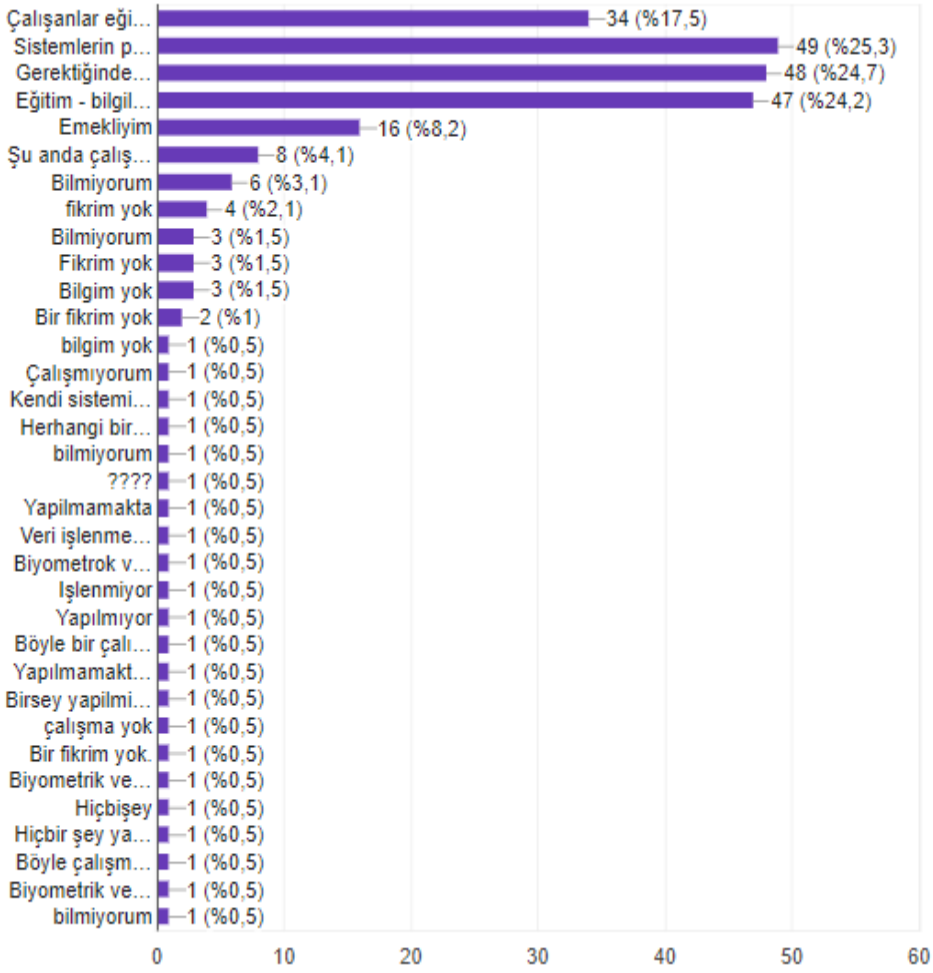
- %55.2 "*Herhangi bir çalışma yürütülmemektedir*"
- %11.9 "*Biyometrik veri işlenmiyor*"
- %9.3 "*Parmak izi*"
- %6.2 "*Biyometrik verilere ilişkin projeler, eğitimler*"
- %5.5 "*Bilmiyorum – bir fikrim yok vb.*"
- %3.1 "*ses tanıma*"
- %2.1 "*göz tarama, iris tarama*"
- %1 "*yüz tanıma*"
- %0.5 "*avuç içi tarama*"



Şekil 4.23: Kuruluşların biyometrik veri ile ilgili çalışmaları yürütme oranı

Diğer soru olarak "*Kuruluşunuzda genel itibariyle kişisel verilerin ve biyometrik veriler de işleniyorsa biyometrik verilerin güvenli olarak saklanması/işlenmesi için ne yapılmaktadır?*" sorulmuştur. Katılımcılar birden fazla seçenek işaretleyebilir; yeni seçenekler ekleyebilmektedir. Bu kapsamda verilen yanıtlar:

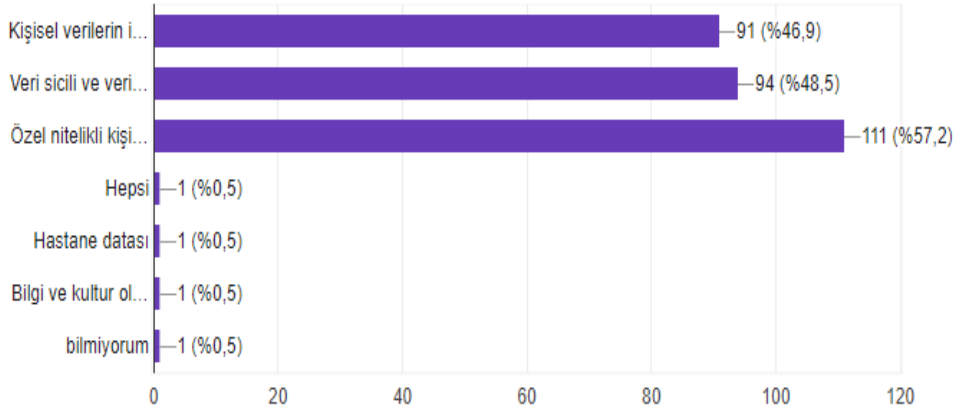
- %25.3 "*Sistemlerin periyodik bakımı yapılmaktadır*"
- %24.7 "*Gerektiğinden fazla veri talep edilmemektedir*"
- %24.2 "*Eğitim, bilgilendirme yapılmaktadır*"
- %17.5 "*Çalışanlar eğitilmektedir*"
- %0.5 "*kendi sistemimiz, kriptolu*"
- %0.5 "biyometrik veri işlenmemektedir"
- %7.5 "*biyometrik veri alınmıyor – bu konuda bilgim yok vb.*" cevaplar vermiştir.
- %13.6 "*bilmiyorum – bilgilendirme yapılmadı vb.*" şeklinde yanıtlamıştır.



Şekil 4.24: Biyometrik verilerin güvenle saklanması yöntemleri

Anketin son sorusu ise "*6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun uyarınca düzenlenen konular ile ilgili ikincil düzenlemeler de yapılacaktır. Bu çerçevede düzenleme yapılmasına ihtiyaç olduğunu düşündüğünüz başlıklar nelerdir? (Not: 28.10.2017 tarihi itibari ile kişisel verilerin silinmesi, anonimleştirilmesi, yok edilmesi ile ilgili Yönetmelik yayımlanmıştır.)*" biçimindedir. Ankete katılanların %57.2'si "*Özel nitelikli kişisel verilerin daha kapsamlı düzenlenmesi (sektörel bazda ayrı düzenlemeler de söz konusu olabilir)*" oylamıştır. Anket 28 Ekim 2017 tarihinden bir buçuk ay kadar önce hazırlanıp katılımcılar tarafından cevaplanmaya başladığı için Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hâle Getirilmesi Hakkında Yönetmelik yayımlanmamıştı. Katılımcıların %46.9'u bu Yönetmeliği oylamışlardır; 28 Ekim 2017 tarihinde Resmi Gazete'de yayımlanan bu Yönetmelik 1 Ocak 2018 tarihi itibari ile yürürlüğe girecektir. Katılımcıların %48.5'i "*Veri sicili ve veri sorumlularının yükümlülüklerine ilişkin detaylı düzenlemeler*" seçeneğini

seçmişlerdir. Bu seçenekler dışında her biri %0.5 oranında olmak üzere "*hastane verilerine ilişkin düzenlemeler*"; "*bilgi ve kültür oluşturulmalı*"; "*hepsi*" yanıtları verilmiştir.



Şekil 4.25: Katılımcıların önerileri

5. SONUÇ VE ÖNERİLER

Kişisel verilerin korunması meselesi sadece Türkiye'de değil, birçok ülkede önem teşkil eden bir konudur. Bilgi güvenliğinin bir uzantısı olan kişisel verilerin korunması için çeşitli stratejiler oluşturulmakta, yasal düzenlemeler çıkarılmaktadır. Sonuç ve öneriler başlığı altında, Türkiye'deki ve karşılaştırmalı uluslararası yasal düzenlemelere ve cevaplandırılan anket çıktılarına değinilerek uygulamadaki örnekler de değerlendirilerek önerilerde bulunulmaya çalışılacaktır. Öneriler, yasal düzenlemeler ve siber güvenlik konu başlıkları altında irdelenecektir.

5.1 Kişisel ve Biyometrik Verilerin Korunmasında Yasal Düzenleme Çerçevesinde Öneriler

Kişisel verilerin korunması için birçok ülke tarafından düzenlenen mevzuatlar, ilkeler ve kurallar çalışma kapsamında açıklandı. Kişisel verilerin korunma düzeyi, ülkelerin refah seviyesini de belirlemektedir.

