Türkiye'de Kişisel Verilerin Korunması ve Vatandaş Algısının Ölçülmesi

Araştırma Makalesi/Research Article

Sündüs ARINMIŞ UZUN

Adli Bilişim Anabilim Dalı, Bilişim Enstitüsü, Gazi Üniversitesi, Ankara, Türkiye
arinmis.sundus@gmail.com
(Geliş/Received:11.05.2020; Kabul/Accepted:05.05.2021)
DOI: 10.17671/gazibtd.735471

Özet— Kişisel veri kavramı ve kişisel verilerin korunması konusu ülkemizde son yıllarda oldukça gelişim göstermiştir. Dünya genelinde meydana gelen ilerlemeler ve tartışmalar doğrudan ülkemizdeki gündemi etkilemektedir. Analitik Hiyerarşi Süreci modeli ayrıştırma, yargıların karşılaştırılması ve önceliklerin sentezi şeklinde üç ana ilke üzerine kurulmuştur. Model kriterlerin önem derecelerinin hesaplanmasını ve alternatifler arasından seçim yapılmasını kolaylaştırmaktadır. Bu çalışmanın amacı, ülkemizde kişisel verilerin işlenmesi ve korunmasına yönelik kavramsal bilgi vermek, konu ile ilgili dünyada ve ülkemizdeki gelişimi hakkında genel bir çerçeve çizmek, son yıllarda gündem olan big data (büyük veri) kavram ve uygulamalarıyla kişisel verilerin korunması ilişkisini incelemek ve son olarak kişisel verilerin işlenmesi ve korunması konusunda vatandaş algısının ölçülerek uygulanması gereken politika hakkında öneriler sunmaktadır. Bu amaçlardan yola çıkarak kişisel verilerin işlenmesi ve korunması konusunda vatandaş algısını ölçmek için beş ana kriter, yirmi alt kriter belirlenmiş ve hiyerarşik yapı oluşturulmuştur. Çalışmanın sonunda kişisel verilerin işlenmesi ve korunması konusunda en önemli kriterin gereklilik olduğu ve güvenilirlik yoğun politikanın seçilmesinin uygun olacağı değerlendirilmektedir.

Anahtar kelimeler- Kişisel veri, kişisel verilerin korunması, vatandaş algısı, analitik hiyerarşi süreci.

Measuring The Protection of Personal Data and Perception of Citizens in Turkey

Abstract— The concept of personal data and the protection of personal data has improved considerably in our country in recent years. Progresses and discussions around the world directly affect the agenda in our country. The Analytical Hierarchy Process model is based on three main principles: decomposition, comparison of judgments and synthesis of priorities. The model makes it easy to calculate the importance of the criteria and to choose among the alternatives. The aim of this study is to provide conceptual information about the processing and protection of personal data in our country, to draw a general framework about its development in the world and in our country, to examine the relationship of personal data protection with the big data concepts and practices that have been on the agenda in recent years and finally It offers suggestions on the policy that should be implemented by measuring the perception of citizens regarding the processing and protection of data. Based on these objectives, five main criteria, twenty sub-criteria were determined and a hierarchical structure was established in order to measure the perception of citizens regarding the processing and protection of personal data. At the end of the study, it is considered that the most important criterion for the processing and protection of personal data is required and it is appropriate to choose a reliable intensive policy.

Key words- Personal data, personal data protection, citizen perception, analytic hierarchy process.

1. GİRİŞ (INTRODUCTION)

Kişisel veri kavramı ve kişisel verilerin korunması hususu dünyada uzun yıllardır tartışılan ve düzenlenen bir konu olmasına rağmen ülkemizde nispeten yeni yeni gündeme gelen, yasal ve idari düzenlemelere konu bir alandır. Kişisel veri kavramını genel olarak bireyin; aile bilgisi, ırkı, etnik kökeni, ten rengi, siyasi görüşleri, sendika üyeliği, cinsel tercihleri, dijital bilgileri, biyometrik verileri

vb. her türlü veri kişisel bilgi olarak tanımlanabilir. Kişisel veri kavramını sınırlandırmak için hassas veri ve hassas olamayan veri ayrımı yapılarak kişisel verilerin korunmasının sınırları çizilmeye çalışılmıştır. Özellikli olarak korunması gereken bilgileri hassas veriler içinde değerlendirmek mümkündür.

Türkiye'de kişisel veri kavramı ve kişisel verilerin korunması anlayışı Avrupa Birliği (AB)'ne üyelik sürecinde gündeme gelmiş birtakım yasal ve idari düzenlemelere konu olmuştur. Bu açıdan ülkemizde mevzuat gelişiminin AB müktesebatı ile uyumlu bir şekilde ilerlediğini söylemek mümkündür. Son yıllarda kişisel verilerin korunması hususu doğrudan big data (büyük veri) olarak tanımlanan gelişmeyle yakından ilişkilidir.

Bu çalışmanın amacı, kişisel veri kavramı ile kişisel verilerin korunması konusunda yasal, idari ve teknolojik gelişmeleri inceleyerek son günlerde gündemde olan big data (büyük veri) karamı ile kişisel verilerin korunması konusu karşılaştırıp kişisel verilerin korunması hususunda vatandaş algısının ölçülmesidir. Vatandaş algısını ölçmek için 5 ana kriter (güvenilirlik, farkındalık, ulaşılabilirlik, yeterlilik ve gereklilik) ve ana kriterlere bağlı 20 alt kriter belirlenmiştir. Çalışmada Saaty (1980) tarafından oluşturulan çok kriterli karar verme tekniklerinden bir tanesi olan (Multiple Criteria Decision Making-ÇKKV) Analitik Hiyerarşi Süreci (AHS) yaklaşımı kullanılmıştır. Bu çalışma ülkemizde kişisel verilerin korunması boyutlarının önem derecesinin ve alternatif politikaların AHS yaklaşımı ile belirlendiği ilk çalışmadır.

Çalışma üç ana bölümden oluşmaktadır. İlk bölümde kişisel veri, kişisel veri kavramı, önemi, türleri açıklanmış, dünyada ve ülkemizde kişisel verilerin korunması konusunun gelişim süreci ile ülkemizdeki idari yapılanma ele alınmış ve big data (büyük veri) kavramı ile kişisel verilerin korunması karşılaştırılmıştır. İkinci bölümde ÇKKV tekniklerinden olan AHS modeli ve uygulama aşamaları açıklandıktan sonra üçüncü bölümde araştırma bulguları ve sonuç bölümü ile çalışma tamamlanmıştır.

2. KİŞİSEL VERİ VE KİŞİSEL VERİNİN KORUNMASI (PERSONAL DATA AND PROTECTION OF PERSONAL DATA)

Son yıllarda kişisel veri kavramı ve kişisel verilerin korunması konularında gerek dünya genelinde gerekse Türkiye'de çok büyük gelişmeler olmuştur. Şüphesiz bu gelişmelerin altında yatan neden kamuoyunda kişisel verilerin kayıt altına alınması, yetkisiz kullanımlar ve kişisel verilere göre bireyleri yönlendirme çalışmalarıdır. Bir siteye abone olunurken veya bir kredi çekerken birçok kişisel veri değişiklik yapılamadığı için mecbur kalınan onaylarla söz konusu kurum veya sitenin kullanımına sunulmaktadır. Birçok kurumsal yapısını tamamlamamış/tamamlamış sitenin veya kurumun kullanıcı sözleşmelerinde değişiklik yapmak mümkün değildir ve aynı zamanda çoğu sözleşmede verilerin üçüncü kişilerle paylaşılabileceğine dair maddeler yer almaktadır. Bu üçüncü kişilerin kim veya ne olduğu ise hiçbir zaman açıklanmaz. Bu bölümde literatürde kişisel veri kavramı ve kişisel verilerin korunmasına ilişkin bilgiler ve açıklamalar yer almaktadır.

2.1. Kişisel Veri (Personal Data)

Gerek ulusal gerekse uluslararası metinlerde kişisel veri kavramı benzer şekilde tanımlanmıştır. Kişisel Verilerin İşlenmesi Sürecinde Kişilerin Korunmasına ve Verilerin Serbest Dolaşımına İlişkin Avrupa Konseyi Direktifi (Veri Koruma Direktifi/VKD)'nde kişisel veri kavramı *"fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye (veri öznesi) ilişkin herhangi bir bilgiyi kastedecektir"* olarak tanımlanmıştır [1].

Söz konusu tanım çoğu ülke tarafından benzer bir şekilde kullanılarak iç hukuka aktarılmasına rağmen farklı ve geniş anlamlar içermesinden dolayı ülkelerce kısıtlanmıştır [2]. En önemli kısıtlamalar bir tanesi Direktif'in geniş tanımlaması içinde sadece gerçek kişilere yer verilip tüzel kişilerin çıkarılması şeklinde olmuştur. Bu durumun temel nedeni ise kişisel veri kavramının doğrudan kişi temel hak ve özgürlükleriyle doğrudan ilişki içinde olmasıdır. Zamanla teknolojik gelişmelerle gerek AB gerekse diğer ülkelerde genetik kimlik, sağlık bilgileri, konum verileri ve çevrimiçi kimlik belirleyiciler de kişisel veri kavramı içine eklenmiştir. 2002/58/EC Elektronik Haberleşme Sektöründe Gizliliğin Korunması ve Kişisel Bilgilerin İşlenmesine İlişkin Avrupa Konseyi Direktifi (Elektronik Veri Koruma Direktifi/EVKD) ile, ise tüzel kişilere ait verilerinde koruma altına alınması amaçlanmıştır. Kişisel veriler kişi temel hak ve özgürlükleriyle ilişkiliyken tüzel kişilere ait veriler ise ticari sır, patent, üretim tekniği ve ticari haklara bağlıdır [3]. Kullanıcının kişisel verileri toplayabilen cihazların sayısındaki muazzam artış, kullanıcıların gizliliğine yönelik en temel ve en ciddi tehdit biçimlerinden birisi olmuştur [4].

Türkiye'de kişisel verilerin tanımı ilk kez 6 Şubat 2004 tarihli ve 25365 sayılı Resmi Gazete'de yayımlanan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik (VKY) ile yapılmıştır. Yönetmelikte, kişisel veri veya bilgiler "*tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgiyi*" şeklinde tanımlanmıştır [5].

Halen yürüklükte olan 24 Temmuz 2012 tarihli ve 28363 sayılı Resmi Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik (EHSKVİY)'te kişisel veri *"belirli veya kimliği belirlenebilir gerçek ve tüzel*

kişilere ilişkin bütün bilgileri" ve kişisel veri ihlali ise *"istem 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 ihlalini"* olarak açıklanmıştır [6].

Kişisel veriler, e-posta mesajlarını, programları, ziyaret edilen web sitelerini, kredi kartı ödemelerini, görüntüleri, videoları, sesleri ve biyo-sensör verilerini, çekilen fotoğrafları vb. içerir [7]. Tüm kişisel veriler insanlarla ilgilidir. Diğer bir deyişle, tüm verilerin sahip olduğu nitelikler bulunur. Kişisel veriler genellikle e-posta gönderenler, toplantılardaki meslektaşlar veya fotoğraflardaki aileler gibi sahibi dışındaki kişilerle de ilgilidir [8]. Kişisel veriler heterojendir. Başka bir deyişle, çeşitli ortamlar, biçimler ve ayrıntılara göre farklılık arz eder [9].

