ANKARA
HACI BAYRAM VELİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN MİKROÇİPLER

Defne Nur KAZANBAŞ

Tez Danışmanı

Prof. Dr. Dilşad KESKİN

YÜKSEK LİSANS TEZİ

ÖZEL HUKUK ANABİLİM DALI

MEDENİ HUKUK BİLİM DALI

EYLÜL 2023


ankara
HBM

KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN MİKROÇİPLER

Defne Nur KAZANBAŞ

YÜKSEK LİSANS TEZİ

ÖZEL HUKUK ANABİLİM DALI

MEDENİ HUKUK BİLİM DALI

ANKARA HACI BAYRAM VELİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

EYLÜL 2023

ETİK BEYAN

Ankara Hacı Bayram Veli Üniversitesi Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Defne Nur KAZANBAŞ

05.09.2023

TEZ ONAY SAYFASI

Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü Medeni Hukuk Anabilim Dalı Medeni Hukuk Programı yüksek lisans öğrencisi tarafından hazırlanan Kişisel Verilerin Korunması Açısından Mikroçipler Başlıklı tez çalışması 05/09/2023 tarih ve 15.30 saatinde yapılan tez savunma sınavında aşağıdaki jüri tarafından OY BİRLİĞİ ile YÜKSEK LİSANS TEZİ olarak KABUL edilmiştir.

	Kabul	**Ret**
Başkan (Prof. Dr. A. Dilşad KESKİN):	X	
Üye (Dr. Öğr. Üyesi Esen KABAŞ TEZCAN):	X	
Üye (Dr. Öğr. Üyesi Elif AYAN DURHAN):	X	

KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN MİKROÇİPLER

(Yüksek Lisans Tezi)

Defne Nur KAZANBAŞ

ANKARA HACI BAYRAM VELİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Eylül 2023

ÖZET

Gelişen teknoloji ve paylaşımın arttığı dijital çağda bireylerin bilgilerinin korunması gerekliliği ortaya çıkmış ve bu kapsamda gerek uluslararası gerekse ulusal alanda birçok düzenleme yapılmıştır. Teknik adıyla bireylerin bilgileri, kişiyi belirleyen veya belirleyebilecek olan kişisel veri adı altında tanımlanmıştır. Kişisel veriler bireyi ayırt edici birçok bilgi anlamına gelmektedir. Kişisel veri paylaşımının artmasıyla bu verilerin ticaretinin yapıldığı ve bireylerin mağduriyetler yaşamaları söz konusu olmuştur. Kişisel veriler birey için önem arz etmekte olup korunmaları için birtakım idari ve teknik tedbirler alınması gerekmektedir. Teknolojinin gelişmeye devam etmesiyle birlikte kişisel veri işleme yollarının artması ve farklılaşması akla deri altı mikroçiplerin kullanımının yaygınlaşması halinde kişisel verilerin korunması alanında nasıl bir durum ortaya çıkacağını getirmiştir. Mikroçiplerle kişisel verilerin işlenmesinin söz konusu olması durumunda bu hususa ilişkin düzenlemeler yapılması ve ek tedbirlerin alınması gerekmektedir.

Bilim Kodu	:	51001
Anahtar Kelimeler	:	Kişisel verilerin korunması, 6698 Sayılı Kanun, Mikroçipler
Sayfa Adedi	:	135
Tez Danışmanı	:	Prof. Dr. A. Dilşad KESKİN

MICROCHIPS FOR THE PROTECTION OF PERSONAL DATA

(M.Sc. Thesis)

Defne Nur KAZANBAŞ

ANKARA HACI BAYRAM VELİ UNIVERSITY

GRADUATE SCHOOL FOR ANKARA HACI BAYRAM VELİ UNIVERSITY

September 2023

ABSTRACT

In the digital age, where the developing technology and sharing increase, the necessity of protecting the information of individuals has emerged and many regulations have been made both in the international and national areas. With its technical name, the information of individuals is defined under the name of personal data that identifies or can identify the person. Personal data means a lot of information that distinguishes the individual. With the increase in personal data sharing, this data is traded and individuals experience grievances. Personal data is important for the individual and some administrative and technical measures should be taken to protect them. With the continuing development of technology, the increase and differentiation of personal data processing methods has brought to mind what kind of situation will arise in the field of personal data protection if the use of subcutaneous microchips becomes widespread. In case of processing personal data with microchips, it is necessary to make regulations and take additional measures regarding this issue.

Science Code	:	51001
Key Words	:	Protection of the Personal Data, Law No. 6698, Microchips,
Page Number	:	135
Supervisor	:	Prof. Dr. A. Dilşad KESKİN

ÖNSÖZ

Hayat kurma telaşının henüz başlarındayken hevesle başladığım yüksek lisans sürecim; hukuk büromuzun açılışı, kişisel verilerin korunması alanında danışmanlık verdiğimiz Odak Veri Danışmanlık Limited Şirketi'nin açılışı, artan iş yükü, düğün hazırlıkları ve aile kurma çabasıyla uzun uğraşlarımı aldı. Yaklaşık 3 senedir aktif bir şekilde serbest avukatlıkla uğraşırken avukatlık stajım döneminde öğrendiğim kişisel verilerin korunması hukuku alanında 3. senesine girmek üzere olan Odak Veri Danışmanlık şirketimiz ile Konya ve daha birçok ilde sayısı 100'ü geçmiş şirkete kişisel verilerin korunması alanında danışmanlık hizmeti vermiş bulunmaktayız. Mesleğimde bu alan üzerine uzmanlaşmam ve uygulamadan pek çok örnek görmüş olmam bu alana ilişkin gelişmeler açısından beni düşündürür oldu ve böylelikle mikroçiplerin kullanımı halinde kişisel verilerin korunması açısından mikroçiplerle kişisel veri işlenmesine ilişki değerlendirmelerde bulunduğum yüksek lisans tezimi yazmaya başladım.

Tezin yazım aşamalarında bilgi ve yardımlarını esirgemeyen, bana her daim anlayışla yaklaşan, her konuda yardım eden, yazım aşamasında umudumu kaybetmememi sağlayan, yönlendirmeleri ve önerileriyle vermiş olduğu destekten ötürü **Sayın Prof. Dr. Dilşad KESKİN**'e sonsuz teşekkürlerimi sunarım.

Tez çalışmamın tamamlanması aşamasında birlikte çalıştığımız hukuk büromuzun ve danışmanlık şirketimizin yoğun iş programına rağmen göstermiş olduğu sabrı, ilgisi, bana olan inancı ve desteği için iş ortağım ve eşim **Sevgili Av. Fatih Sultan KAZANBAŞ**'a yürekten teşekkür ederim.

Tez çalışmamın yanı sıra tüm eğitim-öğretim hayatım boyunca benim için emek sarf eden, akademik çalışmalarım konusunda beni teşvik eden ve türlü fedakarlıklarda bulunan babam **Mustafa YANAR'a** ve annem **Meral YANAR'a** ve kardeşlerim **Onur YANAR** ile **Elif YANAR'a** tüm kalbimle teşekkür ederim.

İÇİNDEKİLER

KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar aşağıda açıklamalarıyla birlikte sunulmuştur.

Kısaltmalar	Açıklama
Bkz.	Bakınız
C.	Cilt
CETS	Council of Europe Treaty Series (Avrupa Konseyi Antlaşma Serisi)
E.	Esas
EC	Europian Council (Avrupa Komitesi)
f.	Fıkra
FDA	Food And Drug Administration (Gıda Ve İlaç Komitesi)
GDPR	General Data Protection Regulation (Genel Veri Koruıma Tüzüğü)
K.	Karar
KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu
m.	Madde
MR	Emar (Manyetik Rezonans Görüntüleme)
NFC	Near Field Communication (Yakın Alan İletişimi)
OECD	Ekonomik İşbirliği ve Kalkınma Örgütü
RFID	Radio Frequency Identification (Radyo Frekansıyla Tanımlama)
s.	Sayfa
S.	Sayı
vb.	Ve benzeri
vd.	Ve devamı
VERBİS	Veri Sorumluları Sicili
YÜHFD	Yeditepe Üniversitesi Hukuk Fakültesi Dergisi

1. GİRİŞ

Gelişen teknoloji ve dijital haberleşme çağı bireyleri teknoloji kullanımından çıkarmış ve teknolojinin bireyleri kullanmasına yol açmıştır. Teknolojinin bireyleri kullanmasının bir örneği, günümüzde bilişim ve teknoloji aracılığıyla bireylerin kişisel verileri alınarak bireylere reklam ve pazarlama faaliyetleri yapılmasıdır. Teknik adıyla "veri ticareti" ismini verdiğimiz bu faaliyet bireylerin kişisel verilerinin hukuka uygun veya uygun olmayan yollarla elde edilerek ticari amaçlar için kullanılmasını kapsamaktadır. Kişisel verilerin korunması düşüncesinin temelinde bireylerin mahremiyetine saygı duyulması, özel hayatının gizliliğinin sağlanması ve bireyin rızası dışında kişisel verilerinin ticaretinin yapılmasının önüne geçilmesi gerektiği kaygısı bulunmaktadır.