Anket sonuçlarında ve kişisel veri düzenlemelerinde adı geçmemekle birlikte, büyük veri ve yapay zekâ kavramları bilişim toplumunun vazgeçilemez kavramlarından birisi olmuştur. Teknolojinin gelişmesi ile birlikte bilgi toplumu kavramı oluşmuştur ve beraberinde büyük veri (big data), nesnelerin interneti (internet of things) gibi birtakım yeni teknolojileri de getirmiştir. Anket sonucunda büyük veri konusu geçmemiş olsa da, kişisel veri ile büyük veri arasındaki ilişkinin irdelenmesi faydalı olacaktır. Teknoloji ile ortaya çıkan yeni konseptlerin hukuksal olarak düzenlenme ihtiyacı doğmaktadır. Yapay zekâ, nesnelerin interneti, büyük veri gibi kavramlara ilişkin çalışmalar arttıkça, bunların uygulamadaki yeri ve önemi de aynı doğrultuda artmaktadır. Dolayısıyla, bu yeni kavramların da hukuki çerçevede korunması ve düzenlenmesi gerekliliği ortaya çıkmaktadır. Büyük veri, son zamanlarda gündeme gelen en önemli konulardan bir tanesidir ve birçok sektör tarafından da bu konuya ilişkin çalışmalar yürütülmektedir. Büyük verilerin işlenmesi ile ilgili mahremiyetin ihlâli, kişisel verilerin korunmasının ihlâli gibi sorunlara yol açabileceği nedeni ile

Devletin ve Kuruluşların gözetiminin artması sonucunda çalışmaların sağlıklı yürütülememesi gibi etik problemler söz konusu olabilmektedir [51]. Büyük verilerin şirketler tarafından işlenmesi gerekliliği Japonya'da kişisel veri düzenlemelerinde de etkisini göstermiştir [28]. Büyük veri, kişilerin durumlarına ve davranış yapılarına ilişkin verileri de içermektedir, bunun sonucunda da özel nitelikli kişisel verileri de kapsamına almaktadır [52]. Büyük verileri aracılığıyla çeşitli firmalar ve kamu kurumları, toplanılan verilerle müşterilerin/tüketicilerin vb. kişilerin hangi durumlarda ne şekilde tepki verebileceğini tespit etmeye başlamıştır [52]. Bütün bu verilerin analizi de kişilerin kişisel verilerinin ilgili kişilerin farkında olmadan alınabilmesi, işlenmesi sonucunu ortaya koymaktadır. Şirketler, ilgili kişilerin açık rızası olmaksızın elde ettikleri kişisel verileri üçüncü kişilere satarak ekonomilerini büyütüp, sektörde rekabetsel üstünlük sağlamaktadırlar. Kişisel verilerin ilgili kişilerin rızası olmaksızın toplanması, paylaşılması vb. eylemler de etiksel olarak mahremiyet hakkını zedeleyerek kişisel verilerin ihlâli sorununu gündeme getirmektedir [52]. KVKK'da kişisel verilerin işlenmesine ilişkin istisnalar göz önünde bulundurularak o istisnalar mevcut ise kişisel veriler işlenebilecektir. Büyük veri, doğru amaçlarla kullanıldığı takdirde yeni kurumsal ve toplumsal olanaklara fırsat sağlayarak değer yaratımına katkıda bulunmaktadır [53]. Bu çerçevede, kişisel verilerin işlenmesi ilkelerinin çizdiği sınırlar çerçevesinde büyük veride kişisel verilerin kullanılması sağlanabilir. Yasal düzenlemelerin teknolojik gelişmeleri göz ardı edecek şekilde katı düzenlenmesi o ülkeye bir fayda sağlamayacaktır. Yeni gelen teknolojilerle birlikte hukuki çerçeve de uyumlu bir şekilde çizilerek teknoloji ve hukuk arasında dengeli menfaat sağlanmalıdır.

Kişisel verilerin hukuka aykırı olarak işlenmesi durumunda ortaya telafisi zor durumlar ve uygulanan ağır yaptırımlar çıkmaktadır. Bu noktada, kişisel verilerin işlenmesi konusunda hem ilgili kişilerin hem de veri sorumlularının ve veri işleyenlerin bilinçlendirilmesi, bu konuya ilişkin eğitim olanaklarının sağlanması çok büyük önem taşımaktadır. Şirketlerin Devlet tarafından denetimi ve hesap verilebilirlik ilkesi gereği yaptığı eylemlerin kapsamını belirtmesi; şirketlerin yanlış yapmamak ve ceza almamak için tekdüze politikalar benimsemesine yol açabilmektedir. Bu durum, anket sonuçlarında da katılımcılar tarafından vurgulanan bir husustur. Bu doğrultuda, şirketlerin kişisel verilerin işlenmesi konusunda titiz çalışmalar yürüterek strateji ve politikalar belirlenmesi ve bu politikalara ilişkin

personellerini bilgilendirmesi çok önemlidir. Bilinçlendirmenin büyük bir kısmı bu şekilde gerçekleşebilecektir.

KVKK uyarınca veri sorumlularına ağır yaptırımlar ve yükümlülükler öngörülmektedir. Anket sonucunda caydırıcılık açısından her ne kadar daha ağır hapis ve para cezaları uygulanmalı şeklinde görüşler olsa da caydırıcılık kadar sorumlulukları paylaştırmak da katkıda bulunacaktır. Sadece teknik personellere hem hukuki hem teknik sorumlulukları yüklemek doğru olmayacaktır. Ya da tam tersi olarak hukuki ve teknik sorumlulukları hukukçulara yüklemek de çözüm olmayacaktır. Hukukçu ve teknik personel işbirliği çerçevesinde veri sorumlusu yükümlülükleri ve görevlerinin yerine getirilmesi, kişisel veri uygulamalarının doğru bir şekilde uygulanmasına katkıda bulunacaktır. Hukukçu meşruluğu ve yasal sorumlulukları irdelerken teknik personeller de bu verilerin güvenle saklanması için yükümlülüklerini yerine getireceklerdir ve böylelikle uzun vadede faydalı olacak stratejiler ve politikalar da belirlenebilecektir.

Biyometrik veriler, her bir kişiye has, değiştirilemez özellikleri ile bilgi güvenliğinin sağlanması açısından şifrelere nazaran çok daha fazla güvenilir verilerdir. Biyometrik veriler, sadece ülkemizde değil dünya genelinde özel nitelikli kişisel veri olduğu için sıkı hukuk kurallarına tabidir. Bu çerçevede biyometrik verilerin hem yasal hem teknik açıdan korunması gerekmektedir.

Biyometrik verilerin ve kişisel verilerin yasal düzenlemelerle güvence altına alması büyük önem taşımaktadır. Yasaların önemi, beraberinde getirdikleri yaptırımlarla caydırıcılık teşkil etmesidir. Ülkemizde KVKK kişisel verilerin ve dolayısıyla biyometrik verilerin korunmasını düzenleyen temel yasadır. Kişisel verilerin korunması hakkı Anayasa kapsamında da güvence altına alınmıştır. Bunlar dışında Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hâle Getirilmesi Hakkında Yönetmelik 28 Ekim 2017 tarihinde Resmi Gazete'de yayımlanarak 1 Ocak 2018 tarihinde yürürlüğe girecektir. Bunun dışında örnek olarak sağlık sektöründe de kişisel verilerin korunması için Yönetmelikler mevcuttur.

Her ne kadar sağlık, bankacılık, haberleşme gibi sektörlere ilişkin kişisel verilerin korunması ile ilgili ikincil düzenlemeler bulunsa da bunların yeterli olmadığı ifade

edilebilir. Öncelikle, veri sicili kavramı büyük önem teşkil etmektedir ve bu sicilin hukuka uygun tutulabilmesi için usul ve esasları detaylıca düzenleyen bir yönetmeliğe ihtiyaç vardır. Kişisel verilerin üçüncü kişilere ve yurt dışına aktarılması hususu da ayrı bir düzenleme ile daha detaylı düzenlenebilir, Kişisel Verileri Koruma Kurumu'nun belirleyeceği standartlar ve şartlar da bu düzenleme kapsamında yer alabilir. Bunlara ek olarak, özel nitelikli kişisel verilere ilişkin düzenlemeler; kişisel verilerin güvenliğinin sağlanmasına yönelik düzenlemeler (sertifikasyon –istisnalar); ilgili kişilerin şikâyet sürecine ve bu şikâyetlerin değerlendirilmesine ilişkin düzenlemeler de düzenlenmesine ihtiyaç duyulan ikincil mevzuatlardır. Özellikle özel nitelikli kişisel verilerin korunması hassas bir mesele olduğu için bunun ayrıca düzenlenerek daha detaylı hükümler öngörülmesi faydalı olacaktır.

İkincil düzenlemeler dışında Amerika'daki sistemde de söz konusu olduğu gibi sektörleri tarafından rehber ilkelerin oluşturulması da önem teşkil etmektedir. Hatta kişisel verilerin işlenmesi ile ilgili yapılan düzenlemeler sektör sektör ayrı yönetmeliklerle detaylı olarak hüküm altına alınabilir. Sağlık sektöründe ve elektronik haberleşme sektöründe yönetmelikler olsa da bunların güncellenerek daha detaylı bir şekilde düzenlenmesi de faydalı olacaktır. Şirketlerin benimsedikleri kurumsal ilkeler günümüz koşullarına adapte edilerek güncellenmeli ve o doğrultuda stratejiler oluşturulmalıdır.

İhtisas mahkemelerinin kurulması da kişisel verilerin korunması bakımından faydalı olacaktır. Kişisel verilerin korunması hususu hukuki olduğu kadar teknik meseleleri de içinde barındırmaktadır ve bu konuda yargılamanın daha adil ve hızlı ilerleyebilmesi için ihtisas mahkemelerinin kurulması önem teşkil edecektir. Bu kapsamda, hakimlere mühendislik eğitimi verilerek bilgi güvenliğinin teknik kısmı hakkında farkındalığının ve bilgisinin artması sağlanabilir. Hakimler teknik bilgilere sahip olmadıkları yerlerde bilirkişi raporlarına da başvurabilir; ancak teknik bilgiye sahip olarak durumu değerlendirmeleri yargılamanın sürecinde ve karar vermelerinde büyük kolaylık sağlayacaktır. Aynı şekilde, veri sorumlusu ve/ya veri işleyen olarak atanacak mühendislerin de hukuki düzenlemelere ilişkin eğitilmesi faydalı olacaktır.

Ankette katılımcıların vurguladığı bir başka husus da "denetim mekanizması"dır. Kişisel verilere uyum süreci ve sonrasında yapılacak her kişisel verilerin işlenmesine

ilişkin eylem sıkı denetim mekanizmaları sayesinde Kuuruluşları bu konuya yönelik çalışmalar yürütmeye yöneltebilir. Denetimin katı olması Kuruluşları korkutmamalıdır; aksine Kuruluşlar titiz çalışmalar yürüterek ve personellerini bilinçlendirerek kişisel verilerin korunması konusunda mevzuata uyum çerçevesinde varlıklarını sürdürebileceklerdir.

Bankacılık sektöründe biyometrik verilerin işlenmesi bakımından birtakım düzenlemeler olsa da verilerin paylaşılması hususunda standartlar karşılanamadığı için sıkıntılar oluşabilmektedir (Yukarıda 3.2.3 numaralı başlıkta yer alan Türkiye İş Bankası parmak izi ile açılan mobil uygulama düzenlemesini kaldırması gibi). Bundan dolayı bankacılık sektöründe kişisel verilerin işlenmesi için ayrı bir yönetmelik oluşturulabilir ve bu standartlara da uyan yazılımlar, veritabanları geliştirilebilir.