Kişisel veri ve kişisel verilerin korunması konusunda ülkemizdeki temel yasal düzenleme olan 07 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan Kişisel Verilerin Korunması Kanunu (KVKK), Türkiye Büyük Millet Meclisi gündemine geldiği zaman yukarıdaki tanım aynen geçerken tüzel kişilerde tanıma dâhil edilmiştir. Ancak Kanun yasalaşırken söz konusu maddeden "*tüzel kişiler*" kaldırılmıştır. AB mevzuatında olduğu gibi ülkemiz yasal düzenlemelerinde de kişisel verilerin korunması hususunda tüzel kişilikler kapsam dışında tutulmuş ve elektronik haberleşme sektörüne yönelik kişisel verilerin korunması hususunda ise genel olarak tüzel kişiliklerde kapsam içine alınmıştır [10]. Kişisel veri kavramı literatürde birçok şekilde tanımlanmıştır. Aşağıda tanımların bir kısmı sunulmuştur:

- Şen, açıklanan mevzuat ve düzenlemelere göre kişisel veriyi, *"kişinin şahsi, ailevi, mesleğine ilişkin kişinin ayırt edici özelliklerini ve niteliklerini göstermeye yarayan her türlü bilgi"* olarak tanımıştır [11].
- Küzeci kişisel veri kavramını, *"belirli veya belirlenebilir bir kişinin kimliğine, etnik kökenine, fiziksel özelliklerine, sağlık durumuna, genetik verilerine, öğrenim veya istihdam durumuna, ikamet adresine, kredi kartına, banka bilgilerine, emniyet bilgilerine, düşünce ve inanç durumuna, alışveriş alışkanlıklarına, telefon rehberine, fotoğrafına, bilgisayarının IP adresine, parmak izine, smslerine, e-maillerine, sosyal paylaşım sitelerindeki aktivitelerine, önceki gün yediği yemeğe kadar varan çeşitli özelliklerini içeren her türlü bilgi"* olarak açıklamıştır [12].
- Lloyd, tarafından kişisel veri, *"kişiyi dolaylı olarak tanıtan kamera kaydı, ses veya görüntüsü, biyometrik yöntemlerle kişiliğinin belirlenmesini sağlayan parmak izi, yüz, iris, yazı, ses tanıma gibi yöntemlerle elde edilen verileri de içeren her türlü kişisel bilgi"* şeklinde tanımlamıştır [13]. Bunun yanı sıra, birey hakkındaki önemsiz olarak görülen veriler veya yayımlanmamış bilgilerin Lloyd'un tanımlamasının içine eklenmesi gerekmektedir.
- Carey kişisel veri kavramının içine bireylerin ırkı, etnik kökeni, ten rengi, siyasi görüşleri, dini, sendika üyeliği, sağlık bilgileri, cinsel tercihleri, mahkûmiyet vb. bilgilerin dâhil edilmesi gerektiğini savunmuştur [14].
- Murray ise, belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgileri kişisel veri olarak kabul etmiştir [15].

Kişisel veri kavramı birçok kişi tarafından oldukça geniş bir şekilde tanımlanmıştır. Ancak bu tanımlamaların sınırını belirlemek oldukça önemlidir. Durant & Financial Authority (İngiliz Temyiz Mahkemesi) kararına göre, kişisel veri olarak değerlendirebilecek bilginin iki özellik taşıması gerektiği ve söz konusu bilginin kişisel veri olarak kabul edilebilmesi için özel hayatın gizliliğini etkilemesi gerektiği vurgulanmıştır [16]. Böylece bir kişinin isminin, adresinin geçtiği ticaret listeleri, maaş bordrosu, kişinin vergi mükellefiyetine ait bilgiler, banka hesap bilgilerinin bütünü kişisel veri kapsamındadır [17]. Bu yaklaşım içinde kişinin başka bilgisinin yer almadığı ismi, elektronik posta veya iş adresi kişisel veri olarak kabul edilmemektedir [16].

2.2. Kişisel Veri Türleri (Personal Data Types)

Kişisel veri kavramını hassas veri ve hassas olmayan veri olarak iki gruba ayırmak mümkündür. Bireylere ait hassas veriler korunması gereken en önemli bilgiler olarak tanımlanabilir. Hassas olmayan veriler ise paylaşılması durumunda kişiye zarar vermeyecek genel geçer bilgilerdir. Ancak bu ayrım gerek ülkeden ülkeye gerekse kişiden kişiye değişmektedir. Sınırların çizilmesindeki zorluk kavramların uygulanması hususunu da sıkıntıya sokabilmektedir.

Hassas kişisel veriler, temel olarak kişisel veri kavramının içine girmesine rağmen özellikli olarak korunması gereken bilgi grubu olarak tanımlanabilir [18]. VKD'nin giriş bölümümün 33. maddesinde hassas verilere yönelik olarak "*veri öznesi açık şekilde rıza göstermezse, temel özgürlükleri veya kişisel mahremiyeti ihlal eden yapıdaki veriler işlenmemelidir.*" ifadesiyle vurgu yapılmıştır. Madde, kişinin rızası olmaksızın temel özgürlüklere ve kişisel mahremiyete yönelik verilerin hassas veri olarak tanımlanabileceğini ifade etmektedir [1]. VKD'nin 51. maddesinde aynı yaklaşımdan yola çıkılarak hassas verilerin özel koruma gerektirdiği hususuna yeniden değinilmiştir.

Hassas verilere yönelik olarak VKD'nin 8. maddesinin 1 bendinde yer alan "*Üye Devletler, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklayacaktır.*" hükmü ile bir diğer tanımlama yapılmıştır [1]. Söz konusu tanımlama ile hassas veriler kapsamında değerlendirilebilecek bilgiler sıralanmış ve

sınıflanmıştır. Yukarıdaki bilgilere teknolojik gelişmelerle ile genetik ve sahibinin belirlenebilmesini sağlayan biyometrik veriler dâhil edilerek kapsam hem genişletilmiş hem de çağın gereklerine uygun hale getirilmiştir. Bu açıdan biyometrik teknolojilerin kullanımı ile kişisel verilerin korunması konusu ayrılmaz bir bütündür [19].

Bu veri ve bilgilerin korunması için daha kapsamlı önlemlerin alınması, yasalarla korumanın garanti altına alınması ve rıza olsa dahi paylaşımların kontrol edilmesi gerekmektedir. Durum AB mevzuatında doğrudan ve dolaylı olarak kişilerin ırkı ve etnik kökeni, ten rengini, siyasi görüşlerini, dini ve felsefi inançlarını, sendika üyeliğini, sağlık ve cinsel yaşamını ve bağımlılıklarını, mahkûmiyet ve güvenlik tedbirlerini, genetik ve biyometrik veriler ile ilgilidir.

Hassas kişisel verilerin tanımlaması ülkeden ülkeye farklılık göstermektedir. Hassas veri kavramı, Hollanda'da özel kişisel veri, İngiltere, İsveç ve Yunanistan'da hassas kişisel veri, 108 nolu Sözleşmede özellikli veri kategorileri olarak isimlendirilmektedir. 07 Nisan 2016 tarihinde yayımlanan ve yayımından 6 ay sonra yürürlüğe giren KVKK'da hassas veriler "*özel nitelikli kişisel veriler*" olarak tanımlanmış ve AB mevzuatı ile uyumlu olarak " *kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefî 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.*" şeklinde tanımlanmıştır [20].

Yukarıdaki tanımlardan anlaşılacağı üzere hassas veriler, bireye sıkı sıkıya bağlı olan temel hak ve hürriyetler kapsamına giren daha sıkı korunması gereken bilgilerdir [17]. Gerek AB mevzuatına gerekse ülkemiz yasal düzenlemelerinde hassas veri olarak tanımlanan bilgiler özel korunma alanına dâhil edilmiştir. Kişilerin açık rızası olmadan işlenmesine yönelik yasaklar gelen hassas verilerin korunmasında veya kişilerin rıza göstermesi hususunda ayrıca düzenlemeler yapılması gerektiği değerlendirilmektedir. Kısa açıklamalar, küçük yazılar veya değiştirilemeyen kullanıcı/abonelik sözleşmeleri kişilerin açık rızasının alındığını iddia ederek haksız kullanımların önünü açmaktadır.

Hassas olmayan kişisel veriler, kişisel veri kapsamında olup paylaşılması veya kayıt altına alınmasının kişiyi mağdur etmeyen veya ayrımcılık tehlikesine düşürmeyen bilgiler olarak tanımlanabilir. Hassas olmayan verileri hassas verileri sayarak belirlemek mümkün olmasına rağmen tanımların tam neyi kastettiğinin belirlenmesi kişisel verilerin korunması için büyük önem taşımaktadır. Buna rağmen hassas olmayan veriler temel hak ve özgürlükleri kapsamında olmayan bilgiler olarak değerlendirilebilir [21]. Hassas olamayan verilerin işlenmesine yönelik yasal düzenlemeler KVKK'daki hükümlerden ziyade daha çok genel hukuk kapsamında işlenebilmektedir [10]. Hangi bilginin hassas kişisel veri veya hassas olmayan kişisel veri kapsamında olduğu zamana ve mekâna göre değişebilmektedir. Bu kapsamda yasal düzenlemelerin hassas olmayan verilere yönelikte birtakım düzenlemelere ihtiyaç duyduğunu söylemek mümkündür.

2.3. Kişisel Verinin Önemi (The İmportance of Personal Data)

Kişisel verilerin paylaşılmasının hangi riskleri ortaya çıkarabileceği, kişisel verilerin toplanmasındaki kuralların varlığından habersizlik veya verilerin firmalar tarafından hangi amaçlarla kullandığının tam olarak tespit edilememesi şüphesiz günümüzün olduğu kadar geleceğimizin de en büyük tartışma konularından biri olacaktır. Özellikle gelişmiş ve gelişmekte olan ülkelerde gerek yasal gerekse idari düzenlemeler uzun yıllardır yapılmasına rağmen konunun ciddiyeti ve önemi anlaşılabilmiş değildir. Özellikle Amerika Birleşik Devletleri (ABD) seçimlerinde kişisel verilerin seçmen davranışlarını yönlendirmek için kullanıldığı iddiası ve siber dünyadaki saldırganlıklar ile zorbalıklar hem kişilerin hem de kurumların dikkatini hiç olmadığı kadar çekmiştir. Kişisel verilerin ve kişisel verilerin korunması konularının önemini aşağıdaki gibi sıralamak mümkündür [22]:

- Bireysel anlamda kimliğe dair unsurların korunması ve bu vesile ile mahremiyet olgusunun ve kişisel haklarının güçlendirilmesi,
- Finansal anlamda sahip olunan verilerin korunması neticesinde, maddi anlamda yaşanabilecek yüksek ölçekli tehdit, kayıp ve risklerden bireylerin korunması,
- Tıbbi anlamda sahip olunan verilerin kötüye kullanılmaması ve bireylerin hayatlarının ve sağlık durumlarının akışını olumsuz yönde etkileyecek şekilde sorunların ortaya çıkmaması,
- Dijital ortamlarda sahip olunan bilgilerin, elde edilen hakların, gönderilen mesajların, yapılan işlemlerin vb. faaliyet ve unsurların mahremiyetinin korunması,
- Kişilik haklarının ve hürriyetlerinin zarar görmesinin engellenmesi,
- Bireylerin, kötü amaçlı faaliyetleri yürüten taraflara karşı hukuki anlamda ellerinin güçlendirilmesi.