Zamanla küçülen teknoloji önce ceplerimize, cebimizdeki telefonlardan kolumuzdaki saatlere ve en sonunda hepsi elimizdeki bir çipe ya da kolumuzdaki bir ekrana dönüşebilecektir. Teknoloji insanlar tarafından taşınabilirken ya da giyilebilirken şimdi derialtına girmesi söz konusudur. Mikroçip kavramı karşımıza hep endüstriyel anlamda çıkmış ve sanayilerde kullanılmıştır. Belki de sadece bilim kurgu filmlerinde gördüğümüz deri altı mikroçipler, belli bir süre sonra hepimizin deri altında olacak ve bu durum normalleşecektir. Endüstriyel mikroçiplerin bulunduğu ve kullandığımız birçok cihazla her tip veri işlenebilirken deri altı mikroçiplerle basit tipte faaliyetlerinin yanı sıra bireylerin kişisel verilerinin de işlenmesi durumu söz konusu olacaktır.

Geçmişten bugüne deri altı mikroçipleri konusunda araştırmalar ve çeşitli deneyler yapılmaya devam etmektedir. Deri altı mikroçip kullanımının son yıllarda popülerleştiği ve kullanım oranının sayıca arttığı gözlemlenmektedir. Avrupa ve Amerika öncelikli olmak üzere farklı ülkelerde deri altı mikroçip üretimi yapan şirketler bulunmaktadır. Şirketlerin çalışmaları günlük kapı açmak arabayı çalıştırmak gibi basit işlerimizi mikroçiple yapmak, sağlık bilgilerimize mikroçipten ulaşılması, ödeme işlemlerini mikroçiple yapmak ve mikroçip kullanımını artırmak üzerine devam etmektedir.

Kişisel veri en basit tanımıyla kişiyi ayırt edici verilere denmektedir. Kimlik bilgileri, iletişim bilgileri, sağlık bilgileri kişisel veri türüdür. Kişisel verilerin aleyhe kullanılmaması için idari ve teknik tedbirler alınmalıdır. Hukukumuzda 6698 sayılı

Kişisel Verilerin Korunması Kanunu bu amaçla yürürlüğe girmiştir. Bu çalışmanın birinci bölümünde kişisel veri kavramına, kişisel verilerin korunmasına, kişisel verilerin korunması kanununa, kişisel verilerin korunması kanunu kapsamındaki yükümlülüklere ve uygulamada kişisel verilerin korunmasına değinilmiş olup ikinci bölümünde mikroçip kavramına mikroçiplerin tarihsel gelişimine, deri altı mikroçiplerin kullanım alanlarına ve mikroçiplerle kişisel veri işlenmesi anlatılmıştır. Üçüncü bölümde ise mikroçiplerin kullanımında kişisel verilerin korunması açısından yaşanabilecek sorunlardan bahsedilmiştir.

2. KİŞİSEL VERİLERİN KORUNMASI HUKUKU

2.1. Kişisel Verilerin Korunmasına İlişkin Temel Kavramlar

2.1.1. Kişisel Veri Kavramı

Kişisel veri, bir kişiye ait olan ve o kişiyi belirlenebilir kılan her türlü bilgiye verilen genel addır. Kişisel veriyi diğer bilgilerden ayıran özellikleri anmak suretiyle yapılan bu tanımlama usulüne kişisel verilerin korunması hukukunda çokça rastlanmaktadır. Gerçekten kişisel verilerin korunması hukukunda öncü kaynaklardan biri haline gelen Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation) de kişisel veri kavramını "tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Veri koruma hukukunun ilk uluslararası düzenlemesi olan OECD(Ekonomik İşbirliği ve Kalkınma Örgütü)'nin "Kişisel Verilerin Sınıraşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri"nde de aynı tanıma yer verdiği görülmektedir.

Veri koruma hukukunun uluslararası doktrinine bakıldığında ise önde gelen tanımların aynı doğrultuda olduğu görülecektir. Örneğin Avrupa Komisyonu kişisel veriyi "kimliği belirli veya belirlenebilir canlı bir bireye ilişkin her türlü bilgi" olarak tanımlamıştır[1].

Türk Hukukunda ise kişisel verinin tanımı 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklinde yapılmıştır. Kişisel verilerin korunmasına ilişkin diğer mevzuatta da buna benzer tanımlar yer almaktadır. Türk veri koruma hukukunun ikincil mevzuatında, Kişisel Verileri Koruma Kurumu'nun yardımcı rehberlerinde ve kararlarında da aynı tanım kullanılmaktadır. Kamu otoritesi yanında Türk hukuk doktrininde de kişisel veri benzer şekilde tanımlanmıştır.

Kişisel verilerin kapsamına ve sayısına ilişkin belirlilik yoktur. Bir bilginin kişisel veri olup olmadığının tespitine yönelik bazı kriterlerden bahsedilebilse de bu kriterler; kesin, somut ve genel olmamakla birlikte yalnızca bir değerlendirme kriteri olarak düşünülebilecektir. Gerçekten Türk veri koruma otoritesinin dikkate aldığı

[1]European Commission. "What is Personal Data*?",* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en, Erişim: 05.05.2021.

kriterlere[2] bakıldığında bir bilginin kişisel veri olup olmadığının tespitinde; verinin bir gerçek kişiye ait olması, verinin sahibi olan kişiyi belirlenebilir kılması, bu özellikler bulunduğu durumda veri niteliğini haiz olması şartlarının varlığının arandığı görülmektedir[3]. Oysa bu kriterlerin genel ve tüm hukuk sistemleri için kapsayıcı olmadığı ortadadır. Nitekim kişisel verinin yalnızca gerçek kişilere ait olması kriteri üzerinde doktrinde tartışmalar mevcut olup tüzel kişilerin de kişisel verilerinin bulunabileceği yönünde görüşler vardır. Yine bunun gibi "verinin sahibi olan kişiyi belirlenebilir kılması" kriterinin de kesin ve somut olduğunu söylemek güçtür. Zira "belirlenebilir kılmak" kavramı her ne kadar Türk veri koruma otoritesi tarafından, verinin ilgili kişinin kimliğini göstermesi yahut kimliğini doğrudan göstermese de herhangi bir kayıtla ilişkilendirilmesini sağlaması, böylece kişinin kimliğini ortaya çıkarır nitelikte olması, şeklinde açıklansa da bu hususta kesin bir sonuca varılamayacaktır. Gerçekten "kişinin herhangi bir kayıtla ilişkilendirilmesi" kriterinin ölçüsü net bir şekilde ortaya konulamamaktadır. Yalnızca devlet otoritesi altında tutulan kayıtların mı bu hususta kabul göreceği yoksa her türlü kaydın mı bu niteliği sağlamaya elverişli olacağı, dolayısıyla kayıtların geçerlilik ölçütünün neye göre belirleneceği gibi bazı sorunlar söz konusudur. Tüm bunlar kişisel verinin tanımı yanında bir verinin "kişisel veri" niteliğini kazanması için taşıması gereken kriterlerin de kesin, somut ve genel bir şekilde tespit edilemeyeceğini ortaya koymaktadır.

Bu çalışmada her ne kadar kişisel verinin tanımlanmasının ve kriterlere bağlanmasının mümkün olmadığı görüşüne katılsak da izah edilecek konuların somutlaşması ve anlaşılabilmesi maksadıyla kişisel veri kavramına Türk veri koruma mevzuatı ve Türk veri koruma otoritesinin değerlendirmeleri temel alınmıştır[4].

---

[2] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler."100 Soruda Kişisel Verilerin Korunması Kanunu", s. 17, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf, Erişim: 07.07.2021.

[3] Boz, A. (2014). *Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri,* Yayımlanmamış Yüksek Lisans Tezi, Ankara, s. 9; Başalp N. (2004). *Kişisel Verilerin Korunması Ve Saklanması*, Yetkin Yayınları, Ankara, s. 21; Özdemir, H.(2009). *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması,* Seçkin Yayıncılık., s. 150; Aksoy, H.C. (2010). *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması"* 1. Bası, Çakmak Yayınevi, Ankara, s. 22.

[4] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi." Kişisel Verilerin Korunması Kanunu Ve Uygulaması", s. 21-22, https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%0K ORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf, Erişim: 08.09.2021.

2.1.2. Özel Nitelikli Kişisel Veri Kavramı

Özel nitelikli kişisel veri, kişisel veri niteliğinin yanı sıra bazı diğer özellikleri barındıran kişisel verilerdir. Özel nitelikli kişisel verinin net bir tanımı olmamakla birlikte, kişisel veri alanında Avrupa'da geçerli mevzuat olan General Data Protection Regulation (GDPR), "Özel Kategorilerdeki Kişisel Verilerin İşlenmesi" başlıklı 9. maddesinde bazı kişisel verileri sayarak bunların işlenmesinin yasak olduğunu ifade etmiştir. Buradan hareketle GDPR'ın "ırk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel veriler ve bir gerçek kişinin kimliğinin teşhisine yönelik genetik veriler ile biyometrik veriler, sağlık ile ilgili veriler veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin veriler"i özel nitelikli kişisel veri olarak kabul ettiği görülmektedir.