5.2 Kişisel ve Biyometrik Verilerin Korunmasında Siber Güvenlik Çerçevesinde Öneriler

Milli yazılımlar da bir ülkenin hem kalkınma hem güvenliğini sağlayabilmek açısından önem arz etmektedir. Kişisel verilerin korunması bakımından ulusal mevzuatımız bulunsa da çoğu kullanılan sistem ithaldir ve bu da kişilerin nezdinde güvensizlik oluşturabilmektedir. Yapılan anketin sonuçlarında da kişilerin bu konudaki endişesi dile getirilmiştir ve yerlileşmenin önemi vurgulanmıştır. Ülkemizde yerli üretim çeşitli sektörlerde gerek yasal zorunluluklarla gerek Devletin stratejileriyle teşvik edilmektedir. Kişisel verilerin korunması tamamen ülkemize ait yüksek güvenlikli milli bir yazılım ve donanım sistemi kurularak sağlanabilir. Yerli üretim, Türkiye'de 5G çalışmaları kapsamında da BTK tarafından desteklenmektedir ve bilişim sektöründe yerli üretim giderek etkisini artırmaktadır. Kişisel verilerin korunması açısından da milli yazılımlar üretilmesi büyük önem taşıyacaktır.

Kişisel verilerin saklanacağı veri kayıt sisteminde kişisel verilerin saklanacağı sürelerin belirlenmesi ve bu verilerin boyutları ile ilgili sorunlar ortaya çıkabilmektedir. Büyük veri ile kişisel veriler arasında bağlantı olabileceğini vurgulamakla beraber, büyük veri alanında çalışmalar yaparak kişisel verilerin saklanması açısından da verilerin boyutlarının daha ekonomik şekilde küçültülerek saklanması ya da büyük veri kapsamında çalışmalar yapılarak güvenlikli bir şekilde

saklanması sağlanabilir. Dolayısıyla, siber güvenlik çerçevesinde büyük veri çalışmalarının da büyük önem taşıdığını vurgulamak yerinde olacaktır.

Her ne kadar kişisel veri düzenlemeleri ile ilgili çeşitli konferanslar, seminerler düzenlenmekte ise de çoğu Kuruluşun maalesef bu düzenlemeler hakkında personellerini yeterli bilgilendirmediği veyahut uyum süreci çalışmalarını düzenli yapamadığı görülmektedir. Bu durum, anket sonuçlarına göre de (örneğin, ankette kişilerin %82.6'sı veri sorumlularına ilişkin yükümlülükler hakkında bir fikirlerini olmadığını beyan etmiştir) doğrulanmaktadır. Çoğu kişi ilgili kişi olarak haklarını bilmemekte; ya da tam tersi çoğu veri işleyen olarak görev yapabilecek kişi de yürütülen çalışmaları bilmemektedir. Bu konuda kişileri bilinçlendirmek en fazla önem teşkil eden husustur. Bilinçli insanlar kişisel verilerin önemini ve haklarını da bilerek kişisel verilerin korunmasında rol alacağı gibi veri sorumluları ve veri işleyenler de aynı şekilde titizlikle çalışmalar yürütürlerse kişisel verilerin korunmasında ideal seviyeye ulaşılabilecektir. Veri sorumluları ve işleyenler için eğitimler, konferanslar, çalıştaylar düzenlenerek yükümlülükleri hakkında bilgilendirme yapılması da faydalı olacaktır. Farkındalık meselesi, kişisel verilerin işlenmesi açısından son derece önemlidir ve gerekli eğitimler, Çalıştaylar düzenlenerek bilinçlendirme sağlanabilir. İlgili kişilerin bütününe ulaşabilmek açısından da Devlet kişileri televizyonlarda verilen kamu spotu gibi reklamlarla kişisel verilerin işlenmesi mevzuatı içeriği ve verilerin önemi hakkında kısa bilgilendirme videoları yayınlayabilir. Bu şekilde çok fazla kişiye ulaşılarak bilgilendirme yapılabilecektir.

Son olarak, AB'de çocuklar gibi toplumun daha fazla korunmaya muhtaç kesimleri açısından kişisel verilerin işlenmesi için ayrıca hükümler düzenlenmektedir. Ülkemizde de korunmaya muhtaç kişiler açısından Kanun'un içine hükümler ekleyerek ya da ikincil düzenlemelerle destekleyerek düzenlemeler yapılabilir.,

5.3 Sonuç

Bilgi toplumunun artık söz konusu olmasıyla birlikte nesnelerin interneti, büyük veri gibi kavramlar ortaya çıkmıştır. Büyük veri konusu Türkiye mevzuatı ve anket sonuçlarında da yer almamakla beraber, kişisel verilerin korunmasında kişisel veriler

ile ilişkili bir kavram olduğu için kişisel verilerin korunması ilkeleri bu çalışmaların yürütülmesinde de etkili olmalıdır; katı düzenlemelerin teknolojik gelişmeleri olumsuz etkilenmesi önlenmelidir.

Kişisel verilerin işlenmesi konusu Dünya genelinde önem teşkil eden ve titizlikle çalışmalar yürütülen bir konudur. Her ne kadar bu konuda yüzde yüz koruma sağlanamasa da yasal düzenlemeler ve teknik önlemlerin alınması ile kişisel verilerin güvenle işlenerek saklanması konusunda önlemler alınmaktadır. Bilgi güvenliğini sağlamak, çağımızın en önemli meselelerinden bir tanesidir. Türkiye'de de siber güvenlik çalışmaları yapılarak bilgi güvenliğinin yüksek seviyede tutulması amaçlanmaktadır.

Her ne kadar 108 Numaralı Sözleşme ile kişisel verilerin korunması düzenlemeleri gündeme gelse de, kişisel verilerin korunması süreci resmi olarak 7 Nisan 2016 tarihinden itibaren başlamıştır. KVKK, 95/46 Sayılı eski AB Kişisel Verilerin Korunması Tüzüğü'nden uyarlanarak oluşturulmuştur. AB'de güncellenmiş Kişisel Verilerin Korunması Tüzüğü, yani GDPR 2018 Mayıs'tan itibaren yürürlüğe girecektir ve 95/46 sayılı düzenlemesinde olmayan yeni haklar, kavramlar ve düzenlemeleri de beraberinde getirmektedir. Dolayısıyla, KVKK düzenlemeleri de tekrar gözden geçirilerek, teknolojik gelişmelerin de ışığında değerlendirilerek ilke ve kurallar ortaya konulmalıdır.

Biyometrik veriler, doğaları gereği özel nitelikli veya hassas kişisel veriler olup daha sıkı koruma kurallarına tabidir. Açık rıza, neredeyse tüm kişisel veri düzenlemeleri bulunan ülkelerde kişisel verilerin işlenmesi için temel şarttır; ancak buna ilişkin istisnalar da ayrıca düzenlenmektedir. Dünya genelinde kişisel verilerin işlenmesi ilke ve kuralları bakımından paralel düzenlemelerin bulunduğunu söylemek yanlış olmayacaktır.

Türkiye'de de biyometrik verilerin tutulması giderek artmaktadır. Bankacılık, sağlık, güvenlik, haberleşme vb. sektörlerde biyometrik verinin kullanımı giderek yaygınlaşmaktadır ve bu konuda düzenlemeler de ortaya çıkmaktadır. Türkiye'de biyometrik verilerin işlenmesine ilişkin temel Kanun KVKK olup bankacılık, sağlık,

elektronik haberleşme sektöründe ikincil düzenlemeler olsa da daha ayrıntılı düzenlemelerin yapılması faydalı olacaktır ve bu konuya ihtiyaç da duyulmaktadır.

Kişisel veriler Kanun uyarınca geniş kapsamda düzenlendiği için özellikle özel nitelikli kişisel verilerin işlenmesinde her sektör bakımından ayrı ayrı düzenleme yapılmasına ihtiyaç duyulmaktadır. Biyometrik veri sistemleri yüksek güvenlik sağlaması ve sahteciliği önlemesi özellikleri dolayısıyla günlük yaşamda ve her sektörde çok sık kullanılmaktadır. İnsanların evlerine giriş çıkışlarında biyometrik verilerini kullanmaları aracılığıyla güvenlik sağlanabileceği gibi işçi ve işveren açısından da iş yerlerine giriş çıkışlarda işçilerin parmak izi vb. biyometrik verilerini kullanmaları aracılığıyla mesai saatlerinin, işe giriş ve çıkış durumları kontrol edilebilmektedir. Yargı kararları bakımından farklı kararlar söz konusu olmakta; yerel mahkeme kararları ile Yargıtay ve Danıştay kararları çelişebilmektedir.