Bunların yanı sıra kişisel verilerin kurumlar açısından da oldukça önemli unsurları vardır. Kurumsal verilerin korunması ve kayıt altına alınması şüphesiz kişisel verilerin işlenmesi ve kayıt altına alınması kadar önemlidir. Kurumlar açısından verilerin önemini aşağıda sıralanmıştır [23]:

- Kurumsal prestij ve imajın, güvenlikli bir kurum algısıyla zedelenmesinin engellenmesi,
- Kurumun müşterilerinin hukuki sorunlar yaşamamaları ve sorunun kurum açısından kamusal bir sorun haline gelmemesi adına gereken önlemlerin alınması,
- Dijital anlamdaki yeterlilik ve kurumun modern bir vizyonunun bulunduğunun ispatı açısından dijital gelişmişliğin uygulamaya konması,

- İş ortakları nezdinde güven arz eden bir imajın yerleştirilmesi ve bu vesile ile de güçlü bir ortak, paydaş vb. algısının piyasada yerleştirilmesi,
- Güvenliğe dair uygulamaların rutin hale getirilmesi ve bu vesile ile de kişisel verilerin değerinin kurum kültürü ile özdeşleştirilmesi.

Yukarıdaki maddeler incelendiğinde çoğunun kişisel verilerin önemi unsurlarıyla yakından ilişkili olduğunu söylemek mümkündür. Gerek kişisel verilerin güvenli bir ortamda tutulmasının gerekse kurumların kendi verilerini veya söz konusu kişisel verileri koruması itibar, güven ve prestij için son derece önemlidir. Her ne kadar yakın bir ilişki olmasına rağmen kişisel verilerin kaydedilmesi ve kullanılması konusunda neredeyse tüm yetki kurumlara aittir. Bu tek taraflı etki ve yetki şüphesiz kurumların daha hassas olmasını gerektirmekte olup kamu gücünün yani yasaların kişisel verilerin korunması ve kayıt altına alınması hususunu düzenlemesi zorunluluğunu doğurmuştur [23].

Kişisel verilerin korunması ve kayıt altına alınmasının kurala bağlı olmasının temelinde insan onurunun korunması yatmaktadır [24]. İnsan onuru, doğuştan gelen kişinin kendisinin değerli olduğunu bilmesini sağlayan duygudur [21]. Kişinin söz konusu duygusunun veya değerinin bir başka kişinin veya kurumun hareketiyle azalması, ortadan kalması veya artması mümkündür. İnsan onuruna etki eden fillilerden birisi de kişisel verilerin kişinin onurunu zedeleyecek amaçlarla kullanılmasıdır [24].

Kişisel verilerin öneminin bir diğer yansıması ise unutulma hakkı üzerinde görülmektedir. Unutulma hakkı temeli af edilme hakkına dayanmaktadır [25]. Günümüzde unutulma hakkı daha çok dijital ortamdaki verilerin veya tüm bilgilerin belirli bir zaman sonra silinmesi anlamında kullanılmaktadır. Teknolojinin çok hızlı bir şekilde değişilmesi gün geçtikçe gizliliğin sınırlarını daraltmakta, kişisel verilerin çok hızlı bir şekilde yayılmasına neden olmakta ve kişisel bilgilerin tüm kullanıcıların erişimine açık hale getirmektedir. Bu durum kişilerin verilerinin gerek dijital gerekse gerçek dünya kayıtlarından silinmesini isteme hakkına götürmektedir. Bireyler, sadece kriminal bilgilerin değil tüm özel veya daha önce açıklandı üzere hassas verilerin silinmesini talep etme hakkına sahiptir [26].

2.4. Kişisel Verinin Korunması (Protection of Personal Data)

Günümüz dünyasına teknolojini hızla gelişmesi insan kişiliğine yönelik tehditlerin artmasına ve söz konusu tehditlere karşı korunma yollarının çeşitlenmesine neden olmuştur. Şüphesiz hukuksal düzenlemelerin güncel sorun ve konuları geriden takip ettiği yadsınamaz bir gerçektir. Buna rağmen kişisel verilerin özelinde insan onurunun, haklarının ve özgürlüğünün korunması hukuksal olarak güvenceye alınmasının uzun bir geçmişi vardır. Kişisel verilerin hukuki niteliğine dair oldukça farklı görüşler ileri sürülmüştür. İlk yasal düzenlemeler kişisel verilerin niteliği itibarıyla kişilik, mahremiyet, mülkiyet veya fikri mülkiyet haklarının bir parçası olarak değerlendirilmiştir. Söz konusu hakkın kişisel hak olarak kabul edilmesi görüşü özellikle Kıta Avrupa'sında yaygın olarak kabul edilmektedir. Nitekim VKD'nin çeşitli maddelerinde kişisel veriler, özellikle kişilik hakkı ile bağlantılı olarak mahremiyet hakkı ile ilişkilendirilmiş ve belli ölçüde insan haklarının korunmasına da vurgu yapılmıştır. Gerçek kişinin yanı sıra tüzel kişiliğin verilerini koruma hakkı da yasal düzenlemelere konu olmuştur. Privacy by Design (bir mal veya hizmetin üretim sürecindeki gizliliği temel alır.) kavramı etrafında şekillenen gizlilik politikaları, veri minimizasyonu, sınırlı amaç ve saydamlık üzerine kurulu iken buna ek olarak mevcut teknoloji, oluşan masraf ve risk konusunda yüksek koruma standartları sağlamak hedeflenmiştir [24].

Kişilik veya mahremiyet hakkı açısından kişisel verilerin korunması kişinin sağlığına, ailevi durumuna, inancına ilişkin bilgiler o kişinin özel alanı içinde olup, bu bilgilerin üçüncü kişilere yayılması, üçüncü kişilere yayılma tehlikesi taşıdığı için bir başkası tarafından saklanması, özel alana müdahale olarak kabul edilecektir [27]. Şüphesiz kişilik hakkı başka birinin görmeyeceği şekilde yalnız kalabileceği, kendi rızasıyla istediği kişilerle görüşebileceği ve kendisini her türlü araçla geliştirebileceği ayrıcalıklı bir alanın oluşturulması ve korunması konusunda güvence vermektedir [24]. Kişisel verilerin korunması ve kayıt altına alınması da şüphesiz mahremiyet hakkı ve kişilik hakkı çerçevesinde değerlendirilir.

Kişisel verilerin korunmasının kişilik hakkı ile irtibatlandırılması birçok açıdan eleştirilmektedir. İlk eleştiriye göre, bazı zamanlar bir kişi hakkında bilgi edinmek amacıyla elde edilen veriler nedeniyle söz konusu kişinin itibarının zedelenebilir. Diğer bir eleştiri ise yasal düzenlemelerin kapsamının oldukça geniş tutulmasından dolayı sadece kişilik hakkının değil birçok temel hak ve özgürlüğünde kişisel verilerin korunması kapsamına dahil edilmesidir. Son olarak, kişisel verilerin korunması konusunda bir kez hata yapıldığı zaman söz konusu bilgiler açıklanacak ve artık korunması neredeyse imkansız olacaktır. Bu yüzden kişilik hakkının korunmasında bir süreklilik olmasına rağmen kişisel verilerin sonsuza kadar tam bir güvenle korunması mümkün değildir [10].

Mülkiyet hakkı çerçevesinde kişisel verilerin korunması hususu değerlendirildiğinde söz konusu verilerin ticari bir değer taşıdığı dikkate alınmıştır. Ticari değer açısından kişisel veriler belirli bir ücret karşılığında satılabilmekte ve alıcılar bulabilmektedir. Özellikle büyük bir veri yığınına sahip kurum veya kişinin kişisel verilerden oldukça büyük paralar kazanması mümkündür. Bu noktada kişinin rızası olmadan bilgilerini ticari amaçlarla kullanılması kişiyi veya kurumu mülkiyet hakkının ihlalinden dolayı mahkemeye vermesine neden olacaktır [17].

Kişisel verilerin korunması, modern dünyada günlük hayatın yadsınamaz bir gerçeğidir. Bu gerçeklik içinde çok sayıda bireyin bilgileri ve her türlü verisi dijital dünyada

saklanmakta, işlenmekte, bazen çalınmakta, dağıtılmakta veya kötü kullanımlara neden olmaktadır [28]. Bilişim suçlarının ortaya çıkmasıyla, maddi kayıplar meydana gelmektedir. Ancak dikkat çeken bir diğer kayıp kişilere özel bilgiler, resim, yazışmalar gibi kişisel bilgilerin yabancı kişilerin eline geçmesidir. Bu verilerin birçok kullanım amacı olmakla birlikte kişilerin özel hayatlarına büyük zarar verilebilmektedir [29]. Bilgi toplumu çağında veri ekonomik bir değer kazanmış ve alınıp satılabilir hale dönüşmüştür. Bu dönüşüm ile birlikte kişisel verilerin korunması, paylaşılması ve farkındalığın yükseltilmesi önemli hale gelmiştir [30].

Bilgi toplumundan bu yana veri ekonomik bir faktör haline gelmiş ve alınıp satılabilir olmuştur. Bu durum kişisel verilerin korunması konusunun önemini artırmış ve insanların bu hususta daha dikkatli olmalarını zorunlu kılmıştır.

Bilgisayar çağında artık veriler kapalı kapılar arkasında saklanmamakta ve sadece güvenlik nedeniyle değil aynı zamanda ihtiyaç duyulması gibi nedenlerden dolayı arşivlenmekteydi. Günümüz dijital dünyasında verilerin kayıt edilmesi maliyetleri azalmış, çok daha hızlı bir şekilde erişim imkânı sağlanmasıyla birlikte güvenlik riskleri de bir o kadar artmıştır. Güvenlik risklerinin ortadan kaldırılması için kurallar koyulması ve uygulanması ise kişisel verilerin korunması ile ilişkilidir [31]. Kaya, kişisel verilerin korunması sürecinin içerisine aşağıdaki unsurların dâhil edilmesini önermiştir [18]:

- **Kimlik bilgileri:** Dini, etnik ve toplumsal kökene dair veriler ile birlikte bağlı bulunan ülkenin kimlik numarasına dair detaylar.
- **Sağlık bilgileri:** Çeşitli rahatsızlıkların detayları, cinsel tercih, cinsel sağlık problemleri vb. hakkındaki detaylar.
- **Bankacılık bilgileri:** Hesap numarası, hesap içeriğine dair bilgiler, banka ya da finans kuruluşları ile gerçekleştirilen anlaşmalar, banka kartı, kredi kartı, çek vb. ticari unsurlara dair bilgiler.
- **Dijital hesap verileri:** E-posta adresi, çeşitli internet sitesi üyelikleri, dijital ortamda gerçekleştirilen satın alma bilgileri vb.

Kişisel verilerin korunması genel olarak yukarıdaki bilgileri kapsamakta olup birçok yasal düzenleme ile güvence alına alınmaya çalışılmıştır. Sonuç olarak kişisel verilerin korunmasının doğrudan kişilik hakkıyla bağlantılı olduğunu söylemek mümkündür. Ayrıca, kişisel verilerin korunmasına ilişkin devletlerin yasal düzenlemeleri ile kurumsal yapılarının yetersiz kalmaktadır.