Türk veri koruma hukukunda da kanun koyucu yaptığı tanımda Kişisel Verilerin Korunması Kanunu(KVKK)'nun 6. maddesinde özel nitelikli kişisel veriyi, "kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançlar, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleri ile ilgili verileri ile biyometrik ve genetik veriler" olarak tanımlanmıştır. Kanunda yapılan bu tanımın yanı sıra "hassas veri"[5] olarak da isimlendirilen özel nitelikli kişisel veriler Türk veri koruma otoritesi tarafından yapılan kriter bazlı tanımda "öğrenilmesi halinde ilgili kişinin mağdur olmasına ya da ayrımcılığa maruz kalmasına neden olabilecek nitelikte veriler" olarak tanımlanmıştır. Özel nitelikli kişisel verilerin öğrenilmesi halinde veri sahibinin mağdur olabileceği ya da ayrımcılığa tabi tutulabileceği bir durumun ortaya çıkması söz konusu olacaktır.

Kanun koyucu ile veri koruma otoritesinin yapmış olduğu bu iki farklı tanımlama usulü birtakım sorunları beraberinde getirmektedir. Bu sorunlardan başta

[5] Orak, B. (2019). *Kişisel Sağlık Verilerinin Korunması,* Yetkin Yayınları, Ankara, s. 9; Bayındır, H. (2019). *Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması,* Yayımlanmamış Yüksek Lisans Tezi, İstanbul, s. 25; Kişisel Verileri Korunma Kurumu Resmi Web Sitesi. Rehberler. "Özel Nitelikli Kişisel Verilerin İşlenme Şartları", s. 1, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0ef45a05-ac30-4f35-bc4b-3b2cbefc9864.pdf, Erişim: 08.07.2021; Kaya C. (2011). "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas(Kişisel) Veriler ve İşlenmesi", İÜHFM, C.LXIX, No:1-2, s. 317-334, s. 319-320, http://dergipark.gov.tr/download/article-file/97634, Erişim: 07.07.2021; Veri türlerinin isimlendirmelerine ilişkin farklı tanımlamalar da görülmektedir, bkz.: Wang M./Jiang Z. (2017). "The Defining Approaches and Practical Paradox of Sensitive Data:An İnvestigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World", İnternatiol Journal of Communication, No:11, Çin, s. 3286-3305, s. 3291, http:// ijoc.org/index.php/ijco/article/viewFile/6892/2111, Erişim: 07.07.2021.

geleni; KVKK m.6'da yapılan tanımın örneklendirme mi yoksa bir sınırlandırma mı olduğunun tespitidir. Kanaatimizce özel nitelikli kişisel veriler sınırlı sayıda değildir. Gelişen teknoloji ve iletişim çağında kişinin mağduriyetine yol açabilecek başka veri tipleri ile karşılaşılabilecektir. Bunun yanında bir başka sorun ise; bir kişisel verinin özel nitelikli kişisel veri olup olmadığının tespitinde bu verinin Kişisel Verilerin Korunması Kanununda yapılan örneklendirmeye dahil olan veri olmasının yanında ilgili kişiyi mağdur etme ya da ayrımcılığa maruz bırakma potansiyeline sahip olmasının aranıp aranmayacağıdır. Burada varılması gereken sonuç kanaatimizce; bir kişiyi mağdur edebilme ya da ayrımcılığa maruz bırakabilme ihtimalinin tespitinde Kanun'da sayılan özel nitelikli kişisel verilerin yanı sıra bu duruma sebebiyet verecek olan veri türünün de doğrudan bu nitelikte kabul edilmesi gerektiğidir.

2.1.3. Veri İşleme Kavramı

Veri işleme, kişisel veri üzerinde yapılan her türlü faaliyet olarak tanımlanabilir. GDPR veri işleme kavramını şu şekilde tanımlamıştır: "İşleme faaliyeti, otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisidir". KVKK'da ise farklı terimlerle buna benzer bir tanım getirilmiştir[6]. Bu tanımda kastedilen otomatik yollarla işleme faaliyeti, insan müdahalesi olmadan yapılan kişisel veri işleme faaliyetidir. Otomatik yollarla veri işleme faaliyetine örnek olarak kamera kayıtları, araç lokasyon takip sistemleri, internet sitesi çerezleri, internet sitesi alışveriş geçmişi gösterilebilir. Otomatik olmayan yollarla işleme ise örneğin ziyaretçi kayıtlarının sekreter tarafından tutulması, fatura bilgilerinin muhasebe programına personel vasıtasıyla girilmesi gibi insan müdahalesi içeren işleme faaliyetidir.

[6] 6698 sayılı Kişisel Verileri Koruma Kanunu (2016). Resmi Gazete. https://www.resmigazete.gov.tr/eskiler/2 0 16/04/20160407.htm, Erişim: 07.07.2021.

2.1.4. Kişisel Veri Sahibi ve İlgili Kişi Kavramları

Kişisel veri sahibi ya da ilgili kişi kavramları, farklı düzenlemelerde aynı anlamda kullanılmakta olan ve verinin ait olduğu kişiyi ifade eden kavramlardır. Bu kavram, GDPR'da "kişisel veri sahibi", KVKK'da ise "ilgili kişi" olarak anılmaktadır[7].

İlgili kişiler, kişisel verilerin sahipleri olarak birtakım haklara sahiptirler. Bu haklardan başlıcaları; kişisel verilerinin işlenmesine rıza göstermek, unutulma hakkı kapsamında bunların yok edilmesini istemek, kişisel verileri hakkında bilgi talep etmek ve kişisel verilerinin değiştirilmesini ve güncellenmesini sağlamaktır. Bu hakların kullanılması ilgili mevzuatta bazı şekil şartlarına tabi tutulmuştur. İlgili kişinin fiil ehliyetine sahip olmaması halinde bu haklar, kanuni temsilcileri vasıtasıyla kullanılır.

2.1.5. Veri İşleyen Kişi Gruplarına İlişkin Kavramlar

Kişisel verileri himayesinde bulunduran ve bu veriler üzerinde işleme faaliyeti gerçekleştiren kişi grupları, bu faaliyetlerin türlerine göre ayrılmaktadır. Bunlar, aşağıda kontrolör[8] ve veri sorumlusu ile işleyici ve veri işleyen şeklinde gruplar halinde incelenmiştir.

2.1.5.1. Kontrolör ve veri sorumlusu kavramları

Kontrolör ve veri sorumlusu kavramları, ulusal ve uluslararası düzenlemelerde aynı veya benzer anlamlarda kullanılan kavramlardır. Kontrolör, kişisel veri işleme faaliyeti gerçekleştirip bu faaliyetin amaç, yöntem ve kapsamını belirleme noktasında tasarruf yetkisine sahip kişi ya da kuruluş olarak tanımlanabilir. GDPR'da yapılan tanımda kontrolörün kişisel verilerin işlenmesine dair amaç ve yöntemleri belirleyen tüzel ya da gerçek kişi kamu kurumu kuruluşu ya da diğer herhangi bir organı olabileceği ifade edilmiştir. KVKK'da yapılan veri sorumlusu tanımında da amaç ve vasıta belirlemesi yönünden GDPR'a paralel bir tanım yapılarak "veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan tüzel ya da gerçek kişi" şeklinde bir tanım yapılmıştır. Bu iki tanım arasındaki farklılığa bakıldığında GDPR'ın tüzel ya da

[7] Voigt, P./ Bussche, A. (2017). "The EU General Data Protection Regulation (GDPR): A practical Guide", Switzerland, Springer, s. 2.
[8] Demirezen, M. (2020). *Kişisel Verilerin Korunması Hukuku ve Uyum Projelerinin Yürütülmesi*, Platon Yayıncılık, İstanbul, s. 41.

gerçek kişiler yanında bu sıfata sahip olmayan kamu kuruluşu ve organlarını da kapsayıcı bir tanım yapmasına karşılık, KVKK'nın veri sorumlusu sıfatını tüzel ya da gerçek kişi olma şartına dayandırdığı görülecektir. Oysa Türk veri koruma hukuku otoritesi olan Kişisel Verileri Koruma Kurumu'nun 25.06.2021 tarihli duyurusuna bakıldığında Türk hukukunda tüzel kişiliğe sahip olmayan adi ortaklığın veri sorumlusu olabileceği yönünde hüküm kurulduğu ya da karar verildiği görülmektedir. Buradan hareketle Türk veri koruma mevzuatında yapılan veri sorumlusu tanımının, Türk hukukunun gereklerine hizmet edemediği, Türk veri koruma otoritesince alınan kararla açıklığa kavuşmuştur. Buna karşın yine Türk veri koruma otoritesinin apartman ve site yöneticilikleri hakkında vermiş olduğu 22.07.2020 tarih 2020/560 sayılı ilke kararında[9] apartman ve site yöneticilerinin veri sorumlusu olamayacağının belirtildiği, gerekçe olarak da bunların tüzel kişiliği haiz olmamasını gösterdiği anlaşılmaktadır. Birbirine zıt olan bu kararlar, bu konuda Türk veri koruma mevzuatının yeterli bir düzenlemeye sahip olmadığını göstermektedir. Her ne kadar Türk veri koruma otoritesinin mevzuattaki açık tanıma aykırı bir karar alarak tüzel kişiliğe sahip olmayan adi ortaklık gibi kurumların da veri sorumlusu olabileceği yönünde görüş bildirmesinin[10] Türk hukukunda kabul edilebilir bir yönü bulunmasa da bu kararın yerinde olduğu kanaatindeyiz. Fakat bu kanaat, açık kanun hükmünün önüne geçemeyeceğinden bu uygulamanın veri koruma otoritesinin kararıyla değil mevzuat değişikliğiyle yapılması gerektiği ortadadır.