Örnek olarak, Danıştay 11. Daire, belediye personelinin mesai giriş çıkış saatlerinin tespitini sağlanmak amacıyla işçilere yüz tarama sistemi uygulaması ile ilgili başvuru hakkında, kamusal alana ilişkin olsa bile özel hayatın gizliliği bakımından bu verilerin ileride kullanılmayacağına ilişkin herhangi bir teminatın da bulunmadığı gerekçesiyle mesai giriş çıkış takibinin yüz tanıma sistemiyle yapılmasını Anayasa'ya aykırı bulmuştur [54]. Bu kapsamda, Danıştay 11. Daire 2017/816 Esas; 2017/4906 Karar numaralı , 13 Haziran 2017 tarihli kararında "*657 sayılı Devlet Memurları Kanunu'nun 99 ve devam eden maddelerinde Devlet memurlarının çalışma saatleri ile günlük çalışma saatlerinin başlama ve bitme saatlerinin tespitine yönelik düzenlemelere yer verilmiş olmakla birlikte,* ***kamu görevlilerinin mesaiye devam durumlarının kontrolü konusunda ayrıntılı bir yasal düzenleme mevzuatımızda bulunmamaktadır.*** *İdarelerce, gelişen teknolojinin kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlamasını doğal karşılamak gerekir. Ancak;* ***teknolojinin kullanılarak kişisel verilerin kayıt altına alınması uygulamasının yukarıda belirtilen hükümlere uygun olması gerektiği kuşkusuzdur****. Bu bağlamda,* ***personelin yüz tanıma sistemi ile mesai kontrolünün yapılması uygulamasının, temel hak ve hürriyetler içerisinde sayılan özel hayatın gizliliği ilkesi kapsamında kişisel bilgi veya kişisel verilerin alınması kavramları içinde değerlendirilmesi gerekmektedir. Olayda, personelden kişisel veri alınması kapsamında olan "yüz tanıma sistemi" ile mesai takibi uygulamasının,***

kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu açık olup, dava konusu işlem tarihi itibarıyla uygulamanın sınırlarını usul ve esaslarını gösteren bir yasal dayanağın bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmaması göz önüne alındığında, yukarıda belirtilen temel haklar ve Anayasal ilkelerle bağdaşmayan dava konusu işlemde ve davanın reddi yolundaki mahkeme kararında hukuka uygunluk bulunmamaktadır. [54]*"*. Danıştay kararı da göz önünde bulundurularak özel nitelikli kişisel verilerin işlenmesinde uygulamada sıkıntılar yaşandığı ve temel hak ve özgürlükler bakımından düzenlemelerle sınırların çizilmesi gerektiği vurgusu yapılmaktadır. Özel nitelikli kişisel verileri işlenmesi bakımından sektörler bakımından ikincil düzenlemelere veya detaylı olarak Yönetmeliklerin düzenlenmesi gerektiğini vurgulamak yerinde olacaktır.

Türkiye mevzuatı ve uluslararası mevzuat göz önünde bulundurulduğu zaman, kişisel verilerin işlenme şartı ve ilkeleri paralel olarak düzenlenmiş olup uygulama alanı, yaptırımlar ve bazı tanınan hak ve yükümlülükler bakımından farklılıklar mevcuttur. Kişisel veriler kamu ya da özel sektör ayrımı yapılmaksızın her sektör bakımından koruma altında bulunması gereken bir alandır. Kişisel verilerin denetlenme mekanizması yine yaptırımlar kadar önem teşkil etmektedir. Sektörlere ilişkin detaylı ikincil düzenlemeler çıkarılmasa bile Amerika'da olduğu gibi sektörlerin uyması gereken rehber ilkeler çıkarılabilir. Rehber ilkelerin bağlayıcılığı açısından Kişisel Verileri Koruma Kurumu bu rehber ilkeleri yayınlayabilir; yargılama sürecinde yerel mahkeme, Danıştay, Yargıtay arasında çıkan ikilemler bu şekilde çözüme kavuşturulabilir.

Veri sorumlularına KVKK ile ağır sorumluklar yüklenmiştir (aydınlatma yükümlülüğü, teknik ve hukuki önlemleri almak ve bu yükümlülüklere aykırı davranmamak vb.) ve veri sorumlularının görevlerini yerine getirebilmesi için görev paylaşımı hukuk ve teknik personeller arasında paylaştırılmak suretiyle yapılırsa yaşanacak muhtemel sorunlar asgari düzeye indirgenebilecektir. Yine bilinçlendirme ve eğitim, kişisel verilerin hukuka uygun işlenebilmesi açısından hem ilgili kişiler hem de veri sorumluları açısından çok büyük önem taşımaktadır. Yasal düzenlemeler kadar teknik önlemlerin alınması da bilgi güvenliğinin temel kilometre taşlarından bir tanesidir. Bu konuda kriptoloji bilimi veri güvenliğini sağlayan temel bilimlerden bir

tanesidir. Yüksek derecede koruma sağlayan şifreleme sistemleri kurularak bilgi güvenliği sağlanmalıdır. Kriptoloji kadar milli yazılımlarımızın bulunması da önemlidir. Kendi milli yazılımlarımızı geliştirerek verilerin ülkemiz sınırları dışına aktarılma ihtimali ortadan kaldırılarak kişilerin de bu yönde güveni daha çok sağlanmış olacaktır.

Bilişim alanı multidisipliner bir alan olduğu için çeşitli sosyal bilimler ve fen bilimleri konuları birbiriyle devamlı etkileşim göstermektedir. Bu çerçevede, hukukçuların bilgi güvenliğinin teknik kısmı hakkında eğitim alması; mühendislerin de bilgi güvenliğinin hukuk kısmı hakkında eğitim alması büyük önem taşıyacaktır. İhtisas mahkemeleri kurularak, kişisel verilerin hukuka aykırı işlenmesine yönelik adli ve cezai vakaların yürütülmesi faydalı olacaktır. İhtisas mahkemelerinde görev alacak hâkimlerin de Hâkimler ve Savcılar Yüksek Kurumu veya BTK nezdinde destek alınarak gerekli eğitimler alması, adli sürecin hızlı ilerlemesi ve doğru sonuçlar alınması bakımından önem teşkil edecektir.

Özetle, kişisel verilerin işlenmesi konusu ilgili kişiler kadar veri sorumluları ve/ya veri işleyenleri de ilgilendirmektedir. İlgili kişilerin farkındalığı artırılarak kişisel verilerin işlenmesi ve şikâyet mekanizmalarında bilincin sağlanması söz konusu olabilecektir. Kişisel verilerin ifşası veya hukuka aykırı olarak işlenmesi durumunda oluşabilecek telafisi zor zararlar ve risklerden haberdar olarak bu bilinçle hareket etmeleri faydalı olacaktır. Veri sorumluları ve işleyenler açısından da kişisel verilerin hukuka uygun olarak işlenmesi hem bu Kuruluşların rekabetsel üstünlük sağlamasını hem de güvenilirliklerinin artması ile sektörde büyümelerini sağlayacaktır. Kişisel verilerin işlenmesi sadece hukuksal bir konu gibi gözükse de, aslında içinde her türlü teknik ve hukuki içeriği barındıran ve son derece önem gösterilmesi gereken, farkındalığın üst düzeyde sağlanılması gereken bir konudur. Kişisel verilerin önemine binaen denetim mekanizmalarının ve gerekli çalışmaların yürütülmesi büyük önem taşıyacak ve ülkenin refah düzeyinin de artmasına katkıda bulunacaktır. Sonuç ve önerileri özetleyen tablo Şekil 4.26'da yer almaktadır.

TEKNİK	YASAL VE EĞİTİM
Milli yazılım oluşturma gereksinimi: Milli yazılım oluşturularak kişisel verilerin bu sistemle aracılığıyla tutulması ile kişisel verilerin tutulduğu güvenilir bir veri kayıt sistemi oluşturulabilir. Böylelikle, kişisel verilerin tutulduğu sistemlerin milli olmasıyla yabancı yazılımlara duyulan güvensizlik de bertaraf edilerek kişilerin güveni artacaktır.	**İkincil düzenlemeler:** • Veri kayıt sistemi • Aydınlatma yükümlülüğü • Özel nitelikli kişisel veriler: Sağlık sektöründe biyometrik verilerin işlenmesine ilişkin düzenlemeler mevcut olsa da çeşitli alanlarda biyometrik verilerin işlenmesine yönelik uygulamada yargı kararları çerçevesinde yeknesaklık olmadığı için birtakım problemler ortaya çıkmaktadır. Sektörlere göre ayrı düzenlemeler çıkarılması veya özel nitelikli kişisel verilerin işlenmesi açısından daha kesin çerçevenin çizilmesini sağlayacak düzenlemelere ihtiyaç bulunmaktadır. • Toplumun daha fazla korumaya muhtaç kesimleri (yaşlılar, çocuklar gibi) bakımından kişisel verilerinin işlenmesi için Kanun içine hükümler eklenerek veya Yönetmeliklerde bu hususa yer vererek ayrıca hükümler düzenlenebilir.
Önleme, tespit ve müdahale güvenlik üçlüsü: Güvenlik yazılımları, donanımları ve benzeri sistemleri yüksek seviyede koruma sağlamalı, denetim mekanizması büyük önem teşkil etmektedir. Uzun vadeli stratejiler belirlenerek bilgi güvenliği ihlâllerine karşın mücadele yöntemleri geliştirilmelidir.	**Kanun uygulanmasında yeknesaklık sağlanması:** Uygulamada mevzuatın kapsamı (Kanunda sayılan istisnalar hariç olmak üzere) özel sektör ve kamu sektörü için uygulanarak her iki sektör için de aynı yükümlülükler söz konusu olmalıdır.

TEKNİK	YASAL VE EĞİTİM
Veri ekonomisinin sağlanması: Tutulan kişisel verilerin boyutlarının büyüklüğü ve saklama süresi dolayısıyla saklanmaları sıkıntı yaratabilir. Verilerin saklanması bakımından verilerin boyutlarının küçültülmesi suretiyle en güvenilir şekilde saklanması için veri tabanı sistemleri oluşturulabilir.	**Bilinçlendirme çalışmaları:** Kişisel verilerin önemini ve kişisel verilerin işlenmesi ihlâllerinde oluşabilecek riskler hakkında gerek ilgili kişiler gerek veri sorumluları ve işleyenlerin bilinçlendirilmesi gerekmektedir. Bilinçlendirme gerçekleşmeden yasal düzenlemelerin ve teknik önlemlerin de bir anlamı kalmamaktadır. Kişiler kişisel verilerini paylaşmanın yaratacağı riskler hakkında bilgi sahibi olmadığı için kimlik bilgileri, ikametgâh ve telefon numaraları gibi kişisel verilerini kolayca ifşa edebilmektedir. Kişisel verilerin önemini vurgulayan kamu spotu reklamları yayınlanarak vatandaşlar bilgilendirilebilir.
Fiziksel güvenliğe önem verilmesi: Kişisel verilerin tutulduğu kayıtlar fiziksel olarak güvenlikli ortamda tutulmalıdır. Öncelikle, veri kayıt sisteminin parçası olmak kaydıyla, otomatik olan veya olmayan yollarla tutulan kişisel verilerin saklandığı veri kayıt sistemleri deprem, sel gibi doğal afet ve yangın gibi olağanüstü durumlara karşı gerekli önlemlerin alındığı, hırsızlığa karşı yüksek güvenlikli ortamlarda tutulmalıdır. Veri sorumlularının ve işleyenlerin işledikleri kişisel verileri kullanarak gerçekleştirdikleri işlemleri başkalarının erişemeyeceği bir şekilde gerçekleştirmeleri gerekmektedir Veri kayıt sistemleri korunaklı olarak muhafaza edilmelidir.	**Eğitim verilmesi:** İlkokul ve liselerde çeşitli konularda seçmeli dersler mevcuttur. Bilişim toplumunda yaşanılması sebebiyle bilişim alanlarında seçmeli dersler verilerek ilkokuldan itibaren kişilerin bilinçlendirilmesinde büyük katkı sağlanabilir. Özellikle telefon üzerinden kısa mesajlar veya kişilerin aranması yoluyla kişilerin kişisel verileri elde edilmektedir. Kişiler, bilişim sistemleri aracılığıyla kolayca dolandırılabilmektedir. Eğitimin ilk dönemlerinden itibaren kişiler kişisel verilerin önemi hakkında eğitim görerek dolandırıcılığa ve kişisel verilerin çalınmasına büyük derecede engel olunabilir.