2.5. Kişisel Verilerin Korunması ve Büyük Veri (Protection of Personal Data and Big Data)

Big data veya büyük veri kavramı son yıllara herkes tarafından bilinmekte ve kullanılmaktadır. Buna rağmen kavramın kökeni ve ilk kullanımı tespit edilememiştir. Diebold, büyük veri kavramının bilgisayar mühendisi, girişimci ve tasarımcı John Mashey tarafından kullanıldığını ve 1990'lı yılların ortalarında Silicon Graphics Inc. firmasında sohbet esnasında ortaya çıktığını ileri sürmüştür [32].

Büyük veri, geleneksel teknoloji ve veri tabanı teknolojileri ile işlenmesi, depolanması ve analizi zor olan verilerin hacmindeki artışı tanımlamak için kullanılmaktadır. Büyük veri kavramı bilgi teknolojileri, işletme ve literatürde nispeten yeni bir kullanıma sahiptir. Yaygınlaşmasından önce kavramın literatürde kullanımına rastlamak mümkündür. Cox ve Ellsworth (1997) 1997 yılında kavramı, veriyi görselleştirmek ve anlamlandırmak için büyük miktarda bilimsel veri olarak tanımlamıştır [33].

Manyika ve diğer yazarlar tarafından kaleme alınan "*Big Data: The Next Frontier for Innovation, Competition, and Productivity*" kitapta gerek büyük veri kitabında ayrıntılı bilgiler sunulmuş gerekse kavram "*etkili bir şekilde depolanması, yönetilmesi ve işlenmesi teknoloji kapasitesinin ötesinde olan veri miktarı*" şeklinde tanımlanmıştır. Zikopoulos ve diğer yazarlar ile Berman büyük veriyi 3V: volume (hacim), velocity (hız) ve variety (çeşitlilik) ile tanımlamıştır. 3V tanımlaması, büyük veriyi açıklamak için ortak bir çerçeve olarak kullanılmaktadır [34].

Hacim, hız ve çeşitlilik terimleri ilk olarak büyük veri zorluklarını tanımlamak için Gartner (küresel araştırma ve danışmanlık firması) tarafından ileri sürülmüştür. Gartner büyük veriyi; gelişmiş kavrama, karar verme ve süreç otomasyonuna olanak sağlayan uygun maliyetli ve yenilikçi bilgi işleme yapıları gerektiren yüksek hacimli, yüksek hızlı ve/veya yüksek çeşitlikte bilgi varlıkları olarak tanımlamıştır [35].

International Data Corporation (IDC) büyük veri teknolojilerini; yüksek hızda kaydetme, işleme, sınıflandırma ve analiz yaparak, geniş kapsamlı çok büyük veri hacimlerinden ekonomik olarak değer çıkarmak için tasarlanan yeni nesil teknolojiler ve mimariler olarak tanımlamıştır [36]. Sonuç olarak, ulaşılabilen tüm kaynaklardan toplanan verinin yakalanması, kaydedilmesi, dağıtılması, karşılaştırılması, yönetilmesi, analiz edilmesi ve sınıflandırılması sonunda ortaya çıkan çok büyük hacimli hızlı, değişken ve karmaşık bilgiyi büyük veri olarak tanımlamak mümkündür.

Dünya Çapında büyük veri yazılım ve hizmetleri için pazar gelirlerinin 2018 yılında 150 milyar dolardan 2020 yılında 200 milyar dolara yükseleceği tahmin edilmektedir. Wikibon'a göre büyük verinin her yıl %10.48 büyümesi beklenmektedir. Accenture firmasına göre, yöneticilerin %79'u, büyük veriyi kullanmayan şirketlerin rekabet güçlerini kaybedecekleri ve yok olma tehlikesiyle karşı karşıya kalabilecekleri konusunda hemfikirler. Ankete katılan yöneticilerin %83'ü rekabet avantajı elde etmek için büyük veri projelerini takip ettiklerini ifade etmişlerdir

[37]. Şüphesiz büyük veri öncelikle teknoloji şirketlerini ve daha sonra tüm işletmeleri etkileyecektir.

Büyük veri kavramı ve uygulamaları birçok kişisel ve kurumsal bilgiye ihtiyaç duymakta olup adeta bu bilgilerden beslenmektedir. Büyük verinin ihtiyaç duyduğu bilgilerin toplanması ve işlenmesi doğrudan doğruya kişisel verilerin korunması hakkının kapsamına girmektedir. Anonim veya hassas olmayan verilerin toplanması konusunda genel bir kabul olmasına rağmen büyük verinin hassas bilgilerin işlenmesine de ihtiyacı vardır. Ayrıca, anonim veya hassas olmayan verilerin işlenmesi söz konusu bilgilerin kime ait olduğunun tahmin edilmesini kolaylaştırmaktadır. Örneğin, America Online (AOL) ve Netflix firmaları kullanıcı bilgilerini anonim hale getirmiş ve veri uzmanları kullanıcı kimliklerini tespit edebilmiştir [23].

Büyük veri gibi popüler bir kavram ve uygulama kişilerin alışveriş verilerinden yeni satın alma davranışlarının tahmin edilmesi veya yönlendirilmesi, sağlık verilerinden hastalıklara yakalanma olasılığına, banka bilgilerinden krediye ihtiyaç duyacağı zamanın tahmin edilmesine veya arama tercihlerinden dünya görüşünün tespit edilmesine kadar birçok çıkarımda bulunulmasına imkân tanır. Şüphesiz tüm bu tahminler ve yönlendirmeler için birçok hassas veriye ihtiyaç duyulacaktır.

Bu yüzden kişisel verilerin işlenmesi ve kayıt altına alınması hususunda ayrıntılı düzenlemeler ve kısıtların uygulanması gerekmektedir. Ulusal kaynakların ve mevzuatın global dünyada söz konusu düzenlemeleri uygulaması gün geçtikçe zorlaşmaktadır. Hem siber saldırılarla çok büyük miktarda veriler ele geçirilmekte hem kurumların verileri iç kaynaklardan dışarı sızdırılmakta hem de kullanıcılar değiştiremediği, okumadığı veya bilmediği sözleşmeleri onaylayarak yani açık rıza beyanlarında bulunarak söz konusu paylaşıma izin verilmektedir. Örneğin, KVKK'nun 5/2/c maddesi "*bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.*" ile 5/2/f maddesinde yer alan "*ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.*" hükümlerine göre kişisel veriler işlenebilecektir. Yine aynı kanunun 6/2 maddesinde yer alan "*özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.*" hükmüne göre rıza kişisel verilerin işlenmesine olanak sağlamaktadır [20].

Sonuç olarak büyük veri kavramı ve uygulamaları çalışabilmesi için muazzam boyutlardaki bilgiye ihtiyaç duymaktadır. Şüphesiz kaynaklar her zaman meşru yollar kullanılarak elde edilen bilgilerden oluşmayacaktır. Bu yüzden nasıl ki kişisel verilerin işlenmesi, kaydedilmesi ve kullanılması kurala bağlandıysa büyük veri uygulamaları ve kaynakları da düzenlenmelidir.

2.6. Dünyada ve Türkiye'de Kişisel Verinin Korunması Gelişmeleri (The Protection of Personal Data, Developments in the World and Turkey)

Globalleşen ve sanallaşan dünyada bireylerin korunması ve güvenliğinin sağlanması son yirmi yılın en çok tartışılan konusu haline gelmiştir. Dünya genelinde kişisel verilerin korunması konusunda ilk düzenlemeler Amerika Birleşik Devletleri'nde 1966 tarihli Bilgi Edinme Hakkı Kanunu (The Freedom of Information Act) ile 1974 tarihli Özel Yaşamın Gizliliği Kanunu (The Privacy Act) olarak kabul edilmektedir [18]. Bir diğer önemli belge ise, Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) tarafından hazırlanan ve 1981'de kabul edilen "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler" raporudur [38]. Dünya çapında en önemli belgelerden biri ise, Birleşmiş Milletler Genel Kurulu tarafından 1990'da "Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler" başlığındaki düzenlemedir [22].

Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi çerçevesinde, Avrupa Konseyi 1960'lı yıllardan itibaren bilgi teknolojileri sektöründeki gelişmelerin de etkisiyle kişisel verilerin korunması, işlenmesi ve hakkına yönelik çeşitli metinleri kabul etmiştir [39]. Kişisel veri kavramı, Avrupa Konseyi'nce 28 Ocak 1981 tarihinde imzaya açılan ve 1 Ekim 1985 tarihinde yürürlüğe giren 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" ile gündeme gelmiş ve resmi bir anlam kazanmıştır.

Türkiye ile Avrupa Birliği entegrasyon ve katılım müzakereleri kişisel verilerin korunması politikaların benimsenmesinde oldukça etkili olmuştur [40]. Küresel gereklilikler ve ekonomik sebeplerle süreç son on yılda oldukça hızlanmıştır. Bu bağlamda Türkiye'nin AB ile müzakerelerinde 23. ve 24. Fasıllarının tamamlanabilmesi ve vize serbestliğine ilişkin süreci, kişisel verilerin korunmasına ilişkin politikaların geliştirilmesi şartına bağlanmıştır [41].

Türkiye, 108 sayılı Sözleşmeyi 28 Ocak 1981 tarihinde imzalamış, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun" ile onaylamış ve oldukça gecikmeli olarak resmi Türkçe çevirisi 17 Mart 2016 tarih ve 29656 sayılı Resmi Gazete'de "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin İlişik Beyanlarla Birlikte Onaylanması Hakkında Karar" olarak yayımlanmıştır. Sözleşmenin onay belgeleri 02 Mayıs 2016 tarihinde Avrupa Konseyi Genel Sekreterliği'ne tevdi edilmiş ve 1 Eylül 2016 tarihinde yürürlüğe girmiştir.

Ayrıca, Cumhurbaşkanlığı Devlet Denetleme Kurulu'nun 2013 tarihli "Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında

Gerçekleştirilen Denetim Çalışmaları" başlıklı raporda 108 sayılı düzenlemenin önemine değinilmektedir [42].

Sözleşmenin geç bir tarih olan 1 Eylül 2016 tarihinde yürürlüğe girmesi evrakların Avrupa Konseyi'ne gönderilmesi ve diğer prosedür işlemlerinin zaman almasından dolayıdır. Sözleşmenin ülkemizde doğrudan yansıması 7 Nisan 2016 Tarihli ve 29677 Sayılı Resmi Gazete'de yayımlanan 6698 sayılı "Kişisel Verilerin Korunması Kanunu" olmuştur. Kanunun yürürlük tarihi ise yayımlanmasından sonra altı ay (7 Ekim 2016) olarak belirlenmiştir [21].

Sözleşmenin amacı, "*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."* şeklinde ifade edilmiş ve söz konusu amacın sözleşmeyi imzalayan her ülkede korunması hedeflenmiştir.

Kişisel veriler, 2010 yılında gerçekleştirilen Anayasa değişikliği ile "Özel hayatın gizliliği ve korunması hakkı" başlığı altında "*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.*" hükmü yer almaktadır. Söz konusu madde doğrudan "Özel hayatın gizliliği ve korunması" başlığı altında yer almakta olup kişisel verilerin mahremiyet konusu ve anlamı Anayasa'da da vurgulanmıştır [43].