2.1.5.2. İşleyici ve veri işleyen kavramları

İşleyici ve veri işleyen kavramları, kontrolör ve veri sorumlusunun vermiş olduğu yetkiye dayanarak, bu yetki ve talimatlarla sınırlı şekilde onların tasarrufundaki kişisel verileri işleyen gerçek ya da tüzel kişi veya kamu kurum kuruluşlarıyla bunların organlarıdır. Öncelikle GDPR ve KVKK'daki gerçek veya tüzel kişi sınırlaması hususunda "veri sorumlusu kontrolör" başlığı[11] altında yapılan açıklamaların burada da aynen geçerli olduğu söylenebilir[12].

---

[9] KVKK. "Kurul Kararları", 22/07/2020 tarih 2020/560 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6798/2020-560, Erişim: 07.07.2021.

[10] Kişisel Verileri Koruma Kurumu. "25.06.2021 tarihli Duyuru", https://www.kvkk.gov.tr/Icerik/6989/ORTAKLIKLARIN-VERBIS-E-KAYIT-YUKUMLULUGU-HAKKINDA-DUYURU,Erişim: 04.06.2022.

[11] Bkz. yukarıda 1.5.1.

İşleyici ve veri işleyenin kontrolör ve veri sorumlusundan temel farkı şu şekilde ifade edilebilir: Kontrolör ve veri sorumlusu kişisel verilerin işlenmesindeki amaç ve vasıtaların belirlenmesi noktasında doğrudan ve kendiliğinden tasarruf yetkisine sahipken işleyici ve veri işleyenler bu kişisel veriler üzerinde veri sorumlusu ve kontrolörün verdiği yetkiye dayalı olarak ve onların belirlediği sınırlarda tasarruf edebilecektir.

İşleyici ve veri işleyen kavramı için en önemli hususlardan biri, bu kişi gruplarının, veri sorumlusunun himayesi dışındaki kişilerden veya veri kayıt sistemi dışındaki kişilerden oluşabileceğidir. Başka bir deyişle, kontrolör ve veri sorumlusunun himayesinde çalışıp onun emir ve talimatlarıyla hareket eden çalışan kişiler veya veri sorumlusunun temsilcileri veri sorumlusu ve kontrolörle aynı himayede bulunduğundan işleyici veya veri işleyen sıfatını kazanamayacaktır. İşleyici ve veri işleyen sıfatına sahip kişi grupları çoğunlukla veri sorumlusuna ve kontrolöre belli alanlarda hizmet sağlayıp bu hizmet dahilinde himayesinde veri sorumlusu ve kontrolörün uhde ve tasarrufundaki kişisel verileri bulunduran ve fakat bu kişisel verilere veri sorumlusunun vermiş olduğu yetkiyle sınırlı olarak erişebilen ve üzerlerinde başkaca bir tasarruf yetkisi bulunmayan kişi gruplarıdır. Bu kapsamda örneğin bir ticari şirketin veri sorumlusu olduğu personel verilerini kaydettiği bulut tabanlı bir sistemde, bu bulut hizmetini sunan kuruluş ya da kişi, işleyici ve veri işleyen sıfatına sahiptir. Veri işleyen ve veri sorumlusu sıfatlarının aynı gerçek veya tüzel kişi üzerinde doğabilmesi mümkündür. Örnekteki bulut hizmet sağlayıcısı, sunduğu bulut hizmetinde depolanan veriler söz konusu olduğunda veri işleyen ve işleyici sıfatına sahipken kendi personel ve müşterilerinin kişisel verileri bakımından veri sorumlusu ve kontrolör olarak hareket eder.

Özetle veri işleyen kavramını veri sorumlusu kavramından ayıran unsur, veri işleme konusunda dayandığı yetki ve veri işleme konusundaki tasarruflarının sınırlılığıdır.

2.1.5.3. Alıcı ve üçüncü kişi kavramları

General Data Protection Regulation tarafından tanımı yapılan alıcı; üçüncü bir kişi olsun veya olmasın, kişisel verilerin açıklandığı bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organı ifade etmektedir. Üçüncü kişi ise ilgili kişi, veri sorumlusu, veri işleyen ve veri sorumlusu ya da veri işleyenin doğrudan

yetkisi altında, kişisel verileri işleme yetkisi bulunan kişiler haricindeki bir gerçek veya tüzel kişi, kamu kurumu, kuruluşu veya organıdır. Alıcı ve üçüncü kişi kavramları Türk veri koruma mevzuatında yer almamaktadır. Fakat alıcı kavramı Türk veri koruma hukukunda alıcı kişi grupları olarak anılmakta ve veri sorumlusu tarafından kişisel verilerin aktarıldığı üçüncü kişi olarak tanımlanmaktadır.

2.2. Kişisel Verilerin Korunmasına İlişkin Düzenlemeler

Kişisel verilerin korunması bireyler için bir haktır. Bu hakkın kapsamına veri sahibi bireyin verileri üzerindeki hakimiyeti ve verilerin işlenmesi, aktarılması gibi konularda karar verme yetkisi dahildir.

2.2.1. Uluslararası Düzenlemeler

Kişisel verilerin korunması alanındaki ilk düzenleme OECD tarafından 1980 yılında "Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler"in[13] kabul edilmesiyle yapılmıştır. Bu ilkeler öneri şeklinde olup, üye ülkeler için bağlayıcı nitelikte değildir[14].

Rehberde kişisel verilerin hukuka aykırı olarak elde edilmesi veya yanlış tutulması, yetkisiz kişilerce kötüye kullanılması gibi risklerin önüne geçilmesi için alınabilecek tedbirlere ve kişisel veri dolaşımının nasıl gerçekleşmesi gerektiğine ilişkin bilgiler yer almaktadır. Üye devletler kendi mevzuatlarında kişisel verilerin korunması hukukuna ilişkin düzenlemelerde Rehber'den oldukça yararlanmış ve genel olarak Rehber'e uygun düzenlemeler yapmışlardır. Her ne kadar kişisel verilerin korunmasına yönelik ilk düzenlemelerin bu Rehber'de yer aldığı söylenebilirse de 10 Aralık 1948 tarihinde kabul edilen "İnsan Hakları Evrensel Beyannamesi"nin 12. maddesinde de özel hayatın gizliliğinin korunmasına ilişkin ifadeler yer almaktadır. 1976 tarihinde yürürlüğe giren "Birleşmiş Milletler Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme"de de özel hayatın ve mahremiyet hakkının korunması

[13]OECD. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personel Data", http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, Erişim: 08.08.2021.

[14] Küzeci, E. (2019). *Kişisel Verilerin Korunması*, 3. Baskı, Turhan Kitabevi, Ankara, s. 114-115; Akgül, A. (2014). *Danıştay ve İnsan Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması,* Beta Yayıncılık, İstanbul, s.114 vd; Özdemir, s. 23; Başalp, s. 24; Gür, İ. (2009). *Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları*, Yayımlanmamış Yüksek Lisans Tezi, Ankara, s. 7; Erarslan S. (2020). *Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller*, 2. Baskı, Oniki Levha Yayıncılık A.Ş, İstanbul, s. 29; Aksoy; s. 4.

gerektiğinden bahsedilmiştir. Birleşmiş Milletler genel olarak kişisel verilerin korunmasını, özel hayatın gizliliği ve mahremiyet hakkının kapsamında değerlendirmiştir.

Teknolojinin gelişmesiyle kişisel veri işlenmesi ve paylaşılmasında önem arz eden dijital veri işlemeye ilişkin, Birleşmiş Milletler Genel Kurulu 14 Aralık 1990 tarihinde "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeleri"ni yayınlamıştır[15]. Bu ilkeler; meşruluk ve dürüstlük ilkesi, doğruluk ilkesi, amacın belirliliği ilkesi, ayrımcılık yasağı ilkesi, güvenlik ilkesi, denetim ve yaptırım ilkesi ve sınır ötesi veri akışı ilkesidir. OECD üye ülkelerin kişisel veriler ile ilgili düzenlemelerinde bu ilkelere uygun hareket etmeleri gerektiğini belirtmiştir[16]. Türk hukukunda da kişisel verilerin korunmasına ilişkin düzenlemeler bu ilkeler ışığında düzenlenmiştir.