TEKNİK	YASAL VE EĞİTİM
Büyük veri ve yapay zekâ: Büyük veri, kişisel verilerin işlenmesi bakımından da bğyğk önem taşımaktadır. Büyük veri çalışmalarına ağırlık verilerek kişisel verilerin saklanması açısından önem kazanacaktır.	**Multidisipliner alanlar arasında yardımlaşma ve eğitim:** Veri sorumlularının yükümlülükleri göz önünde bulundurulduğunda hem teknik hem hukuki çerçeveden yükümlülükleri bulunmaktadır. Sadece hukukçular veyahut sadece teknik donanıma sahip mühendislerin veya uzmanların tekelinde kişisel verilerin korunması mümkün olmayacaktır.
	İhtisas mahkemelerinin kurulması: Kişisel verilerin işlenmesi meselesi hukuki olduğu kadar teknik bir meseleyi de teşkil etmektedir. Her ne kadar hâkimler teknik bilgi gerektiren hususlarda bilirkişiye başvursa da, bilişim alanında çıkan tüm uyuşmazlıklar bakımından ihtisas mahkemeleri kurularak bu konuda hukuki ve teknik donanıma sahip hakimler tarafından uyuşmazlıklar çözülmelidir.
	Büyük veri ve yapay zekâ: Büyük veri, kişilerin durumlarına ve davranış yapılarına ilişkin verileri de içermektedir, bunun sonucunda da özel nitelikli kişisel verileri de kapsamına almaktadır. Büyük veri, doğru amaçlarla kullanılırsa yeni kurumsal ve toplumsal olanaklara fırsatlar sağlayacaktır. Bu çerçevede, kişisel verilerin işlenmesi ilkelerinin çizdiği sınırlar çerçevesinde büyük veride kişisel verilerin kullanılması sağlanabilir. Yeni gelen teknolojilerle birlikte hukuki çerçeve de uyumlu bir şekilde çizilerek teknoloji ve hukuk arasında dengeli menfaat sağlanmalıdır.

Şekil 4.26 Tez sonucu ve önerilere ilişkin karşılaştırmalı tablo

KAYNAKLAR

[1] **Adalı, E.** (2016). Bilgisayar ve Bilgi Güvenliği Yönetimi, *Bilgisayar ve Bilgi Güvenliği* (s. 29-37). İstanbul : Özkaracan Matbacılık

[2] **Canavan John. E.** (2001). Fundamentals Of Network Security, *Basic Security Concepts*,(s. 1-21) USA: Canavan

[3] **Cole, Dr. E. & Krutz, Dr. R. & Conley, J. W.** (2005). Network Security Bible, *Information System Security Principles* (s. 4-6). Indianapolis : Wiley

[4] **Panko R. R**. (2010). Corporate Computer and Network Security, *The Elements of Cryptography* (2nd ed., s. 107-148). New Jersey: Pearson

[5] **Slay J. & Koronios A.** (2006). Information Technology Security & Risk Management, *Basic Cryptography and Public Key Infastructure* (3rd ed., s. 130-150). Australia: Wiley

[6] **Adalı, E.** (2016). Bilgisayar ve Bilgi Güvenliği Yönetimi, *Şifreleme Yöntemleri* (s. 111-134). İstanbul : Özkaracan Matbacılık

[7] **Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi,** *İstanbul Bilgi Üniversitesi İnsan Hakları Hukuku Uygulama Ve Araştırma Merkezi*, http:// humanrightscenter. bilgi.edu.tr / tr / content/ 157-kisisel-verilerin-otomatik-isleme-tabi tutulmas - karssnda- bireylerin- korunmas-sozlesmesi/ , erişim tarihi 20.10.2017

[8] **108 numaralı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi** (2016). *T.C. Resmi Gazete, 29656*, 17 Mart 2016

[9] **Türkiye Cumhuriyeti Anayasası** (1982). *T.C. Resmi Gazete*, *17863*, 9 Kasım 1982.

[10] **Kişisel Verilerin Korunması Kanunu** (2016). *T.C. Resmi Gazete, 29677*, 7 Nisan 2016

[11] **Kişisel Verilerin Korunması Hakkında Kanun Tasarısı** (2016), http://www2.tbmm.gov.tr/d26/1/1-0541.pdf, Erişim tarihi 20.10.2017

[12] **Kişisel Verileri Koruma Kurumu**, *Kişisel Verilerin Korunması Kanunu ve Uygulaması Kitapçığı* (2017), (s. 12-94)

[13]**Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik** (2012). *T.C. Resmi Gazete, 28363,* 24 Temmuz 2012

[14] **General Data Protection Regulation.** (2016*) Official Journal of the European Union*, 4 Mayıs 2016

[15] **Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik** (2017). *T.C. Resmi Gazete, 30224,* 28 Ekim 2017

[16] **Kişisel Verileri Koruma Kurumu'ndan Veri Sorumluları Sicili Hakkında Yönetmelik Taslağı**, *Kişisel Verileri Koruma Kurumu*, Erişim: 14.11.2017, http://www.kvkk.gov.tr/docs/verisorumlularisicili.pdf

[17] **Kişisel Verileri Koruma Kurumu**, Basın Açıklaması, Erişim: 14.11.2017, http:/www.kvkk.gov.tr/haberverisorumlularisicilibasinaciklamasi.html

[18] **The History of the General Data Protection Regulation.** (t.y.) Erişim: 10 Ekim 2017, https :// edps. europa. eu / data – protection / data protection/ legislation / history – general – data – protection - regulation_en

[19] **Protection of Personal Data.** (24.11.2016) Erişim: 10 Ekim 2017, http://ec.europa.eu/justice/data-protection/index_en.htm

[20] **Maldoff G.** (2016). Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization, *The International Association of Privacy Professionals,* Erişim: 1.11.2017, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/

[21] **Williamson C.** (2017). Pseudonymization Vs. Anonymization And How They Help With GDPR, *Progtegrity*, Erişim: 1.11.2017, http:// www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr/

[22] **Boardman R. & Mullock J. & Mole A.** (2017) Bird&Bird Guide to the General Data Protection Regulation, Erişim: 20.10.2017, https :// www. twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en

[23] **Jolly I.** Data protection in the United States: overview, (t.y.) *Thomson Reuters Practical Law*, Erişim: 3.11.2017, https:// uk. practicallaw. thomsonreuters. com/6-502 0467 ? transition Type = Default & contextData=(sc.Default)&firstPage=true&bhcp=1

[24]**Summary of the Privacy Act,** (t.y.) Erişim: 2.11.2017, https://www.epa.gov/laws-regulations/summary-privacy-act

[25] **Washington Information Directory 2016 – 2017**, (2016). Amerika Birleşik Devletleri CQ Press, https:// books. google. com.tr/ books? id=F2MuDAAAQBAJ&pg=PT1515&dq=privacy+act+usa&hl=tr&sa

=X&ved=0ahUKEwibhNmJwKnXAhVjJsAKHWPmB0wQ6AEIYTAI#v=onepage&q=privacy%20act%20usa&f=false (Orijinali 2016'da basılmıştır)

[26] **Privacy Act, Food Drug Administration**, (t.y.) Erişim: 3.11.2017, https://www.fda.gov/RegulatoryInformation/FOI/PrivacyAct/default.htm

[27] **Lovells H.** (2017). Changes in Japan Privacy Law to Take Effect in Mid-2017; Key Regulator Provides Compliance Insights, Lexology, Erişim: 4 Kasım 2017, https:// www. lexology. com / library / detail. aspx?g= efa0a2b0-b73e-456c-b4fa-26a268e9e751

[28] **Takase K.** (2017). GDPR matchup: Japan's Act on the Protection of Personal Information, IAPP, Erişim: 3.11.2017, https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/

[29] **Han F. & Hu J. & Kotagiri R.** (2011) Advanced Topics In Biometrics, Chapter 19 *Biometric Authentication For Mobile Computing Applications*, s.461-478, www.worldscientific.com

[30] **Önal M.** (2013). *RFID Mimarisi Ve Programlama*, (1. Baskı, s. 241 - 253), İstanbul : Kodlab, Erişim: 5.11.2017, https:// books. google. com.tr/ books?id=DT6nBAAAQBAJ&pg=PA246&dq=biyometrik+veri&hl=tr&sa=X&ved=0ahUKEwjBm6qLyKfXAhUKKcAKHRG1A7gQ6AEIOzAE#v=onepage&q=biyometrik%20veri&f=false

[31] **Satapathy S. C. & Joshi A**. (2017). Information and Communication Technology for Intelligent Systems (ICTIS 2017), Bhatnagar S. *Cooperative Multimodal Approach for Identification* – (Volume 1, s. 13-18), Erişim: 5.11.2017, https:// books. google. com. tr/ books? İd = 0BUwDwAAQBAJ&printsec=frontcover&dq=%C4%B1nformation+and+communication+technology+for+intelligent+systems&hl=tr&sa=X&ved=0ahUKEwjFuIv38_fXAhXDXhQKHThjCpIQ6AEIKDAA#v=onepage&q=%C4%B1nformation%20and%20communication%20technology%20for%20intelligent%20systems&f=false

[32] **Eye Biometrics** (t.y.), MIS Biometrics, Erişim: 4.11.2017, http:// misbiometrics.wikidot.com/eye

[33] **Fingerprinting Criticisms.** (t.y.), Erişim: 4.11.2017, http:// www.fingerprinting. com/fingerprinting-criticism.php.