Türkiye'de kişisel verilerin korunmasına konusunda en geniş birincil yasal düzenleme olan 6698 sayılı Kanun'un yayımlanmasından önce Türk Ceza Kanunu'nun (TCK) kişisel verilere ilişkin hükümler ile söz konusu veri ihlallerine yönelik bir güvence olarak düzenlenmiştir. TCK'nın bölümü "*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*" başlıklı 9. bölümü ile kişisel verilerin ihlali, kişisel verilerin kayıt altına alınması, hukuka aykırı bir şekilde dağıtılması, ele geçirilmesi, silinmesi ve korunması konuları ele alınmıştır [41].

Yukarıda açıklanan ve ele alınan kişisel verilerin korunmasına yönelik bütün birincil kaynaklara ilave olarak ikincil derecede pek çok yasal düzenleme de mevcuttur**.** Bunlar arasında Türk Ceza Kanunu, Türk Medeni Kanunu, Ceza Muhakemesi Kanunu, İş Kanunu, Bankacılık Kanunu, Banka ve Kredi Kartları Kanunu, Elektronik İmza Kanunu, Fikir ve Sanat Eserleri Kanunu, Bilgi Edinme Kanunu, İş Kanunu, Vergi Usul Kanunu, Nüfus Hizmetleri Kanunu, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, Noterlik Kanunu, Basın Kanunu, Türkiye Radyo ve Televizyon Kanunu, Adli Sicil Kanunu, Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, Polis Vazife ve Selahiyet Kanunu Tıbbi Deontoloji Sözlüğü, Elektronik Haberleşme Kanunu, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik, Elektronik İmza Kanunu, Türk Borçlar Kanunu, Türk Ticaret Kanunu, Nüfus Hizmetleri Kanunu, Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkındaki Yönetmelik ile çeşitli yüksek mahkeme kararları sayılabilir [42].

2.7. Kişisel Verileri Koruma Kurumu (Personal Data Protection Authority)

Kişisel Verileri Koruma Kurumu Kanun ile verilen görevleri yerine getirmek üzere, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz olarak kurulmuştur. Kurum kişisel verilerin korunmasına ilişkin aşağıdaki yetkilere sahiptir [20]:

- *Görev alanı itibarıyla, uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak.*
- *İhtiyaç duyulması hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak.*
- *Kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda uluslararası kuruluşlarla iş birliği yapmak, toplantılara katılmak…*

Kişisel Verileri Koruma Kurulu ise KVKK ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Kurulun kişisel verilerin korunmasına ilişkin görev ve yetkileri aşağıdaki gibidir [20]:

- *Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak.*
- *Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak.*
- *Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak.*
- *Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek.*
- *Veri Sorumluları Sicilinin tutulmasını sağlamak.*
- *Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak.*
- *Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak.*
- *Veri sorumlusunun (kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi tanımlar) ve*

temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak…

Ülkemizde "*kişisel verilerin işlenmesinde başta özel hayatı gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları*" belirleyen ve yöneten yegâne kurum olan Kişisel Verileri Koruma Kurumu idari yapılanmasını tamamlamış ve etkin bir şekilde çalışmaya başlamıştır.

Daha önce ifade edildiği üzere AHS yaklaşımı karar vermek için belirlenen kriterleri sıralamayı ve alternatifler arasından seçim yapmaya yardımcı olmaktadır. Kişisel verilerin korunmasına yönelik olarak politikalar geliştirilmesi kamu yönetiminin karar alması gerekmektedir. Çalışma içinde bu kararlar güvenilirlik yoğun, farkındalığın artırılması, gerekliliğin yükseltilesi temelli olarak üç ana kısma ayrılmıştır. Uygulanan anket ile beş ana kriter ve dört alt kriter ile alternatifler arasında seçim yapılması öngörülmüştür. Böylece kamu yönetiminin uygulayacağı politikanın önceliği tespit edilebilir hale getirilmiştir. Aşağıdaki bölümde bu seçimin yapılabilmesini mümkün kılan ve çalışmada kullanılan yöntemin tanımlaması yapılmıştır.

3. ANALİTİK HİYERARŞİ SÜRECİ YAKLAŞIMI (ANALYTICAL HIERARCHY PROCESS APPROACH)

Çok kriterli karar verme tekniklerinden biri olan AHS, Thomas L. Saaty tarafından 1970'li yılların başlarında geliştirilmiş olup karar alma süreçlerinde kullanılan farklı ölçütleri de dikkate alan bir modeldir [44]. AHS, grup veya bireylerin karar alma sürecindeki önceliklerine dikkate alarak gerek niceliksel gerekse niteliksel kriterleri kriterleri belirlemeye, kriterlerin ağırlıklarını hesaplamaya ve nihai karara ulaşılmasının amaçlandığı matematiksel bir tekniktir [45].

AHS kriterleri ayrıştırma, yargıların karşılaştırılması ve önceliklerin sentezi olmak üzere üç temel kural çerçevesine dayanmaktadır [46,47]. Model, karar verme aşamasında olanların karşılaştıkları sorun ile ilgili olarak amaç, kriterler ve alternatif kararlar belirleyerek hiyerarşik bir yapı oluşturmaları gerektiği ileri sürmektedir [48]. Böylece problemin hiyerarşik parçalara ayrılmasıyla anlaşılması kolaylaşacaktır. AHS ikili kıyaslama aracılığıyla yargıların önceliklerini ve ağırlıklarını belirlemeye ve böylece problemin anlaşılırlığın yükselmesi ile birlikte kararların rasyonelleştirilmesine yardımcı olur [49,50]. Yargıların karşılaştırılması önem derecelerinin belirlenmesini ve her bir faktörün problem üzerindeki göreceli etkisini göstermektedir [51].

3.1. Analitik Hiyerarşi Süreci Modelinin Uygulanma Aşamaları (Application Phases of the Analytical Hierarchy Process Model)

Bir karar verme probleminin AHS ile çözümlenebilmesi için gerçekleştirilmesi gereken aşamalar aşağıda tanımlanmıştır. Her bir aşamada, formülasyon ile birlikte ilgili açıklamalar yapılmıştır [47]. AHS uygulama aşamaları aşağıdaki gibi özetlenmektedir [52]:

1. Adım. Modelin kurulması ve problemin formüle edilmesi: AHS'de karar sürecini ve kararı etkileyen tüm faktörler anket çalışmasıyla veya uzman kişilerle yapılan görüşmeler sonucunda belirlenmelidir. Araştırma konusunda yapılan çalışmalar ile amaç, ana kriterler, alt kriterler ve alternatifler oluşturularak hiyerarşik model meydana getirilir [53]. Bu model ile temel hedef belirlenir, hedefe ulaştırılacak kriterler ile kriterlere bağlı olarak alt kriterler oluşturulur. Sonrasında hedefe ulaşmayı sağlayan kriterler kullanılarak alternatifler değerlendirilir. Aşağıda AHS yaklaşımı açıklanmıştır.

2. Adım. Verilerin toplanması, ikili karşılaştırmalar matrislerinin oluşturulması: Hiyerarşik yapı oluşturulduktan sonra aşağıdaki tabloda yer alan veya daha geliştirilmiş hali literatürde yer alan ikili karşılaştırma ölçeği [47] kullanarak veriler kıyaslanır ve (nxn) ikili karşılaştırmalar matrisi oluşturulur [54].

3. Adım: Hiyerarşinin her bir aşamasındaki elemanların göreli ağırlıklarının (özvektör) hesaplanması: İkili karşılaştırmalar matrisi oluşturulduktan sonra, toplamı 1.00 veya yüzde 100 olacak şekilde normalleştirme işlemine tabi tutularak matrislerin özvektörleri hesaplanır. Özvektörlerin hesaplanması için sütunlarda yer alan değerler toplanarak sütun toplamları elde edilir. Daha sonra sütunda yer alan her değer sütun toplamına bölünerek normalleştirilir. Son olarak, satırda yer alan değerlerin ortalamaları bulunarak özvektörler elde edilir.

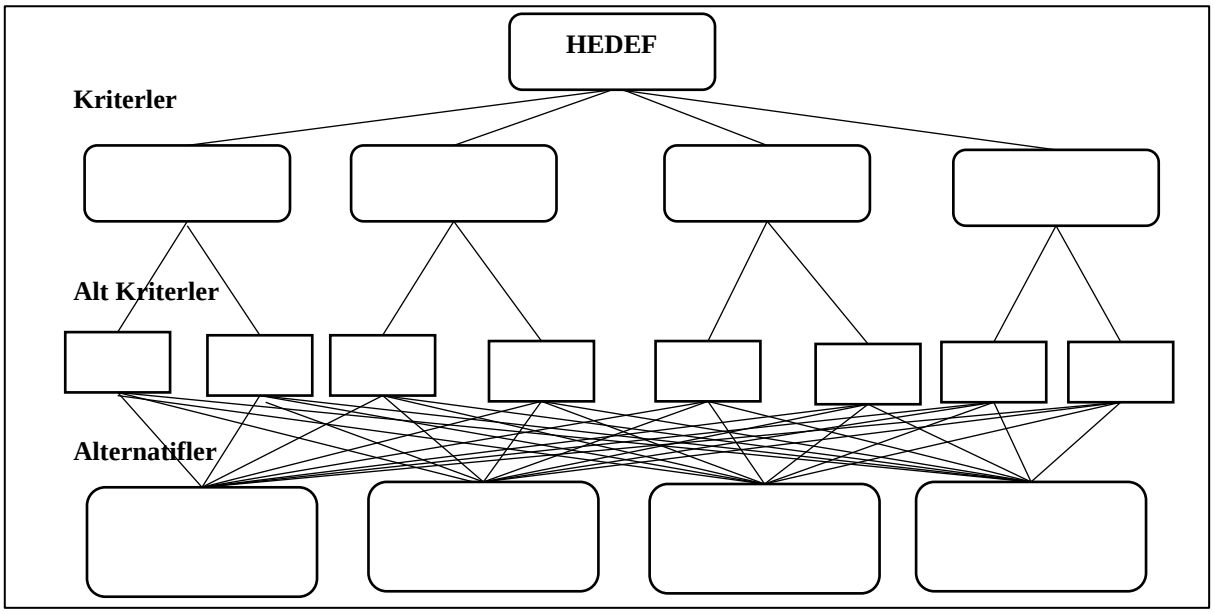
***4. Adım: Sonuçların geçerliliği için tutarlılık oranının hesaplanması*:** İkili karşılaştırmaların kendi içlerinde tutarlı olması için Tutarlılık Oranının (CR) 0.1'in altında yer alması gerekmektedir [51]. Tutarlılık oranı literatürde genellikle aşağıdaki yöntemle hesaplanmaktadır

Tutarlılık indeksi CI = $(\lambda_{max} - n)/(n - 1)$ hesaplanır. Tutarlılık oranı (CR = CI/RI), tanlo 2'den (RI =rassal tutarlık indeksi, λmax= ikili karşılaştırmalar matrisinin en büyük özvektör değeri ve n = sütun sayısını) yararlanarak hesaplanabilir. Farklı matris büyüklüklerine göre uygun CR değerleri oluşturulmuştur. 3*3 matriste CR değeri = 0.05; 4*4 matriste CR değeri = 0.08; daha büyük matrisler için bu değer 0.1'dir [56].