Tarihsel süreçte kişisel verilerin korunmasına ilişkin olarak en kapsamlı ve detaylı düzenlemeler Avrupa Konseyi tarafından yapılmıştır. 1 Ekim 1985 tarihinde yürürlüğe giren "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi", kişisel verilerin korunması alanında bağlayıcılığı bulunan ilk uluslararası sözleşmedir. Bu sözleşme 108 No'lu sözleşme olarak da bilinmektedir. Sözleşme Türkiye tarafından da 2001 yılında imzalanmış ve 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazete'de yayımlanan onay kanunu ile bağlayıcılık kazanmıştır. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun temelinde de bu sözleşme bulunmaktadır. 108 No'lu sözleşme daha sonra 18 Mayıs 2018 tarihinde "Kişisel Verilerin İşlenmesine İlişkin Bireylerin Korunmasına İlişkin Sözleşmede Değişiklik Yapılmasına Dair Protokol" (CETS No.223) ile yenilenmiştir[17]. Bu Protokol "108+" olarak anılmaktadır ve 108 sayılı Sözleşmedeki eksiklikleri gidermeyi amaçlayan ek bir düzenleme niteliğindedir.

1950 yılında yürürlüğe girmiş olan Avrupa İnsan Hakları Sözleşmesi ise doğrudan doğruya kişisel verilerin korunması alanında olmasa da özel hayatın

[15] Birleşmiş Milletler Genel Kurulu. (1990). " Guidelines fort he Regulation of Computarized Personal Data Files", http://www.refworld.org/pdfid/3ddcafaac.pdf, Erişim: 10.08.2021.
[16] Dülger, M.V.(2020). *Kişisel Verilerin Korunması Hukuku,* 3. Baskı, Hukuk Akademisi, İstanbul, s. 90.
[17]Avrupa Konseyi. "Convention108+: The Modernised Version Of A Landmark Instrument", https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108, Erişim: 10.08.2021.

gizliliğine ilişkin hükümler içermektedir. Fark edilmelidir ki Avrupa ülkeleri kişisel verilerin korunması alanındaki düzenlemeler konusunda diğer ülkeler için kılavuz konumundadır. Bu alanda birçok düzenleme ilk kez Avrupa'da yapılmıştır. Bu alanda çalışmalarına devam eden Avrupa Birliği, 24 Ekim 1995 tarihinde "96/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi"ni düzenlemiştir. Direktif uyarınca üye devletler kendi aralarında kişisel veri transferini engelleyememekte ve yasaklayamamaktadırlar. Bu direktifle kişisel verilerin Avrupa Birliği ülkeleri arasında serbest dolaşımının mümkün olup olmadığı hususu açıklığa kavuşturulmuştur. Üye devletlerin hepsinin iç düzenlemelerini Direktife göre yapmaları gerekliliğinin öngörülmesine rağmen bu amaca ulaşılamamış ve ülkelerin veri işleme faaliyetlerinde farklılıklar ortaya çıkmıştır[18].

Avrupa Birliği ülkelerinin gözetmeleri gereken hakların içeriği, 2000 yılında yürürlüğe giren "Avrupa Birliği Temel Haklar Şartı" ile netlik kazanmıştır. Bu şartlar arasında kişisel verilerin korunması şartı da yer almaktadır. Bu haklar kapsamında herkes kişisel verilerinin korunmasını isteme hakkına sahip olacak, kişisel verilerin kullanımı için rıza alınması gerekecek ve tüm bu süreçleri denetleyen bağımsız bir denetim makamı kurulacaktır. İlerleyen süreçte bireyler arasındaki dijital iletişim arttığı için 2002 yılında *"Avrupa Parlementosu ve Konseyi'nin 2002/58/AT Sayılı Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Yönergesi"* yürürlüğe girmiştir.

AB Parlamentosu daha sonra da bu alanda çeşitli direktifler çıkartmıştır. Bunların bazıları, *"Yetkili Makamlar Tarafından Suçun Önlenmesi, Soruşturulması, Tespiti veya Kovuşturulması veya Cezai Süreçlerin Yürütülmesi Amacıyla İşlenen Kişisel Verilere İlişkin Gerçek Kişilerin Korunmasına ve Bu Tür Verilerin Serbest Dolaşımına Dair Direktif", "2006/24/EC Sayılı İletişim Trafik Verilerinin Saklanması Yönergesi"* ve ve *"45/2001 Sayılı Avrupa Birliği Kurumları Veri Koruma Tüzüğü"* olarak sayılabilir.

95/46/EC sayılı AB Veri Koruma Direktifi'nin modernize edilmesi ve gelişen çağa ayak uydurması için bir takım değişikliklere gidilmiştir. Mevcut düzenlemeler

[18] Voigt, P./ Bussche, A. s. 2.

eski ve yetersiz kalmış ve bu nedenle 24 Mayıs 2016 tarihinde General Data Protection Regulation düzenlenmiştir. GDPR'a ilham veren en önemli husus, kişisel verilerin güvenliği ve gizliliğinin devlete karşı sağlanması gerekliliğidir[19]. GDPR tarafından düzenlenen veri koruma yasalarına uymama hususunda ciddi yaptırımlar getirilmiştir. Son dönemde veri koruma düzenlemelerine ilişkin en kapsamlı düzenleme olan GDPR, diğer ülkeler için de bir örnek teşkil etmiş ve kendi mevzuatlarını GDPR'a uydurma gerekliliği doğmuştur.

2.2.2. Ulusal Düzenlemeler

Türk hukukunda kişisel verilerin korunması alanında ilk düzenleme, direkt olarak kişisel verilerin korunması tabiri altında olmayıp "özel hayatın gizliliği" başlığı altında Türk Ceza Kanununda yer almıştır. 1982 Anayasasının "Özel Hayatın Gizliliği" başlıklı 20. maddesinde özel hayatın gizliliği bir temel hak olarak anılmıştır. 7 Mayıs 2010'da bu maddeye ekleme yapılarak kişisel verilerin korunması gerekliliği ve bu hususdaki düzenlemelerin kanunla yapılacağı belirtilmiştir.1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nun 135-138.[20] maddeleri arasında kişisel verilerin korunmasının ihlaline ilişkin yaptırımlar öngörülmüştür[21].

Ülkemizde kişisel verilerin korunmasına yönelik ilk kapsamlı düzenleme, 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı *"Kişisel Verilerin Korunması Kanunu"*dur. Bu kanun, uygulamadaki eksikliklerini Kişisel Verileri Koruma Kurulu tarafından alınan kararlarla gidermeye çalışarak GDPR'ın seviyesine yaklaşmayı amaçlamaktadır[22].

[19] Dülger, Kişisel Verilerin Korunması Hukuku, s. 54.
[20] Bu maddelere ilişkin ayrıntılı bilgi için bkz.: Dülger, Kişisel Verilerin Korunması Hukuku,s. 309 vd.;Küzeci, s. 404 vd.; Sarıusta, K. (2018). *Kişisel Verilerin Ceza Hukuku Yoluyla Korunması,* Yayımlanmamış Yüksek Lisans Tezi, Gaziantep, s. 111 vd.; Dinkci, F. (2014). *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye Örneği,* Yayımlanmamış Yüksek Lisans Tezi, Samsun, s. 69 vd.
[21]Açıkgöz, A.N. (2005). "Gerekçeli-Karşılaştırmalı ve Açıklamalı Yeni Türk Ceza Kanunu", Van, s. 304, http://www.ceza-bb.adalet.gov.tr/makale/187.doc, Erişim: 08.08.2021.
[22] Kaya, M.B./Taştan, F.G. (2018). *Kişisel Veri Koruma Hukuku*, 1.Baskı, Oniki Levha Yayıncılık A.Ş., s. 45 vd.

2.3. Kişisel Verilerin Hukuki Niteliği

Kişisel veriler bireyin üzerinde tasarruf yetkisine sahip olduğu bilgileridir. Kişisel verilerin korunması özel hayatın gizliliği, insan onuru gibi kavramlarla iç içedir. Birey için kişisel verilerinin korunması bir haktır[23].

Kişisel verilerin hukuki niteliğine ilişkin çeşitli görüşler bulunmaktadır. Kişisel verilerin kişilik değeri olduğu ve bu çerçevede korunması gerektiğine ilişkin görüşler mevcuttur. Bu görüşteki kişiler, kişisel verilerin kişilik hakkının bir uzantısı niteliğinde olduğunu savunmaktadır[24]. Bu görüşteki kişilere göre kişisel veriler kişilik hakkı çerçevesinde korunmalıdır[25]. Kişilik hakkı bireye ait korunması gereken tüm değerleri kapsayan haktır[26]. Kişisel verileri kişilik değeri olarak nitelendirmek, kanaatimizce bireyin kişisel verilerini sadece özel hayatı ile sınırlı kılacak ve kamuya açık kişisel verilerini korumasız bir durumda bırakacaktır.