[34] **Wilson T.V.** (t.y.), How Stuff Works : "How Biometrics Works: Voiceprints". Erişim: 5.11.2017, http://science.howstuffworks.com/biometrics3.htm

[35] **Arslan B. & Sağıroğlu Ş.** (2016). Mobil Cihazlarda Biyometrik Sistemler Üzerine Bir İnceleme, Politeknik Dergisi, 2016; 19 (2); (s. 101-114)

[36] **Çam O.** (2016, 23 Mart) Parmak izi ile Giriş özelliği İşCep uygulamasından kaldırıyor. *Esesrehber. Com*, Erişim adresi https:// www. esesrehber. com/parmak-izi-ile-giris-ozelligi-iscep-uygulamasindan-kaldiriyor/

[37] **Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ** (2007). *T.C. Resmi Gazete, 26643*, 14 Eylül 2007

[38] **Banka Kartları Ve Kredi Kartları Kanunu** (2006). *T.C. Resmi Gazete, 26095*, 23 Şubat 2006

[39] **Bankaların İç Sistemleri Ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik** (2014). *T.C. Resmi Gazete, 29057*, 11 Temmuz 2014

[40] **Bankacılık İşlemlerinde Şifre Git Gide Yok Oluyor.** (2016, 13 Mart). *Bthaber.com*, Erişim Adresi: http://www.bthaber.com/biyometri-ve-guvenlik/bankacilik-islemlerinde-sifre-git-gide-yok-oluyor/1/17602

[41] **Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelik** (2016). *T.C. Resmi Gazete, 29863*, 20 Ekim 2016

[42] **Sağlık Bakanlığı** (t.y.) Bilgi Güvenliği Politikaları Yönergesi Ve Kılavuzu, Erişim: 5.11.2017, https://bilgiguvenligi.saglik.gov.tr/Home/Mevzuat

[43] **Sosyal Sigortalar Ve Genel Sağlık Sigortası Kanunu** (2006). *T.C. Resmi Gazete, 26200*, 31 Mayıs 2006

[44] **Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliği** (2013). *T.C. Resmi Gazete, 28597*, 24 Mart 2013

[45**] Sosyal Güvenlik Kurumu Başkanlığı Biyometrik Yöntemlerle Kimlik Doğrulama Sistemlerine Ait Kılavuz** (2013). Erişim: 1 Kasım 2017, http://www.sgk.gov.tr/wps/wcm/connect/0900dd23-85c3-4af9-b3de-ae43a81f3543/Duyuru_30042013.pdf?MOD=AJPERES&CACHEID=0900dd23-85c3-4af9-b3de-ae43a81f3543

[46] **Medula Hastane.** (t.y). Erişim: 3.11.2017, http://medulamedula.com/medula-hastane

[47] **Mortek Teknoloji**, Biyometrik kimlik Kaydı Sık Sorulan Sorular (t.y.) Erişim: 4.11.2017, http://www.mortek.com.tr/Sayfalar/Sik-Sorulan-Sorular/30

[48] **Nüfus Hizmetleri Kanunu** (2006). *T.C. Resmi Gazete, 26153*, 29 Nisan 2006

[49] **Wessing T.** (2016). Health data and data privacy: challenges for data processors under the GDPR, Erişim: 12.9.2017, https://united-kingdom. taylor wessing.com/globaldatahub/article-health-data-privacy-under-gdpr. ht ml

[50] **Biometric data and the General Data Protection Regulation** (2017). Erişim: 19.9.2017, http://www.gemalto.com/govt/biometrics/biometric-data

[51] **Narin B.** (2017, 7 Ağustos) Büyük Veri ve Yoğun Veri kucaklaşıyor. Journo.com, Erişim: 13 Kasım 2017, Erişim adresi: https://journo.com.tr/buyuk-veri-yogun-veri-kucaklasiyor

[52] **Ilıcak A.** (2016, 10 Şubat) Büyük veri işliyoruz derken aman kişisel verileri ihlal etmeyin. Dunya.com, Erişim: 13 Kasım 2017, Erişim adresi: https://www.dunya.com/kose-yazisi/buyuk-veri-isliyoruz-derken-aman-kisisel-verileri-ihlal-etmeyin/27093

[53]**Aybay İ.** (t.y.) Büyük Verinin İki Yüzü. TÜSİAD. Erişim: 13 Kasım 2017, Erişim adresi: http:// tusiad. org / tr /fikir – ureten – fabrika / item / 8348-buyuk-verinin - iki-yuzu

[54] **Eralp Özgür** (2017, 11 Kasım) Bilişim Hukuku Kararları. Eralp.av.tr, Erişim: 13 Kasım 2017, Erişim adresi: http://www.eralp.av.tr/danistay-11-daire-baskanligi-2017816-esas-20174906-karar-tarihi-13-06-2017/

[55] **Greenleaf G.** (2017). Global Tables of Data Privacy Laws and Bills (5th Ed 2017), Privacy Laws & Business International Report, 14-26, Erişim: 15.11.2017, Erişim adresi: https:// papers. ssrn. com /sol3/papers.cfm?abstract_id=2992986.

EKLER

EK A: ANKET SORULARI

Kişisel Veri Düzenlemeleri (Biyometrik Veriler)

Bu anket formu, özellikle biyometrik veri kullanan sektörlerde hizmet veren kişilerin kişisel veri mevzuatına ilişkin farkındalıklarının ölçülmesini, görüş ve önerilerinin alınmasını sağlamak amacıyla oluşturulmuştur. Mevzuatımız; kişisel verileri genel ve özel nitelikli (hassas) olarak iki kategoride toplamıştır. Bu çerçevede, 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 mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. Biyometrik veriler, gerek ülkemizde gerek Avrupa Birliği'nde hassas veri niteliğinde olup korunmaktadır. Dijital çağın hayatımıza girmesiyle birlikte biyometrik veriler sağlık, bankacılık, haberleşme, otomotiv, güvenlik ve benzeri gibi çeşitli sektörlerde kullanılmaktadır. Biyometrik veri kişiye özgü olup benzersizdir ve parmak izi, yüz tanıma, iris tanıma, ses tanıma gibi türleri vardır. İlerleyen yıllarda kırılması kolay olan şifreler yerine daha güvenilir, kompleks ve kırılması zor olan biyometrik verilerin alması düşünülmektedir. Bu çerçevede, biyometrik verilerin kopyalanmaması ve güvenli bir şekilde depolanması çok büyük önem arz etmektedir.

Anketin amacı, özellikle biyometrik veri kullanan sektörlerde (biyometrik veri konusunda hizmet verenler, işçi-işveren ilişkisi kapsamında biyometrik verilerin toplanması, hayatın herhangi bir alanında biyometrik veri kullanımının söz konusu olması vb) hizmet veren kişilerin kişisel veri mevzuatına ilişkin farkındalıklarının ölçülmesini, görüş ve önerilerinin alınmasını sağlamak ve çözüm önerileri geliştirmek için veri toplamaktır.

Bölüm 0

Bu kısımda katılımcılara ve çalışmakta olduğu kurumlara (kamu tüzel kişiliği/şirket vb.) ilişkin kısa sorular yer almaktadır.

Aşağıdaki bölümlerde de, eğer emekliyseniz veyahut çalışmıyorsanız ilgili sorularda "emekliyim" ve "şu anda çalışmıyorum" seçeneklerini işaretleyebilirsiniz.

Aşağıdaki yaş aralıklarından hangisindesiniz? *

- ○ 18 - 24
- ○ 25-34
- ○ 35-44
- ○ 45-54
- ○ 55+

Cinsiyetiniz nedir? *

- ◯ Kadın
- ◯ Erkek

Öğrenim durumunuz? *

- ◯ İlköğretim
- ◯ Lise
- ◯ Lisans
- ◯ Yüksek Lisans
- ◯ Doktora
- ◯ Diğer...

Çalıştığınız Kuruluşunuzun bünyesinde yaklaşık kaç kişi istihdam edilmektedir? (Emekliyseniz ya da çalışmıyorsanız aşağıdaki ilgili şıkları da işaretleyebilirsiniz)

- ◯ 1-10
- ◯ 10-30
- ◯ 30-50
- ◯ 50-100
- ◯ 100+
- ◯ Emekliyim
- ◯ Şu anda çalışmıyorum
- ◯ Diğer...

Çalıştığınız, çalışmıyorsanız uzmanlık alanınız veya emekli olduysanız daha önce çalışmış olduğunuz kuruluş hangi sektör/lerde hizmet vermektedir? (Birden fazla da işaretlenebilir)

- [ ] Sağlık
- [ ] Bankacılık
- [ ] Haberleşme
- [ ] Ulaşım
- [ ] Otomotiv
- [ ] Güvenlik
- [ ] Eğitim
- [ ] Bilişim - Mühendislik vb.
- [ ] Hukuk
- [ ] Diğer...

Bölüm 1

Mevzuata ilişkin farkındalık soruları içermektedir.

Kişisel Verilerin Korunması Hakkında Kanun ile ilgili herhangi bir bilginiz var mıdır?

- ( ) Düzenlemeyi duydum, içeriğini yeterince biliyorum.
- ( ) Düzenlemeyi duydum; ancak içeriğini yeterince bilmiyorum.
- ( ) Düzenlemeyi duymadım, içeriği hakkında bilgim yok.

Mevzuattan haberdar iseniz, Kişisel Verilerin Korunması Hakkında Kanun'un beklentilerinizi karşıladığını düşünüyor musunuz? (Mevzuattan haberdar değilseniz bu soruyu geçiniz)

- ○ Evet, tam anlamı ile eksiksiz bir düzenleme olmuştur.
- ○ Hayır, beklentileri karşılamamaktadır.
- ○ Eksiklikler mevcut olmakla beraber beklentileri karşılamaktadır.
- ○ Diğer...

Kişisel verilerin korunmasında yalnızca yasal düzenlemenin yeterli olacağını düşünüyor musunuz?