Tablo 2. Rassal indeks tablosu
(Random index table)

N	1	3	5	7	9	10
RI	0	0.58	1.12	1.32	1.45	1.49

5. Adım: Farklı amaçlar için göreli ağırlıkların kullanılması: Karar hiyerarşisinin her seviyesinde en yüksek puana sahip olan kriter diğer kriterlerden daha önemlidir. Alternatifler arasından seçim yapabilmek için son seviyedeki her bir elemanın göreli bileşik ağırlığı hesaplanmalıdır [55].



Şekil 1. AHS'nin hiyerarşik yapısı
(The hierarchical structure of AHS)

Tablo 1. İkili karşılaştırma ölçeği
(Binary comparison scale)

Önem Değerleri	Değer Tanımları
1	Her iki faktörün eşit öneme sahip olması durumu
3	1. Faktörün 2. faktörden daha önemli olması durumu
5	1. Faktörün 2. faktörden çok önemli olması durumu
7	1. Faktörün 2. faktöre göre çok güçlü bir öneme sahip olması durumu
9	1. Faktörün 2. faktöre göre mutlak üstün bir öneme sahip olması durumu
2, 4, 6, 8	Ara değerler

AHP yönteminin son aşamasında problemin çözümlenmesi gerekmektedir. Çözüm için problemin karar alternatifleri sıralanması için karma öncelikler vektörü hesaplanmalıdır. Söz konusu karma öncelikler vektörler bir değişkenin nihai olarak önceliklendirilmiş ağırlıklı ortalamalarından elde edilmektedir. Elde edilen nihai önceliklere göre karar alternatif puanı da denilmektedir. Sıralama ile karar vericiler alternatif kararlardan en yüksek puanı alanı veya herhangi bir alternatifi seçmektedir [55]. Bu süreç için genellikle literatürde Expert Choice paket programı kullanılmaktadır.

3.2. Araştırmanın Metodolojisi (Research Methodology)

AHS ve modelin uygulanma aşamaları kullanılarak kişisel verilerin korunması hususunda vatandaş algısının ölçülmesi amaçlanmıştır. Algının ölçülmesiyle vatandaşların kişisel verilerin korunmasına ilişkin endişeleri "*güvenirlik*", algı düzeyleri "*farkındalık*", zarara uğrama veya uğrama ihtimalinde "*ulaşılabilirlik*", yasal, idari ve teknolojik kapasite "*yeterlilik*" ve beklentiler "*gereklilik*" ana kriterleri ile ölçülmüş ve hesaplamalar yapılmıştır.

Vatandaş algısının ölçülmesi için beş ana kriter ve her bir ana kriterin altında dört alt kriter olmak üzere toplam yirmi alt kriter belirlenmiştir. Algının ölçülmesiyle kişisel verilerin işlenmesi ve korunması konusunda vatandaşların en hassas olduğu ana kriterin ve alt kriterlerin belirlenmesi hedeflenmiştir. Son olarak tüm değerlendirmeler yapıldıktan sonra "*güvenirlik temelli politika*", "*farkındalığın artırılması politikası*" ve "*gerekliliğin yükseltilmesi politikası*" alternatifleri değerlendirilmiştir.

Araştırmanın temel sınırlılığı ise örneklemin 40 kişi olmasıdır. Buna rağmen, aşağıda açıklanacağı üzere hem AHS modeli için en az 10 örneklemin yeterli olması hem de anketin yüz yüze uygulanması araştırmanın güvenirliğini yükseltmiştir.

Kişisel verilerin işlenmesi ve korunması konusunda çalışmalar yapan kişilerle ve daha önce gerçekleştirilen çalışmalar incelenerek 5 adet ana kriter ve 20 adet alt kriter belirlenmiştir. Kamu yönetimi güvenilirlik yoğun, farkındalığın artırılması, gerekliliğin yükseltilesi politikaları arasında seçim yapması gerektiği varsayılmıştır. Politikalar arasında seçim yapılması için beş ana kriter ve bunlara bağlı dört adet alt kriter oluşturulmuştur. Araştırma modelindeki amaç, ana kriterler, alt kriterler ve alternatifler tablo 3'te gösterilmiştir.

Tablo 3. Araştırmanın modeli
(Model of the research)

AMAÇ: Kişisel Verilerin İşlenmesi ve Korunması Konusunda Vatandaş Algısının Ölçülmesi					
ANA KRİTERLER					
	Güvenilirlik	**Farkındalık**	**Ulaşılabilirlik**	**Yeterlilik**	**Gereklilik**
ALT KRİTERLER	Resmi veya özel kurumların, işlediği kişisel verileri güvenli bir şekilde koruyabilmesi.	Kişisel Verilerin Korunması Kanunu hakkında bilgi sahibi olunması.	Kişisel verilerin kullanılarak zarara uğrandığında yardım ve destek alınabilmesi.	Kişisel verilerin korunması ve kimlik hırsızlığına karşı alınan kanuni veya idari tedbirler ile politikaların yeterli olması.	Kişisel verilerin korunması için daha sıkı idari ve yasal tedbirlerin alınması.
	İdari ve yasal tedbirler ile teknolojik önlemlerin kişisel verilerin korunmasında yeterli olması.	Kişisel verilerin işlenmesinin ve müşteri bilgi gizliliğinin korunması ve yükümlülüklerin kapsamlı olması.	Kişisel verilerin nasıl korunduğunu öğrenebilme ve isteğe bağlı değiştirebilme yetkisi.	Sosyal medya (facebook, twitter vb.) sitelerinin güvenlik önlemlerinin yeterli olması.	Çalışılan kurumda ve kamuoyunda kişisel verilerin korunmasına yönelik daha fazla eğitim ve bilgilendirme yapılması.
	Mevzuata uyum süreci kapsamında çalışılan yerdeki veri sorumlusunun ve veri işleyenin belirlenmesi.	Resmi veya özel kurumların kişisel verileri işleyerek başka kişilere ulaşmaya çalışması veya bilgileri paylaşması.	Sosyal medya hesaplarının kapatılmasına rağmen kişisel verilerin istenilen kurum ve şirketlere verilebilmesi.	Devletin kişisel verilerin korunması politikasının izlenebilir, denetlenebilir ve iyileştirilebilir olması.	Yasal ve idari düzenlemeler uyarınca veri sorumlusunun ve veri işleyenin yükümlülüklerinin açıklanması ve kontrol edilmesi.
	Siber saldırı veya personel hatalarına yönelik mevcut teknolojinin, önlemlerin ve kurum içi politikaların güven vermesi.	Kişisel verilerin 3. kişiler tarafından sık sık dolandırıcılık, sahtecilik, sanal korsanlık, siyasi kanaat değiştirme vb. amaçla kullanılması.	Hassas olamayan basit kişisel verilerden kişinin kimlik, sağlık, dijital vb. oldukça hassas bilgilerine erişebilme.	Çalışılan yerde kişisel ve idari veri güvenliğinin sağlanması için önlemlerin yeterli olması.	Kişisel verilerin güvenliğin sağlanması için daha ileri teknolojiler, sıkı önlemler alınması ve uluslararası işbirliğinin sağlanarak şeffaf düzenlemeler yapılması.
ALTERNATİFLER					
Güvenilirlik Yoğun Politika		**Farkındalığın Artırılması Politikası**		**Gerekliliğin Yükseltilesi Politikası**	

Araştırmanın yöntemi olarak betimsel araştırma seçilmiştir. Betimsel araştırmalar geçmişte veya hala var olan bir durumu ortaya çıkarmak için kullanılır. AHS modelinin uygulanmasında ve ikili karşılaştırmalar matrislerinin oluşturulmasında rastgele seçilen 40 kişinin görüşlerinden yararlanılmıştır. AHS yöntemi değerlendirme yapmak için çok sayıda veriye ihtiyaç duymamakta ve en az 10 örnek kullanılması durumunda değerlendirme yapabilmektedir [52,53]. İkili karşılaştırma matrislerinde vatandaşlardan elde edilen verilerin geometrik ortalaması kullanılmış [53] ve kişisel verilerin işlenmesi ile korunmasına ilişkin algının ölçülmesi amaçlanmıştır. Verilerin toplanmasında anket yöntemi kullanılmıştır. Tablo 3'te belirtilen araştırma modeline uygun anket formu hazırlanmış ve uygulanmıştır. Anketteki ana kriterlerin ve alt kriterlerin ağırlığını belirlemek, alternatiflerin sıralamasını yapmak ve verileri analiz etmek için AHS yönteminde Expert Choice paket programı ile yaş, cinsiyet, medeni durum gibi demografik verilerin analizinde SPSS 22 paket programı kullanılmıştır.

4. BULGULAR (RESULTS)

Ankete katılım sağlayanların cinsiyet, medeni durum, yaş, eğitim, aylık gelir, meslek ve daha önce kişisel verilerine ankete katılım sağlayanların izni olmadan erişim olup olmadığına dair soruya verilen cevapların sonuçları aşağıdaki tabloda sunulmuştur. Ankete katılım sağlayan 40 kişiye yöneltilen sorulara verilen cevapların yüzde analizi yukarıda sunulmuş olup cevaplar analiz edildiğinde; katılımcıların %35'i kadın ve %65'i erkektir. Katılımcıların yaş değişkeni açısında ağırlıklı olarak 35-44 (%32,5) yaş aralığında olduğu görülmüştür. Eğitim düzeyleri açısından katılımcıların dağılımı daha çok lisan düzeyine yoğunlaşmıştır. Aylık gelir açısından ise yoğunlaşma 5.001 ve üzeri (%40) TL arasındadır. Meslek kriterinde yoğunlaşma işçi (%77,5) değişkenindedir. Katılımcılar %32,5'i ise daha önce kişisel verilerine izinleri olmadan erişildiğini ifade etmiştir.

Demografik özellikler genel olarak değerlendirildiğinde dağılımın toplum yapısına uygun olduğunu söylemek mümkündür. Anketin giriş bölümünde sorulan "*daha önce kişisel verilerinize izniniz olmadan erişildi mi?*" sorusuna verilen cevaplar oldukça önemlidir. Katılımcıların üçte biri daha önce izinleri olmadan kişisel verilerine ulaşıldığını ifade etmiş olup anketin genel sonucu ile bağlantılı olarak endişelerin ve sorunun büyüklüğünü göstermiştir.