Avrupa'da kişisel verilerin korunmasına ilişkin temel düşünce bu korunma hakkının temel insan haklarından olduğu yönündedir. Amerika Birleşik Devletleri'nde ise kişisel verilerin korunmasına ilişkin tedbirlerin kapsamının genişletilmesinin özel sektör faaliyetlerini çok etkileyeceği düşünülmekte ve bu nedenle kişisel veriler üzerindeki hakkın Anayasal bir hak olmayıp mülkiyet hakkı olarak nitelendirilmektedir[27]. Bu nedenle Amerika'da ekonomik bir değer olarak düşünülen ve böylece ticarete konu edilebilen kişisel veriler için korumanın az olduğu yönündeki görüşte kişiler mevcuttur[28]. Amerika'daki bir diğer görüşteki kişiler ise kişisel veriler üzerindeki hakkın bir fikri mülkiyet hakkı olduğu yönündedir. Bu görüşteki kişiler;

---

[23] Akkurt, S.S. (2020). "Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", Kişisel Verileri Koruma Dergisi, C. 2, S. 1, s. 24.
[24] Keskin, D. (2022). *Bizzat Karar Verme Hakkı*, Adalet Yayınevi, Ankara, s. 180.
[25] Keskin, s. 180.
[26] Serozan, R. (2018). Medeni Hukuk-Genel Bölüm: Kişiler Hukuku, 8. Basım, Vedat Yayıncılık, İstanbul, s. 454; Oğuzman, M.K./Seliçi, Ö./Oktay-Özdemir, Ş. (2018). Kişiler Hukuku (Gerçek ve Tüzel Kişiler), 17. Basım, Filiz Kitabevi, İstanbul, s. 168.
[27] Nadezhda, P. (2009). "Property Rights in Personal Data: Learning from the American Discourse", Computer Law & Security Review, Vol.25, No.6, s. 507; Göçmen Uyarer, S. (2019). *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, Seçkin Yayıncılık, Ankara, s. 23; Korkmaz, İ. (2019). *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, 2.Basım, Ankara, s. 85.
[28] Schwartz, P.M. (2004). "Property, Privacy, And Personal Data", Harvard Law Review, vol.117, s. 2056; Singh, A. (2016). "Protecting Personal Data As A Property Right", ILI Law Review, Winter Issue, s. 126.

kişisel verilerin düşünce, eser gibi bireye ait manevi haklardan olduğunu savunmaktadır[29].

Kişisel verilerin korunması hakkının özel hayatın gizliliği hakkının bir alt türü veya faklı bir görünüm biçimi olduğunu düşünenler de bulunmaktadır. Bu görüşe göre kişisel verilerin korunması, özel hayatın gizliliği hakkının kendine has özellikli bir türünü oluşturmaktadır[30]. Kişisel verilerin, her ne kadar özel hayatın gizliliğinin içerisinde değerlendirilebilse de bağımsız bir hak niteliğine sahip olduğunu düşünenler de vardır[31]. Kanaatimizce de kişisel veriler bahsedilen haklardan farklı oldukları için; bir kişilik değeri, anayasal hak veya fikri mülkiyet hakkı olmayıp bağımsız bir hak niteliğinde değerlendirilmeli ve korunmaları için ayrı düzenlemeleri gerektirmektedir[32].

2.4. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi, veriler üzerinde veri sorumlusu yahut veri işleyenler tarafından yapılan her türlü faaliyeti karşılayan çatı kavramı oluşturur. Bu kapsamda kişisel verilerin veri sorumlularınca kaydedilmesi, elde edilmesi, alıcı gruplara yahut veri işleyenlere aktarılması, açıklanması, üzerinde değişiklikler yapılması, muhafaza edilmesi, depolanması, sınıflandırılması, kullandırılması ya da kullanımının engellenmesi gibi işlemlerin tümü kişisel verilerin işlenmesi faaliyetidir.

Kişisel verilerin işlenmesi, uluslararası ve ulusal mevzuat ve sözleşmelerde bazı şartlara tabi tutulmuştur. Bu kapsamda kişisel verilerin kaydedilmesi ya da aktarımı gibi veri üzerinde yapılacak tüm işlemlerin anılan şartlara uygun şekilde yerine getirilmesi bir yükümlülüktür.

Kişisel verilerin işlenmesi için yalnızca mevzuattaki şartların sağlanması yeterli değildir. Aynı zamanda tüm işleme faaliyetlerinin veri koruma hukukunun temel prensiplerini oluşturan kişisel verilerin işlenmesine ilişkin temel ilkelere uygun şekilde

[29] Samuelson, P. (1999). "Privacy as Intellectual Property", Stanford Law Review, Vol. 52, s. 3, https://www.jstor.org/stable/1229511, Erişim: 08.08.2021.
[30] Çelik, Y. (2017). "Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı", TAAD, Yıl. 8, Sayı. 32 s. 391; Dülger, Kişisel Verilerin Korunması Hukuku, 81; Hukukumuzda kişisel verilerin özel hayatın gizliliği hakkının bir alt başlığı olduğu yönünde gerekçelendirilmiş kararlar da mevcuttur. Örnek kararlar için bkz: Danıştay 12. Dairesi Karar Tarihi: 15.05.2006 2005/6811 E. 2006/1959 K..
[31] Küzeci, s. 69.
[32] Akkurt, s.29.

yapılması gerekmektedir. Aksi halde yerine getirilen şartların ve dayanılan hukuki sebeplerin geçersizliği ile karşılaşılması kaçınılmaz olacaktır.

Kişisel verilerin temel ilkelere ve mevzuatta belirtilen şartlara uygun olarak işlenmesi, veri sorumluları için bir yükümlülük olmakla birlikte bunların yanı sıra veri sorumlularınca yerine getirilmesi gereken birçok yükümlülük de bulunmaktadır[33].

Kişisel verilerin mevzuatta anılan işleme şartlarına ve temel ilkelere uygun olarak işlenip işlenmediğinin ve bu faaliyetler dolayısıyla veri sorumlusunun sahip olduğu yükümlülükleri yerine getirip getirmediğinin denetimi ise veri koruma otoritelerince yerine getirilmektedir. Bu bağlamda 6698 sayılı KVKK ile Türk veri koruma otoritesi olarak Kişisel Verileri Koruma Kurumu, ihdas edilmiştir. Anılan veri işleme faaliyetine ilişkin tüm yükümlülüklerin denetimi de Türkiye'deki faaliyetler bakımında Kişisel Verileri Koruma Kurumu'na bırakılmıştır.

2.4.1. Kişisel Verilerin İşlenmesinin Hukuka Uygunluğu

2.4.1.1. Genel olarak

Kişisel verilerin işlenmesinin hukuka uygun olması için gerekli şartlar, ülkelerin veri koruma alanındaki mevzuatlarına göre farklılık arz etmektedir. Türk hukukunda bu şartlar 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda 5., 6., 8. ve 9. maddelerde düzenlenmiştir. KVKK, 5. maddesinde kişisel verilerin işlenmesindeki genel şartları, 6. maddesinde özel nitelikli kişisel verilerin işlenmesindeki şartları, 8. maddesinde kişisel verilerin aktarılmasındaki şartları, 9. maddesinde ise yurt dışına aktarılmasındaki şartları hüküm altına almıştır. KVKK'nın bu maddelerinde metot olarak yasaklayıp istisna halleri sıralama yöntemi tercih edilmiştir. Kişisel verilerin hukuka uygun olarak işlenmesinden bahsedilebilmesi için KVKK'nın 5.maddesinde sayılan hukuki sebeplerden birine dayanılması şarttır. Kişisel veriyi hukuka uygun işleyebilmek için kural olarak ilgili kişinin açık rızası gerekmektedir. Ancak kişisel veri işlemenin: kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili

[33] Bkz. aşağıda 4.3..

olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarının bulunması durumunda açık rıza aranmaksızın kişisel veri işleme faaliyeti yapılabilecektir.

2.4.1.2. Kişisel verilerin hukuka uygun olarak işlenmesinin şartları

Kişisel verilerin işlenmesi kavramından, kişisel veriler üzerinde yapılan her türlü faaliyet anlaşılmalıdır. KVKK'nın 5. maddesinde kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği hüküm altına alınmıştır. Bu belirleme ile "açık rıza" kişisel verilerin hukuka uygun olarak işlenmesi şartlarından biri olarak ortaya çıkmaktadır. Maddenin devamında sayılan istisnalarda açık rıza alınmasına gerek olmadığı hususu da tüm bu istisnaların ayrı ayrı birer hukuki sebep olarak kabul edildiğini göstermektedir[34].

2.4.1.2.1. Kanunlarda açıkça öngörülmesi

KVKK'da sayılan kişisel verileri açık rıza aranmaksızın işlemenin hukuki sebeplerinden ilki *"kanunlarda açıkça öngörülmesi"* dir. Buna göre veri sorumlusu, kanunlarda açıkça öngörülmesi durumunda kişisel verileri, ilgili kişiden rıza almaksızın işleyebilecektir. Bu konuda somut örnek olarak Vergi Kanunu ve ilgili mevzuatı gereği veri sorumlularının ilgili kişilere ait kişisel verileri işlemesi yani kaydetmesi ve aktarması, İş Kanunu gereği işverenin işçisine ait bilgileri işlemesi gibi durumlar gösterilebilir[35]. Kanunda öngörülen durumun veri sorumlusu için bir yükümlülük veya hak olarak belirlenmesinin, bu hukuki sebebe dayanılması bakımından herhangi bir farkı yoktur. Bu durumda veri sorumlusu, anılan hukuki sebebe dayanabilecek olup ayrıca bir başka hukuki sebebin mevcudiyeti aranmayacaktır.