- ○ Evet
- ○ Hayır
- ○ Belki

Kişisel verilerin korunması için aşağıdakilerden hangisi (hangileri) gereklidir? * (Birden fazla seçenek işaretleyebilirsiniz)

- ☐ Yasal düzenleme
- ☐ Yönetmelik düzenlemesi
- ☐ Teknik bağlamda fiziksel güvenliğin sağlanması
- ☐ İdari bağlamda hukuki olarak ağır yaptırımlar getirilmesi ve bu kapsamda veri sorumlularının titizlikle çalışması
- ☐ Kurumlararası işbirliği ile politikalar benimsenmesi ve kişisel verilerin korunması hususunda yeknesaklık sağlanması
- ☐ Diğer...

Kurumunuzda Kişisel verilerin korunması mevzuatına uyum sağlamak için hangi çalışmalar yapılmaktadır? (Birden fazla seçenek işaretleyebilirsiniz)

- [ ] Eğitim verilmiştir.
- [ ] Mail gönderilmek suretiyle vb. bilgilendirme yapılmıştır.
- [ ] Veri işleyen tayin edilerek kişisel verileri korumak için gereken stratejiler belirlenmiştir
- [ ] Hiçbiri
- [ ] Bir fikrim yok
- [ ] Şu anda çalışmıyorum
- [ ] Emekliyim
- [ ] Diğer...

Mevzuata uyum süreci kapsamında, kurumunuzda veri sorumlusu (veri sorumlusu, kişisel verilerin işlenme araçlarını ve amaçlarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumludur ve gerçek veya tüzel kişi olabilirler) ve veri işleyen (veri sorumlusunun verdiği yetki ile kişilerin kişisel verilerini işleyecek gerçek kişi veya tüzel kişi/ler) belirlenebildi mi? *

- ( ) Evet
- ( ) Hayır
- ( ) Belirlenmesine çalışılıyor
- ( ) Bir fikrim yok
- ( ) Şu anda çalışmıyorum
- ( ) Emekliyim
- ( ) Diğer...

Mevzuat uyarınca veri sorumlusunun yükümlülüklerini nasıl değerlendiriyorsunuz?

- ( ) Çok ağır
- ( ) Uygulanabilir değil
- ( ) Bir fikrim yok

Yukarıdaki soruya verdiğiniz yanıt "çok ağır" veya "uygulanabilir değil" ise nedenlerini açıklayabilir misiniz?

Uzun yanıt metni

Kurumlarda sizce veri işleyen nasıl belirlenmelidir? *

- ○ Hukuk ve Teknik kişilerden oluşan bir grup olmalı
- ○ Sadece bilgi işlemci olmalı
- ○ Diğer...

Veri sorumlusunun ve veri işleyenin kişisel verileri işlenen kişileri (ilgili kişi) aydınlatma yükümlülüğü bulunmaktadır. Bu kapsamda, aydınlatma yükümlülüğü ile ilgili hangi seçenek kuruluşunuzun mevcut uygulamasını en iyi açıklamaktadır?

- ○ Evet, aydınlatma yükümlülüğüne ilişkin çalışma yürütülmektedir
- ○ Hayır, aydınlatma yükümlülüğüne ilişkin herhangi bir çalışma yürütülmemektedir
- ○ Henüz çalışma yapılmadı; ancak ilerleyen zamanlarda yapılması yönünde hazırlıklar yapılmaktadır.
- ○ Bir fikrim yok
- ○ Şu anda çalışmıyorum
- ○ Emekliyim

Kişisel verilerinin hukuka aykırı işlenmesi durumunda İlgili kişinin haklarından olan Veri sorumlusuna başvuru kavramı ile ilgili bilginiz var mı?

- ○ Evet, biliyorum
- ○ Hayır, bilmiyorum

Kişisel verilerin işlenmesi ile ilgili hukuka aykırı bir durum oluştuğunda veri sorumluları bakımından ağır idari ve mali yaptırımlar söz konusudur. Bu konuda herhangi bir bilgilendirme yapıldı mı? *

- ○ Evet
- ○ Hayır
- ○ Bir fikrim yok
- ○ Şu anda çalışmıyorum
- ○ Emekliyim

Yukarıda soruya "Evet" işaretlediyseniz veya konu hakkında bilgi sahibi iseniz, (Yukarıdaki soruya evet dışında işaretleyenler bu soruyu pas geçebilir) kişisel verilerin işlenmesi ile ilgili hukuka aykırı bir durum oluştuğunda öngörülen ağır idari ve mali yaptırımlar hakkında görüşleriniz ve önerileriniz nelerdir?

Uzun yanıt metni

Bölüm 2

Güvenlik ve verilerin işlenmesi ihlali durumunda alınacak ihlal öncesi ve sonrasına ilişkin önlemler ile ilgili sorular içermektedir.

Kuruluşunuzda veri güvenliğini sağlamak için ne tür güvenlik ürünleri kullanılmaktadır? (Birden çok seçeneği işaretleyebilirsiniz)

- ☐ Yazılım programları
- ☐ Donanımsal programlar
- ☐ Buluttan hizmet almak
- ☐ Antivirüs programları
- ☐ Bir fikrim yok/Bilmiyorum
- ☐ Emekliyim
- ☐ Şu anda çalışmıyorum
- ☐ Diğer...

Veri güvenliğini sağlamak için sistemlerinizde periyodik kontrol ne kadar sıklıkta yapılmaktadır?

- ◯ Haftada bir
- ◯ İki haftada bir
- ◯ Ayda bir
- ◯ İki ayda bir
- ◯ Periyodik kontrol yapılmamaktadır
- ◯ Bir fikrim yok/Bilmiyorum
- ◯ Emekliyim
- ◯ Şu anda çalışmıyorum
- ◯ Her gün düzenli kontroller yapılmaktadır.
- ◯ Diğer...

Kuruluşunuzda veri güvenliğinin korunması için yeterli önlemlerin alındığına inanıyor musunuz?

- ◯ Evet
- ◯ Hayır
- ◯ Şu anda çalışmıyorum
- ◯ Emekliyim
- ◯ Bir fikrim yok
- ◯ Diğer...

Kuruluşunuzda hiç veri güvenliği ihlâli yaşandı mı? *

- ○ Hiç yaşanmadı
- ○ Bir fikrim yok/Bilmiyorum
- ○ Sık sık
- ○ Bazen
- ○ Şu anda çalışmıyorum
- ○ Emekliyim
- ○ Diğer...

Veri ihlâlleri yaşanıyor ise bu ihlâller ne gibi sebeplerden ötürü yaşanmaktadır? (Birden fazla da işaretleyebilirsiniz)

- ☐ Siber saldırılar (DDoS, DoS, Truva atı, vb)
- ☐ Personel hataları - kusurları
- ☐ Sermaye yetersizliği sebebiyle sistemlerin korunması için yeterli teknik donanımın sağlanmaması
- ☐ Yanlış uygulama
- ☐ Sistemin hacklenmesi suretiyle verilerin elde edilmesi
- ☐ Şu anda çalışmıyorum
- ☐ Emekliyim
- ☐ Bir fikrim yok/Bilmiyorum
- ☐ Diğer...

Bölüm 3

Anketimizin son kısmında, kişisel verilerin ve biyometrik verilerin korunmasına yönelik izlemiş olduğunuz politikalara ilişkin sorular yer almaktadır.

Herhangi bir kişi ya da kuruma ne tür biyometrik veri verdiniz? (Birden fazla seçenek de işaretleyebilirsiniz) *

- [ ] Vermedim
- [ ] Parmak izi
- [ ] Damar haritası
- [ ] İris
- [ ] Yüz tanıma
- [ ] Diğer...

Biyometrik verinizi hangi Kuruma verdiniz? (Birden fazla seçenek işaretleyebilirsiniz)

- [ ] Vermedim
- [ ] Emniyet Genel Müdürlüğü (pasaport, yeni ehliyet kartları)
- [ ] Hastaneler (avuç içi tarama yöntemi vb)
- [ ] İş yeri (işe giriş-çıkışlarda parmak izi okutma vb)
- [ ] Ev güvenlik sistemi
- [ ] Bankalar (İnternet Bankacılığı vb)
- [ ] Nüfus Müdürlüğü, İçişleri Bakanlığı (yeni kimlik kartları)
- [ ] Diğer...

Biyometrik verilerinizin işlenmesi ve sahip olduğunuz haklarınız ile ilgili tarafınıza herhangi bir bilgilendirme yapıldı mı?

- ○ Biyometrik veri vermedim
- ○ Bilgilendirme yapıldı
- ○ Bilgilendirme yapılmadı
- ○ Diğer...

Biyometrik verilerin en güvenli biçimde korunabilmesi için ne tür önlemlerin alınması gerektiğine inanıyorsunuz? (Birden fazla seçenek de işaretleyebilirsiniz)

- ☐ Veri işleyici-sorumlusunun eğitimi
- ☐ İlgili kişi ve veriye ulaşma yetkisi olanların farkındalığının artırılması
- ☐ Hukuki düzenlemeler ile
- ☐ Teknik destek - önlemlerin alınması ve bu suretle en üst düzey korumanın sağlanması
- ☐ Diğer...

Biyometrik verilerle ilgili Kuruluşunuzun yürütmüş olduğu çalışmalar var mı? Varsa bunlar nelerdir? (Birden fazla seçenek işaretleyebilirsiniz)

- ☐ Parmak izi
- ☐ Ses tanıma
- ☐ Göz tarama, iris tarama
- ☐ Biyometrik verilere ilişkin projeler, eğitimler
- ☐ Herhangi bir çalışma yürütülmemektedir
- ☐ Şu anda çalışmıyorum
- ☐ Emekliyim
- ☐ Biyometrik veri işlenmiyor
- ☐ Diğer...

Kuruluşunuzda genel itibariyle kişisel verilerin ve biyometrik veriler de işleniyorsa biyometrik verilerin güvenli olarak saklanması/işlenmesi için ne yapılmaktadır? (birden fazla seçeneği işaretleyebilirsiniz)

- [ ] Çalışanlar eğitilmektedir
- [ ] Sistemlerin periyodik bakımı yapılmaktadır
- [ ] Gerektiğinden fazla veri talep edilmemektedir
- [ ] Eğitim - bilgilendirme yapılmaktadır
- [ ] Emekliyim
- [ ] Şu anda çalışmıyorum
- [ ] Diğer...