Kişisel verilerin korunmasına ilişkin vatandaş algısının ölçülmesi için beş ana kriter ve her ana kriterin altında dört adet alt kriter oluşturulmuştur. Öncelikle ana kriterlerin

ikili karşılaştırılması yapılmış daha sonra her bir ana kriterin altında yer alan dört adet alt kriterin ikili karşılaştırılması yapılmıştır. Böylece ana ve alt kriterlerin önem dereceleri ve ağırlıkları hesaplanmıştır. Sonuçlar aşağıdaki tablo 5'te sunulmuş olup diğer açıklamalar tablodan sonra yapılmıştır:

Tablo 4. Katılımcıların demografik özellikleri ve diğer bilgiler
(Demographic characteristics and other information of the participants)

		Sayı	**Yüzde (%)**		**Sayı**	**Yüzde (%)**
Cinsiyet	Kadın	14	35	Erkek	26	65
Medeni Durum	Bekâr	24	60	Evli	14	35
	Diğer	2	5			
Yaş	18-24	3	7,5	25-34	12	30
	35-44	13	32,5	44-54	11	27,5
	55 ve üzeri	1	2,5			
Eğitim	İlköğretim	4	10	Lise	4	10
	Lisans	23	57,5	Lisans Üstü	9	22,5
Aylık Gelir	0-2.500 TL	2	5	2.501-3.000 TL	6	15
	3.001-4.000 TL	14	35	4.001-5.000 TL	2	5
	5.001 ve üzeri	16	40			
Meslek	Öğrenci	3	7,5	İşçi	31	77,5
	Memur	4	10	Diğer	2	5
Daha önce kişisel verilerinize izniniz olmadan erişildi mi?	Evet	13	32,5	Hayır	27	67,5

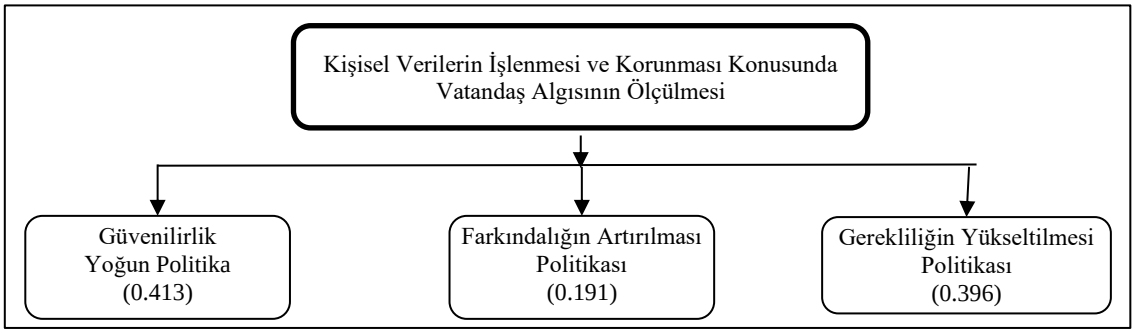
Tablo 5. Ana ve alt değerlendirme kriterlerinin ağırlıkları (Weights of main and sub-evaluation criteria)

Güvenilirlik (0.22)	Resmi veya özel kurumların, işlediği kişisel verileri güvenli bir şekilde koruyabilmesi.	0.427
	İdari ve yasal tedbirler ile teknolojik önlemlerin kişisel verilerin korunmasında yeterli olması.	0.329
	Mevzuata uyum süreci kapsamında çalışılan yerdeki veri sorumlusunun ve veri işleyenin belirlenmesi.	0.112
	Siber saldırı veya personel hatalarına yönelik mevcut teknolojinin, önlemlerin ve kurum içi politikaların güven vermesi.	0.132
Farkındalık (0.10)	Kişisel Verilerin Korunması Kanunu hakkında bilgi sahibi olunması.	0.148
	Kişisel verilerin işlenmesinin ve müşteri bilgi gizliliğinin korunması ve yükümlülüklerin kapsamlı olması.	0.082
	Resmi veya özel kurumların kişisel verileri işleyerek başka kişilere ulaşmaya çalışması veya bilgileri paylaşması.	0.317
	Kişisel verilerin 3. kişiler tarafından sık sık dolandırıcılık, sahtecilik, sanal korsanlık, siyasi kanaat değiştirme vb. amaçla kullanılması.	0.453
Ulaşılabilirlik (0.15)	Kişisel verilerin kullanılarak zarara uğrandığında yardım ve destek alınabilmesi.	0.181
	Kişisel verilerin nasıl korunduğunu öğrenebilme ve isteğe bağlı değiştirebilme yetkisi.	0.278
	Sosyal medya hesaplarının kapatılmasına rağmen kişisel verilerin istenilen kurum ve şirketlere verilebilmesi.	0.442
	Hassas olamayan basit kişisel verilerden kişinin kimlik, sağlık, dijital vb. oldukça hassas bilgilerine erişebilme.	0.099
Yeterlilik (0.21)	Kişisel verilerin korunması ve kimlik hırsızlığına karşı alınan kanuni veya idari tedbirler ile politikaların yeterli olması.	0.312
	Sosyal medya (facebook, twitter vb.) sitelerinin güvenlik önlemlerinin yeterli olması.	0.428
	Devletin kişisel verilerin korunması politikasının izlenebilir, denetlenebilir ve iyileştirilebilir olması.	0.129
	Çalışılan yerde kişisel ve idari veri güvenliğinin sağlanması için önlemlerin yeterli olması.	0.131
Gereklilik (0.32)	Kişisel verilerin korunması için daha sıkı idari ve yasal tedbirlerin alınması.	0.327
	Çalışılan kurumda ve kamuoyunda kişisel verilerin korunmasına yönelik daha fazla eğitim ve bilgilendirme yapılması.	0.132
	Yasal ve idari düzenlemeler uyarınca veri sorumlusunun ve veri işleyenin yükümlülüklerinin açıklanması ve kontrol edilmesi.	0.344
	Kişisel verilerin güvenliğin sağlanması için daha ileri teknolojiler, sıkı önlemler alınması ve uluslararası işbirliğinin sağlanarak şeffaf düzenlemeler yapılması.	0.197

Tablo 5 incelendiğinde değerlendirmeye alınan beş ana kriterden en yüksek ağırlığa sahip olan kriterin *gereklilik* (0.32) olduğu görülmektir. Gereklilik kriterini *güvenilirlik* (0.22), *yeterlilik* (0.21), *ulaşılabilirlik* (0.15) ve *farkındalık* (0.10) takip etmektedir.

Güvenilirlik ana kriteri alt kriter bazında değerlendirildiğinde "*resmi veya özel kurumların, işlediği kişisel verileri güvenli bir şekilde koruyabilmesi*", farkındalık ana kriterinde "*kişisel verilerin 3. kişiler tarafından sık sık dolandırıcılık, sahtecilik, sanal korsanlık, siyasi kanaat değiştirme vb. amaçla kullanılması.*", ulaşılabilirlik ana kriterinde "*sosyal medya hesaplarının kapatılmasına rağmen kişisel verilerin istenilen kurum ve şirketlere verilebilmesi.*", yeterlilik ana kriterinde "*sosyal medya (facebook, twitter vb.) sitelerinin güvenlik önlemlerinin yeterli olması.*" ve gereklilik ana kriterinde ise "*kişisel verilerin korunması için daha sıkı idari ve yasal tedbirlerin alınması.*" alt kriteri en yüksek öneme sahip alt kriterler olarak belirlenmiştir.

Ana ve alt kriterlerin ağırlıkları belirlendikten sonra Expert Choice programı kullanılarak alternatifler değerlendirmiştir. Çalışmanın uzunluğu dikkate alınarak sadece amaç üzerinden değerlendirme yapılmış ve şekil 2'de sonuçlar sunulmuştur:



Şekil 2. AHS sonuçlarına göre alternatiflerin önem dereceleri
(Significance of alternatives according to AHS results)

Vatandaşların politika taleplerinde üç alternatif belirlenmiştir. Ana kriter ve alt kriter bazında sonuçlar toplu olarak değerlendirildiğinde öncelikli politika beklentisinin *güvenilirlik yoğun* (0.413) olması gerektiği sonucuna ulaşılmıştır. Daha sonra ise sırasıyla *gerekliliğin yükseltilmesi* (0.396) ve *farkındalığın artırılması politikası* (0.191) politikaları talep edilmektedir.

5. SONUÇ VE DEĞERLENDİRME (CONCLUSION AND EVALUATION)

Sosyal medya sitesine veya herhangi bir internet sitesine dahi üye olurken birçok kişisel bilginin verilmesi ve bir kullanıcı sözleşmesinin onaylanması istenmektedir. Çoğu kullanıcı bilgileri doğru olarak vermekte ve kullanıcı sözleşmesini hiç okumadan veya okunsa dahi değiştirilemeden onaylamaktadır. Kullanım süresi arttıkça internet sitesi veya sosyal medya birçok kişisel veriyi doğrudan veya dolaylı yoldan toplamaktadır. Bazen siber saldırılar ile söz konusu kişisel veriler internet ortamında satılmakta, suiistimal edilmekte veya kişilere maddi kayıplar yaşatılmaktadır. Bunun bir diğer göstergesi ise son dönemde oldukça çok tartışılan kişisel verilerin siyasi tercihlerin yönlendirilmesinde kullanılmasıdır. Ayrıca birçok ülkenin istihbarat toplamak için kişisel verileri topladığı, kullandığı ve üçüncü kişilere sattığı bilinen bir gerçektir. Son bir yıl içinde Çin Halk Cumhuriyeti vatandaş puanlama sistemiyle bazı hizmetlerin alınmasının engellemesi, ülke dışına çıkışın yasaklanması, banka kanallara erişimin sınırlanması ve hatta hapis cezalarına varan bir sistemi devreye almayı planlamaktadır. Tüm bu gelişmeler kişisel verilerin işlenmesi ve korunması hususunu uluslararası kamuoyunun en önemli gündem maddelerinden biri haline getirmiştir.

Bu çalışmanın amacı, kişisel verilerin işlenmesi ve korunması konusunda vatandaş algısının ölçülmesidir. AHS metodundan faydalanılarak belirlenen beş ana kriter önem derecesine sıralanmış, ana kriterlere göre oluşturulan alt kriterler kıyaslanmış ve üç politika alternatifinin hangisinin seçilmesi gerektiği değerlendirilmiştir.

Yapılan analizlere göre vatandaşların en çok önem verdiği sırasıyla gereklilik, güvenilirlik ve yeterlilik kriterleri olmuştur. Ana kriterler genel olarak değerlendirildiğinde vatandaşların kişisel verilerin kullanılması için gerek yasal gerek idari gerekse teknolojik önlemlerin artırılması ve daha sıkı tedbirlerin alınması gerektiğini ifade etmişlerdir. Bunun yanı sıra gerek *güvenilirlik* gerekse *yeterlilik* kriterleri birlikte değerlendirildiğinde kişisel verilerin işlenmesi ve korunmasına yönelik kişi, kurum ve veri güvenliğine yönelik şüphelerin olduğu ve yasal, idari veya kurumsal yapının iyileştirme ihtiyaç duyulduğunu söylemek mümkündür. Bunların yanı sıra yasal ve idari düzenlemelerle hem kişisel verilerin işlenmesi ve korunmasına yönelik yasal, idari, teknolojik yapının yeterliğinin yükseltilmesine hem de herhangi bir ihlalde veya durumda kurumlara ulaşabilmenin mümkün olmasına, yasal hakların ve kişisel verilerin korumasının bilinmesine ihtiyaç vardır. Kişisel verilerin işlenmesi ve korunmasına yönelik daha fazla tanıtım, bilgilendirme, toplantı yapılması veya diğer kitle iletişim araçlarının kullanılması gerekmektedir.