---

[34] Bu bölümde öncelikle istisna olarak sayılan hukuki sebepler sonra da açık rıza hukuki sebebi izah edilecektir. Bu metodolojinin seçilme sebebi açık rıza hukuki sebebine diğer hukuki sebeplerin mevcudiyeti durumunda da dayanılmaması gereği olup bu durum da ayrıca açıklanacaktır.

[35] Uncular, S. (2018). *Kişisel Verilerin Korunması Kanunu ve AB Genel Veri Koruma Tüzüğü Kapsamında İş İlişkisinde İşçinin Kişisel Verilerinin Korunması,* Seçkin Yayıncılık, Ankara, s. 91.

2.4.1.2.2. Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması

Kişisel Verilerin Korunması Kanununda sayılan diğer bir hukuki sebep *"fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması"* halidir. Kişinin bilincinin yerinde olmaması, acil durumlar sebebiyle rıza alınabilmesinin mümkün olmaması, üçüncü kişilerin hayat ya da beden bütünlüğü için bir zorunluluk meydana gelmesi gibi durumlarda, ilgili kişilere ait kişisel verilerin işlenmesi gerekebilecektir. Bu hallerde başka bir hukuki sebep aranmaksızın ilgili kişilerin kişisel verileri işlenecektir. Bu hukuki sebebe dayanılan kişisel veri işleme faaliyetlerinin en başında sağlık sektöründe gelişen ani ve acil durumlarda, hasta yahut hasta yakınına ait bilgilerin kaydedilmesi gösterilebilir[36].

2.4.1.2.3. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması

Kişisel Verilerin Korunması Kanununda sayılan bir başka hukuki sebep *"Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması"* sebebidir. Şayet veri sorumlusu, bir sözleşme yapmak veya bir sözleşmedeki yükümlülüklerini yerine getirebilmek için, sözleşmenin taraflarının kişisel verilerini işlemek zorunda ise bu durumda farklı bir hukuki sebebe dayanması gerekmeyecektir. Burada anılan gereklilik somut olayın özelliklerine göre belirlenecektir. Örneğin bir araç kiralama sözleşmesinin kurulabilmesi için kişinin kimlik bilgileri yanında ehliyet bilgilerinin de alınması sözleşmenin kurulması için bir gereklilik olarak ortaya çıkacakken aracın müşteriye ikametinde teslim edilmesi şeklinde bir anlaşmanın yerine getirilmesi için ikamet adresinin işlenmesi de sözleşmenin ifasıyla ilgili gerekliliktir.

[36] Güven, V. (2016). *Sağlık Hukukunda Tıbbi Kayıtların Tutulmasından ve Saklanmasından Doğan Sorumluluk*, Ankara, Adalet Yayınevi, s. 5.

2.4.1.2.4. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması

Kişisel Verilerin Korunması Kanununda sayılan bir hukuki sebep; *"Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması"* halidir. Veri sorumlusunun bir hukuki yükümlülüğünün mevcut olması ve bu yükümlülüğü yerine getirebilmesi için ilgili kişiye ait kişisel verileri işlemesi gerekmesi durumunda bu hukuki sebebe dayanılabilecektir. İşverenin ücret hesap pusulası düzenlemesi için işçisine ait gerekli bilgileri işlemesi yahut özel eğitim kuruluşunun çalışanlarının Kanun'da sayılan suçlardan hükümlü olup olmadığını öğrenmek amacıyla gerekli bilgilerini işlemesi durumunda bu hukuki sebebe dayanılabileceği söylenebilir[37].

2.4.1.2.5. İlgili kişinin kendisi tarafından alenileştirilmiş olması

Kişisel Verilerin Korunması Kanunundaki hukuki sebeplerden bir başkası, *"ilgili kişinin kendisi tarafından alenileştirilmiş olması"* sebebidir. Alenileşmek, herkesçe bilinir duruma gelmek anlamını taşımaktadır[38]. Bazen birey, kendisine ait kişisel verileri belli amaçlarla kullanılması için herkese açık şekilde paylaşabilmektedir. Örneğin bir araç satış sitesinde satıcının telefon numarasını paylaşması bu minvaldedir. Bu şekilde ilgili kişilerce alenileştirilmiş olan kişisel verilerin, alenileştirme amacıyla sınırlı olarak herkes tarafından kullanılması ve işlenmesi mümkündür. Böyle bir durumda farklı bir hukuki sebebe dayanılmaksızın kişisel veri işleme faaliyeti yapılabilecektir. Burada önemli olan husus, alenileştirme amacıyla sınırlılıktır. Bu hukuki sebebe dayanmak için kişisel verisini alenileştirmiş olan ilgili kişinin kişisel verisi, alenileştirmedeki amacına uygun olarak kullanılabilecek olup farklı amaçlarla başka bir hukuki sebebe dayanılmadıkça işlenemeyecektir.

[37] Manav, E. A. (2015). "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", Gazi Üniversitesi Hukuk Fakültesi Dergisi C.XIX, Y.2015, Sa. 2, s. 97. https://dergipark.org.tr/tr/download/article-file/789086, Erişim: 04.04.2022.
[38] Türk Dil Kurumu Güncel Türkçe Sözlüğü. https://sozluk.gov.tr/, Erişim: 15.09.2021.

2.4.1.2.6. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması

Kişisel Verilerin Korunması Kanununda sayılan bir başka hukuki sebep, *"bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması"* halidir. Tıpkı bir sözleşmenin kurulması ya da ifası için zorunlu olma sebebi gibi burada da kişisel verinin işlenmesi bir gerekliliğe ve hatta zorunluluğa dayanmaktadır. Buradaki zorunluluğun sebebi ise bir hakkın tesisi, kullanılması veya korunmasıdır. Yalnız bu hukuki sebepte sözleşmenin kurulması ve ifası için gerekli olma sebebinden farklı olarak kişisel verinin, sözleşmenin taraflarına ait olması gibi bir şart bulunmamaktadır. Veri sorumlusu, bir hakkın tesisi, kullanılması veya korunması için ilgili kişiye ait kişisel verileri başka bir hukuki sebebe gerek duymaksızın işleyebilecektir. Örnek olarak KVKK m. 11 gereği veri sorumlusuna başvuru yapılabilmesi için bu başvuruda ilgili kişiye ait bazı kişisel verilerin[39] yer alması gerekliliği, açılabilecek olan davalar yahut yasal takipler için zamanaşımı süresince karşı tarafa ait kişisel veri içeren bilgilerin saklanması[40] gibi durumlar gösterilebilir.

Bir hakkın tesisi, kullanılması veya korunmasının temelinde kamu yararı da yer alabilir. Kamu yararının yer aldığı durumlarda kişinin kişisel verilerini paylaşımı üzerindeki tasarruf yetkisi geri planda olacaktır. Bu nedenle kişisel verilerin işlenmesinde hukuka uygunluk sağlanırken kişinin kişisel verisi üzerinde bizzat karar verme yetkisinin sınırlandırılması ancak daha üstün menfaatlerin varlığı halinde söz konusu olabilecektir[41].

2.4.1.2.7. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

Kişisel Verilerin Korunması Kanununda açık rıza gerekliliğinin istisnaları arasında sayılan son hukuki sebep ise *"ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"* sebebidir. Bu hukuki sebep, istisnai durumlarda uygulanması gereken

[39] 10.03.2018 tarih 30356 sayılı Resmi Gazete'de yayımlanan Veri Sorumlusuna Başvuru Usul Ve Esasları Hakkında Tebliğ'in 5/2 fıkrasında sayılanlardan olan kişisel veriler.
[40] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler, "Kişisel Verilerin İşlenme Şartları", s. 11, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/9feefe58-9b0f-49c9-a0c7-2b2eb8c012bb.pdf, Erişim: 24.11.2021.
[41] Keskin, s. 181.

oldukça hassas bir hukuki sebep niteliği taşır. Her durumda bu hukuki sebebe dayanılması mümkün olmamakla birlikte dayanılması katı şartlara tabi tutulmuştur. Gerçekten bu hukuki sebebe dayanılması için; menfaatin veri sorumlusuna ait olması, mevcut ve meşru olması, ilgili kişinin temel hak ve hürriyetlerine zarar verilmemesi ve buna ilişkin denge testi yapılmış olması şartları kümülatif olarak aranmaktadır. Bu hukuki sebebin, diğer hukuki sebeplere dayanılamaması durumunda uygulanabilecek son çare yahut tüm işleme faaliyetleri yasal kılacak bir yol olarak düşünülmesi doğru değildir. Bu hukuki sebebe dayanılarak işlenecek olan kişisel veri için mutlaka menfaat ile işlenecek kişisel verinin niteliğinin gözetileceği kapsamlı bir denge testi yapılması gerekmektedir. Bu hukuki sebebe dayanılarak yapılan kişisel veri işleme faaliyetine örnek olarak iş yerinde güvenlik kamerası ile görüntü kaydı yapan veri sorumlusunun bu faaliyeti gösterilebilir. Veri sorumlusu menfaati çerçevesinde yer alan güvenliği sağlama amacıyla kişilerin görüntü verisini işlemektedir.