6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun uyarınca düzenlenen konular ile ilgili ikincil düzenlemeler de yapılacaktır. Bu çerçevede düzenleme yapılmasına ihtiyaç olduğunu düşündüğünüz başlıklar nelerdir? (Birden fazla seçenek de işaretleyebilirsiniz, ilave görüşünüz varsa "diğer" şıkkını tıklayarak görüşünüzü belirtebilirsiniz) (Not: 28.10.2017 tarihi itibari ile kişisel verilerin silinmesi, anonimleştirilmesi, yok edilmesi ile ilgili Yönetmelik yayımlanmıştır.) *

- [ ] Kişisel verilerin işlenmesi, anonimleştirilmesi, yok edilmesi, silinmesi işlemleri
- [ ] Veri sicili ve veri sorumlularının yükümlülüklerine ilişkin detaylı düzenlemeler
- [ ] Özel nitelikli kişisel verilerin daha kapsamlı düzenlenmesi (sektörel bazda ayrı düzenlemeler de söz konusu olabilir)
- [ ] Diğer...

EK B: DÜNYA'DAKİ KİŞİSEL VERİ DÜZENLEMELERİNE İLİŞKİN ÖRNEK ÇİZELGE [55]

(OCAK 2017'de güncellenmiştir)

Çizelge B.1: Dünya'daki kişisel veri düzenlemelerinden kesitler

Ülke	Kişisel Veri Düzenlemeleri	İlk Hali (Yıl)	Son Hali (Yıl)	Bölge	Sektör	Kişisel Verileri Koruma Kurumu Adı
Angola	Lei da Protecção de Dados Pessoais	2011	2011	Afrika	Kamu + Özel	Agência da Protecção de Dados
Güney Kore	Personal Information Protection Act 2011	1994	2015	Asya	Kamu + Özel	Personal Information Protection Commission; Korea Information Security Agency; Korea Communications Commission
Hong Kong	Personal Data Privacy Ordinance	1995	2012	Asya	Kamu + Özel	Privacy Commissioner for Personal Data
Zimbambwe	Access to Information and Protection of Privacy Act	2002	2002	Afrika	Kamu + Özel	Media and Information Commission
Nepal	Right to Information Act	2007	2007	Asya	Kamu	National Information Commission
Malezya	Personal Data Protection Act	2010	2013	Asya	Özel	Personal Data Protection Commissioner
Tayland	Official Information Act 1997	1997	1997	Asya	Kamu	Official Information Commission
Filipinler	Data Privacy Act	2012	2012	Asya	Kamu + Özel	National Privacy Commission
Singapur	Personal Data Protection Act	2012	-	Asya	Özel	Personal Data Protection Commission
Bahamalar	Data Protection (Privacy of Information) Act	2003	2003	Karayipler	Kamu + Özel	Data Protection Commissioner
Avustralya	Privacy Act 1988	1988	2012	Avustralya	Kamu + Özel	Office of the Australian Information Commissioner
Yeni Zellanda	Privacy Act 1993	1993	2010	Avustralya	Kamu + Özel	Privacy Commissioner (Te Mana Matapono Matatapu)
Vietnam	Law on Protection of Consumers' Rights	2010	2010	Asya	Özel	Henüz kurulmadı.
Bermuda	Personal Information Protection Act	2016	2016	Karayipler	Kamu + Özel	Henüz oluşturulmadı. (Privacy Commissioner)
Kazakistan	Law on Personal Data	2013	2015	Merkez Asya	Kamu + Özel	Committee on Communication, Informatisation and Information
Avusturya	Datenschutzgesetz	1978	2013	Avrupa (AB)	Kamu + Özel	Data Protection Commission (Datenschutzkommission)

Ülke	Kişisel Veri Düzenlemeleri	İlk Hali (Yıl)	Son Hali (Yıl)	Bölge	Sektör	Kişisel Verileri Koruma Kurumu Adı
Çek Cumhuriyeti	Personal Data Protection Act	1992	2000	Avrupa (AB)	Kamu + Özel	Office for Personal Data Protection (Urad Pro Ochranu Osobnich Udaju)
Danimarka	Act on Processing of Personal Data	1978	2000	Avrupa (AB)	Kamu + Özel	Data Protection Agency (Datatilsynet)
Estonya	Data Protection Act	2003	2003	Avrupa (AB)	Kamu + Özel	Data Protection Inspectorate (Andmekaitse Inspektsioon)
Almanya	Federal Data Protection Act	1977	2015	Avrupa (AB)	Kamu + Özel	Federal Data Protection Commissioner (Bundesbeauftragten für den Datenschutz)
Yunanistan	Law on the Protection of individuals with regard to the processing of personal data	1997	2011	Avrupa (AB)	Kamu + Özel	Hellenic Data Protection Authority (ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ)
Fransa	Law relating to the protection of individuals against the processing of personal data	1978	2014	Avrupa (AB)	Kamu + Özel	Data Protection Commission (Commission Nationale de l'Informatique et des Libertés)
Finlandiya	Personal Data Act	1987	2000	Avrupa (AB)	Kamu + Özel	Data Protection Ombudsman (Tietosuojavaltuutetun Toimisto)
Macaristan	Act on Informational Self-Determination and Freedom of Information	1992	2011	Avrupa (AB)	Kamu + Özel	National Authority for Data Protection and Freedom of Information
İrlanda	Data Protection Act	1998	2003	Avrupa (AB)	Kamu + Özel	Data Protection Commissioner (An Coimisinéir Cosanta Sonraí)
İtalya	Consolidation Act regarding the Protection of Personal Data	1996	2013	Avrupa (AB)	Kamu + Özel	Data Protection Commission (Garante per la protezione dei dati personali)
Letonya	Law on Protection of Personal Data of Natural Persons	2000	2014	Avrupa (AB)	Kamu + Özel	State Data Inspectorate (Datu Valsts Inspekcija)
Lüksemburg	Data Protection Law	1979	2007	Avrupa (AB)	Kamu + Özel	National Data Protection Commission (Commission nationale pour la protection des données)
Hollanda	Personal Data Protection Act	1988	2015	Avrupa (AB)	Kamu + Özel	Data Protection Authority (Autoriteit Persoonsgegevens)
Litvanya	Law on Legal Protection of Personal Data	1996	2011	Avrupa (AB)	Kamu + Özel	State Data Inspectorate (Valstybine Duomenu Apsaugos Inspekcija
Malta	Data Protection Act	2001	2001	Avrupa (AB)	Kamu + Özel	Data Protection Commissioner
Portekiz	Lei da proteçao de dados pessoais	1991	1998	Avrupa (AB)	Kamu + Özel	National Data Protection Commission (Comissão Nacional de Protecção de Dados)
Polonya	Act on the Protection of Personal Data	1997	2016	Avrupa (AB)	Kamu + Özel	Inspector General for Personal Data Protection (Generalny Inspektor Ochrony Danych Osobowych)

Ülke	Kişisel Veri Düzenlemeleri	İlk Hali (Yıl)	Son Hali (Yıl)	Bölge	Sektör	Kişisel Verileri Koruma Kurumu Adı
Romanya	Law on the protection of individuals with regard to the processing of personal data etc	2001	2005	Avrupa (AB)	Kamu + Özel	National Supervisory Authority for Personal Data Protection (Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal)
Slovakya	Act on the Protection of Personal Data	1992	2013	Avrupa (AB)	Kamu + Özel	Inspection Unit for the Protection of Personal Data
İspanya	Ley Orgánica de Protección de Datos de Carácter Personal	1992	1999	Avrupa (AB)	Kamu + Özel	Data Protection Commissioner (Agencia de Protección de Datós)
İsviçre	Data Protection Act	1992	2006	Avrupa (AB)	Kamu + Özel	Federal Data Protection and Information Commissioner
Türkiye	6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun	2016	2016	Avrupa	Kamu + Özel	Kişisel Verileri koruma Kurumu
Şili	Privacy Law	1999	2012	Latin Amerika	Kamu + Özel	Servicio de Registro Civil
Kolombiya	Data Protection Law	2008	2012	Latin Amerika	Kamu + Özel	Superintendence of Industry and Commerce
Bulgaristan	Law for Protection of Personal Data	2002	2011	Avrupa (AB)	Kamu + Özel	Commission for Personal Data Protection (Комисия за защита на личните данни)
Hırvatistan	Act on Personal Data Protection	2003	2011	Avrupa (AB)	Kamu + Özel	Data Protection Agency
Kıbrıs	The Processing of Personal Data (Protection of the Individual) Law	2001	2012	Avrupa (AB)	Kamu + Özel	Personal Data Protection Commissioner
Belçika	Law on Privacy Protection in relation to the Processing of Personal Data	1992	2011	Avrupa (AB)	Kamu + Özel	Privacy Commission (Commission de la vie privée)

ÖZGEÇMİŞ

Ad-Soyad **:** Göksu Hazar ERDİNÇ

Doğum Tarihi ve Yeri **:** Ankara, 01.01.1991

E-posta **:** erdincg@itu.edu.tr

ÖĞRENİM DURUMU:

- **Lisans** **:** 2013, Bilkent Üniversitesi, Hukuk Fakültesi, Hukuk

MESLEKİ DENEYİM VE ÖDÜLLER:

- 2014 yılında avukatlığa başladı. Bilişim hukuku, tahkim, ticaret hukuku, iş hukuku, borçlar hukuku gibi konular üzerinde çalıştı.
- 2015 yılında İstanbul Teknik Üniversitesi Bilişim Enstitüsü bünyesinde Bilişim Uygulamaları anabilim dalında yüksek lisans yapmaya başladı.
- 2015 yılında araştırma görevlisi olarak İstanbul Teknik Üniversitesi Bilişim Enstitüsü'nde çalışmaya başladı.

  .

TEZDEN TÜRETİLEN YAYINLAR/SUNUMLAR:

- **Erdinç G.H., Karaçuha E.** 2017. Kişisel Verilerin Korunmasında Mevcut Durum ve Öngörüler, Türkiye 22. İnternet Konferansı, 2 Kasım 2017, İstanbul, Türkiye