Alt kriterlerin önem derecesi sonuçları incelendiğinde kamunun yasal ve idari düzenlemeler ve teknolojik önlemler ile kişisel verilerin korunmasına önem vermesi, kişisel verilerin üçüncü kişiler tarafından sık sık dolandırıcılık, sahtecilik, sanal korsanlık, siyasi kanaat değiştirme vb. amaçla kullanıldığı ve buna önlem alınması gerektiği, sosyal medya hesaplarının oldukça büyük miktarda kişisel veriyi topladığı ve kullandığı veya üçüncü kişilere sattığının farkında olunduğu, sosyal medya (facebook, twitter vb.) sitelerinin güvenlik önlemlerinin yeterli olmadığı ve kişisel verilerin korunması için daha sıkı idari ve yasal tedbirlerin alınması gerektiği sonuçlarına ulaşılmıştır. Genel bir değerlendirme yapıldığında, vatandaşların sosyal medya sitelerinin kişisel verilerin işlenmesi ve kullanılması konusunda endişe duyduklarını ve daha sıkı yasal ve idari tedbirlerin alınmasını talep ettiklerini söylemek mümkündür. Politika alternatifleri incelendiğinde ise, vatandaşlar sırasıyla *gerekliliğin yükseltilmesi* ve *farkındalığın artırılması politikasını* talep etmektedir. Bu çerçevede vatandaşların öncelikle kişisel verilerin işlenmesi ve kullanılması konusunda güvenliklerin sağlanmasını daha sonra mevcut yasal, idari ve teknolojik imkanların artırılmasını ve son olarak erişim, ihlal, kullanma gibi kişisel verilerin işlenmesi ve kullanılması konusunda farkındalıkların yükseltilmesini talep ettikleri sonucuna ulaşılabilir.

Çalışma içinde değerlendirmeye alınan boyutları çoğaltarak, azaltarak veya alt kriterleri yeniden değerlendirerek gerek kişisel verilerin korunmasına ilişkin makalelerde gerekse diğer çalışmalarda kullanmak mümkündür. Ayrıca kişisel verilerin işlenmesi ve korunması hususunda VIKOR, ANP, Bulanık AHS veya Bulanık ANP gibi diğer ÇKKV yöntemleri kullanılabilir.

KAYNAKLAR (REFERENCES)

[1] İnternet: 1995/46 EC Kişisel Verilerin İşlenmesi Sürecinde Kişilerin Korunmasına ve Verilerin Serbest Dolaşımına İlişkin Avrupa Konseyi Direktifi (Veri Koruma Direktifi). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3Aen%3AHTML, 15.02.2020.

[2] H. C. Aksoy, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Çakmak Yayınları, Ankara, 2010.

[3] İnternet: Avrupa Birliği Parlamentosu ve Konseyi, 2002/58 Sayılı Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve. Mahremiyetin Korunması Direktifi, OJ 2002 L 201, http://europa.eu.int/information_society/eeurope/2002/action_plan/pdf/actionplan_en.pdf, 15.02.2020.

[4] D. Konstantinos, R. Konstantinos, D. George, "A Dynamic Intelligent Policies Analysis Mechanism for Personal Data Processing in the IoT Ecosystem", *Big Data Cogn. Comput.* 4(2), 9, 2020.

[5] İnternet: Telekomünikasyon Sektöründe Kişisel Verilerin Korunması Alanında Çıkarılan Yönetmelik. 25365 sayılı ve 6 Şubat 2004 tarihli Resmi Gazete, https://www.resmigazete.gov.tr/eskiler/2004/02/20040206.htm, 15.02.2020.

[6] İnternet: Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik. 28363 sayılı ve 24 Temmuz 2012 tarihli Resmî Gazete, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=16405&MevzuatTur=7&MevzuatTertip=5, 15.02.2020.

[7] T. Teraoka, "Organization and exploration of heterogeneous personal data collected in daily life". *Hum. Cent. Comput. Inf. Sci*. 2(1), 2012.

[8] V. Zheng W. Y. Zheng, X. Xie,, Q. Yang, "Collaborative location and activity recommendations with GPS history data", ***19th international conference on World wide web (WWW '10)***, Association for Computing Machinery, New York, NY, USA, 1029–1038, 2010.

[9] G. Jim; Bell, C. L. Roger, "MyLifeBits: A personal database for everything", *Communications of the ACM*, 49, 89-95, 2006.

[10] A. Ç. Ayözger, **Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması**, Doktora Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, 2016.

[11] E. Şen, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", *İstanbul Barosu Dergisi*, 83(3), 1197-1214, 2009.

[12] E. Küzeci, "Anayasal Bir Hak: Kişisel Verilerin Korunması", *Bilişim Dergisi*, 128, 142-149, 2011.

[13] I. J. Lloyd, **Information Technology Law**, 6th Edition, Oxford University Press, Oxford, 2011.

[14] P. Carey, **Data Protection: A Practical Guide to UK and EU Law**, Third Edition, Oxford University Pres, Oxford, 2009.

[15] A. Murray, **Information Technology Law (The Law and Society)**, Oxford University Press, Oxford, 2010.

[16] S. Room, **Data Protection & Compliance in Context**, The British Computer Society Publishing and Information Product London, Swindon, United Kingdom, 2007.

[17] A. Akgül, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması,** Beta Yayınları, İstanbul, 2014.

[18] C. Kaya, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 69(1-2), 317-334, 2011.

[19] Š. Darius, L. Marius, "Treatment of biometrically processed personal data: Problem of uniform practice under EU personal data protection law", *Computer Law & Security Review*, 33(5), 618-628, 2017.

[20] İnternet: Kişisel Verilerin Korunması Kanunu. 29677 sayılı ve 07 Nisan 2016 tarihli Resmi Gazete, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf, 15.02.2020.

[21] H. Özdemir, "Haberleşmenin Gizliliği ve Kişisel Veriler", *EÜHFD*, XIII(1-2), 285-304, 2009.

[22] D. Kılınç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", *AÜHFD*, 61(3), 1089-1170, 2012.

[23] M. S. Çekin, "6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi", *İÜHFM*, C., 74 (2), 629-644, 2016.

[24] O. Şimşek, **Anayasa Hukuku Kişisel Verilerin Korunması**, Beta Yayınları, İstanbul, 2008.

[25] C. Terwangne, **The Right to be Forgotten and the Informational Autonomy in the Digital Environment**, European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, 2014.

[26] T. Henkoğlu, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Ankara, Yetkin Yayınları, 2015.

[27] E. Bucher, **Schweizerisches Obligationenrecht Allgemeiner Teil**, 2. Aufl., Zürich, 1988.

[28] S. Karlıdağ, "Ekonomi Politik Açıdan Kişisel Verilerin Korunması", *Amme İdaresi Dergisi*, 46(1), 127-152, 2013.

[29] A. Gözler, U. Taşçı, "Sınıf Öğretmenliği Bölüm Öğrencilerinin Bilişim Suçları", *Bilişim Teknolojileri Dergisi*, 8(3), 147, 2015.

[30] C. Paşaoğlu, E. Cevheroğlu, "Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması", *Bilişim Teknolojileri Dergisi*, 13(2), 183-195, 2020.

[31] N. Tekin, "Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", *Uyuşmazlık Mahkemesi Dergisi*, (4), 222-262, 2014.

[32] İnternet: F. X. Diebold, A Personal Perspective on the Origin(s) and Development of 'Big Data': The Phenomenon, the Term, and the Discipline, Social Science Research Network. Penn Institute for Economic Research (PIER), Research Paper Series, Paper No. 13-003 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2202843, 21.01.2020.

[33] M. Cox, D. Ellsworth, "Application-Controlled Demand Paging for Out-of-core Visualization", **8th Conference on Visualization 97**, Phoenix, AZ, U.S.A., 235- 244, 1997.

[34] K. Chen, G. Sun, L. Liu, "Towards Attack-Resilient Geometric Data Perturbation", **SIAM International Conference on Data Mining, Society for Industrial and Applied Mathematics**, 78-89, 2007.

[35] İnternet: Gartner It Glossary *BigData*, https://www.gartner.com/it-glossary/big-data/, 21.01.2020.

[36] O. Hamami, "Big Data Security: Understanding the Risks", *Business Intelligence Journal*, 19(2), 20-26, 2014.

[37] İnternet: What is Big Data?, https://www.newgenapps.com/technology/big-data, 21.01.2020.

[38] H. A. Ünver, G. Kim, "Türkiye'de Veri Gizliliği ve Gözetimi: Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirilmesi", *Ekonomi ve Dış Politika Araştırmalar Merkezi*, İstanbul, 2016.

[39] J. Warner, "The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps", *University of Ottowa Law&Technology Journal*, 2, UOLTJ 75, 75-104, 2005.

[40] P. Pehlivan, "Türkiye'de Katılım Bankacılığı ve Bankacılık Sektöründeki Önemi", *Sosyal Ekonomik Araştırmalar Dergisi*, 16(31), 2016.

[41] Ö. Kutlu, S. Kahraman, "Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi", *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, 5(4), 2017.

[42] L. Keser, M. B. Kaya, B. Kınıkoğlu, "Hukuki Analiz, Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi", *İstanbul Bilgi Üniversitesi & TEPAV Dergisi*, 39-74, 2014.

[43] İnternet: Türkiye Cumhuriyeti Anayasası, (1982).17863 Mükerrer sayılı ve 9 Kasım 1982 tarihli Resmi Gazete, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf, 21.01.2020.

[44] F. Y. Partovi, "Determining What to Benchmark: An Analytic Hierarchy Process Approach", *International Journal of Operations &Production Management*, 14(6), United Kingdom, 1994.

[45] F. Wu, "Housing Environment Preference of Young Consumers in Guangzhou, China: Using The Analytic Hierarchy Process", *Property Management*, 28(3), 174-192, 2010.

[46] P. K. Dey, E. K. Ramcharan, "Analytic Hierarchy Process Helps Select Site for Limestone Quarry Expansion in Barbados", *Journal of Environmental Management*, 88, 1384-1395, 2008.

[47] T. L. Saaty, "How To Make A Decision: The Analytic Hierarchy Process", *Interfaces*, 24(6), 1994.

[48] M. J. Liberatore, R. L. Nydick, "The Analytic Hierarchy Process in Medical and Health Care Decision Making: A Literature Review", *European Journal of Operational Research*, 189 (1), 194-207, 2008.

[49] M. Punniyamoorty, M. Ponnusamy, G. Lakshmi, "A Combined Application of Structural Equation Modeling (SEM) And Analytic Hierarchy Process (AHP) in Supplier Selection. Bencmarking", *An International Journal*, 19 (1), 70-92, 2012.

[50] S. Vinodh, K. R. Shivraman, S. Viswesh, "AHP-Based Lean Concept Selection in A Manufacturing Organization", *Journal of Manufacturing Technology Management*, 23 (1), 124 – 136, 2012.

[51] C. Chang, C. Wu, C. Lin, H. Lin, "Evaluating Digital Video Recorder Systems Using analytic Hierarchy and Analytic Network Processes", *Information Sciences*, 177, 3383–3396, 2007.

[52] T. Ustasüleyman, "Bankacılık Sektöründe Hizmet Kalitesinin Değerlendirilmesi: AHS-TOPSIS Yöntemi", *Bankacılar Dergisi*, 69, 2009.

[53] P. Lam, K. Chin, "Identifying and Prioritizing Critical Success Factors For Conflict Management in Collaborative New Product Development", *Industrial Marketing Management*, 34, 761– 772, 2005.

[54] J. Yang ve H. Lee, "An AHP Decision Model For Facility Location Selection", *Facilities*, 15(9-10), 241-254, 1997.

[55] E. W. L. Cheng, H. Li, D. C. K. Ho, "Analytic Hierarchy Process (AHP), A Defective Tool When Used Improperly", *Measuring Business Exellence*, 6(4), 2002.

[56] K. I. Shyjith, S. Kumanan, "Multi-criteria decision-making approach to evaluate optimum maintenance strategy in textile industry", *Journal of Quality in Maintenance Engineering*, 14(4), 375-386, 2008.