2.4.1.3. Açık rızanın taşıması gereken özellikler

2.4.1.3.1. Kişisel verilerin işlenmesinde açık rıza

Kanun; kişisel veri işlemenin temel şartı olan açık rızayı, *"belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* olarak tanımlanmıştır. Yani ilgili kişilerin, kişisel verilerin işlenmesine ilişkin rıza göstermesi durumunda, veri sorumlularınca kişisel verileri işlenebilecektir. Açık rıza, kişisel verilerin korunması alanının yapı taşlarından biri olup yalnızca alelade bir hukuki sebep olarak düşünülmemeli ve üzerinde ihtimamla durulmalıdır. Açık rıza, olumlu bir irade beyanı olup zımnen açık rıza verilebilmesi ülkemiz mevzuatı için mümkün değildir. Açık rıza, belirli bir konuya ilişkin olmalıdır. Genel nitelikli bir açık rıza beyanının hukukumuzda geçerliliği yoktur[42]. Belirli bir konuya özgülenmesi gereken açık rıza beyanında, her bir kişisel veri işleme faaliyeti -ikincil işleme faaliyetleri- için

[42] Kişisel Verileri Koruma Kurumu, Açık Rıza Alırken Dikkat Edilecek Hususlar isimli duyurusunda *"Belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki açık rızalar 'battaniye rızalar' olarak kabul edilmekte ve hukuken geçersiz sayılmaktadır. Örneğin; 'Her türlü ticari işlem, her türlü bankacılık işlemi ve her türlü veri işleme faaliyeti' gibi belirli bir konu ve faaliyeti işaret etmeyen rıza beyanları battaniye rıza kapsamında değerlendirilebilecek durumlardır."* ifadelerine yer vermiştir, https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar#:~:text=Kanun%20%C3%A7er%C3%A7evesinde%20a%C3%A7%C4%B1k%20r%C4%B1za%2C%20ki%C5%9Finin,ger%C3%A7ekle%C5%9Ftirece%C4%9Fi%20fiil%20konusunda%20yol%20g%C3%B6stermesidir, Erişim: 10.08.2021.

ayrı ayrı açık rıza alınması gerekmektedir[43]. Yani kişisel verinin kaydedilmesine ve aktarılmasına ilişkin açık rızanın ayrı ayrı alınması gerekmekle birlikte kişisel verilerin işlenmesi ile özel nitelikli kişisel verilerin işlenmesi için gerekli olan açık rızanın da ayrı ayrı alınması gerekmektedir.

Açık rıza bilgilendirmeye dayanmalıdır. Bilgilendirmeye dayalı olma şartı, aydınlatılmış açık rıza kavramını ortaya çıkarmaktadır. Bir açık rıza beyanında mutlaka açık rızanın neden alındığı, kişisel verilerin nasıl kullanılacağı ve veri işleme amacı gibi bilgilerin yer alması gerekmektedir. Bu durum kesinlikle aydınlatma yükümlülüğü ile karıştırılmamalıdır. Burada ifade edilmek istenen yalnızca ilgili kişinin neye rıza gösterdiğinin bilincinde olarak açık rıza beyanında bulunmasıdır. Bu bilgilendirmenin farklı metinlere ve özellikle aydınlatma metinlerine atıf yapılarak yerine getirilmesinin uygulamada çokça görülen hatalardan olduğu kanaatindeyiz. Açık rıza beyanı ile aydınlatma yükümlülüğü birbirinden tamamen ayrı olgulardır ve bunların aynı çatı altında birleşmesi de söz konusu değildir[44].

Açık rıza, özgür iradeye dayanmalıdır. Bir hizmetin sunulması için açık rızanın zorunlu tutulması yahut sözleşme ilişkisinde zayıf tarafta olan kişilerden alınan kapsamlı açık rıza beyanları, açık rızayı hükümsüz hale getirecektir[45]. Ayrıca diğer hukuki sebeplerden birine dayanılabileceği durumlarda açık rıza hukuki sebebine dayanılarak açık rıza beyanı alınmasına gerek olmadığı gibi böyle bir durum dürüstlük ilkesine de aykırı düşer[46]. Son olarak, bir kişisel veri işleme faaliyeti için açık rıza alınmış olması o faaliyeti hukuka uygun hale getirmez; kişisel verilerin işlenmesinde temel ilkelere uygunluk denetimi açık rıza hukuki sebebine dayanıldığında da yapılır[47].

---

[43]Kişisel Verileri Koruma Kurumu Resmi Web sitesi. Rehberler, "Açık Rıza", s. 4, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf, Erişim: 11.11.2021.

[44] 10.03.2018 Tarih 30356 Sayılı Resmi Gazete'de yayımlanan *"*Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul Ve Esaslar Hakkında Tebliğ"de m.5/1-f: *"Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir."* Şeklinde hüküm yer almaktadır.

[45] Bkz. "Bir sigorta şirketi tarafından hizmetin açık rıza şartına bağlanması hakkındaki ihbar" ile ilgili olarak Kişisel Verileri Koruma Kurulunun 20.04.2021 tarihli ve 2021/389 sayılı Kararı. https://kvkk.gov.tr/Icerik/6967/2021-389, Erişim: 12.09.2021.

[46] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler, "Kişisel Verilerin İşlenme Şartları", s. 2-3, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/9feefe58-9b0f-49c9-a0c7-2b2eb8c012bb.pdf, Erişim: 16.11.2021.

[47] Bkz. "Belediyede memur olarak görev yapan ilgili kişinin, veri sorumlusu bünyesinde işe giriş çıkış takibinin biyometrik veri işlenerek yapılması" hakkında Kişisel Verileri Koruma Kurulunun 01.12.2020

Kişisel verilerin hukuka uygun olarak işlenmesinde mevzuat sistematiği, tıpkı GDPR'da olduğu gibi, özel nitelikli kişisel verilerin işlenmesi açısından farklı düzenleme yapılması şeklindedir. Bu doğrultuda özel nitelikli kişisel verilerin işlenmesinde gereken hukuki sebep belirlemesi farklı şekilde yapılmıştır. KVKK'nın 6. maddesinde özel nitelikli kişisel veriler, *"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"* şeklinde sınırlı sayı ilkesine dayalı olarak sayılmıştır. Bu özel nitelikli kişisel verilerin hukuka uygun olarak işlenmesi için gerekli hukuki sebepler noktasında ise sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesinde farklı, diğer özel nitelikli kişisel verilerin işlenmesinde farklı hukuki sebepler tayin edilmiştir. Fakat tüm özel nitelikli kişisel veriler için, diğer kişisel verilerde olduğu gibi açık rıza hukuki sebebine dayalı olarak kişisel veri işlenmesi mümkündür. Bu durumda açık rıza hukuki sebebine dayalı olarak işlenen özel nitelikli kişisel verilerin, özel nitelikli olmayan kişisel verilerle eş değerde olduğu gibi bir yanılgıya düşülmemesi gerekmektedir. Zira özel nitelikli kişisel verilerin işlenmesinde diğer kişisel verilerin işlenmesiyle aynı hukuki sebeplere dayanılabiliyor olması, bunların değerinin aynı olması sonucunu doğurmayacaktır. Nitekim böyle bir durumda mevzuat sistematiğinin bu verilerin hukuka uygun şekilde işlenmesi hususunu ayrı ayrı düzenlemesi mantıksız olacaktır. Bu farklılık kendisini kişisel verilerin işlenmesinde dayanılan hukuki sebebin tespitinde bazı yönlerden gösterecektir. Örneğin, özel niteliği haiz bir kişisel veri ile bu nitelikte olmayan bir kişisel verinin ilgili kişinin açık rızasına dayalı olarak işlenmesi halinde, kişisel verinin işlendiği amaçla orantılı olması temel ilkesi uyarınca yapılacak olan hukuka uygunluk denetiminde, özel nitelikli kişisel verilerin hassas niteliği sebebiyle işlenme amacının belirlenmesinde daha titiz davranılması ve orantılılığın sağlanmasında daha güçlü amaçların bulunması aranmalıdır. Aksi halde ilgili kişinin açık rıza beyanının geçersiz sayılması, bu orantısızlık dolayısıyla da veri işleme faaliyetinin hukuka aykırı hale gelmesi söz konusu olacaktır.

tarihli ve 2020/915 sayılı Kararında açık rıza alınmış olmasına rağmen kişisel veri işleme faaliyeti ölçülülük ilkesine aykırı bulunmuş ve açık rıza beyanı hükümsüz sayılmıştır.

2.4.1.3.2. Özel nitelikli kişisel verilerin işlenmesinde açık rıza

Sağlık ve cinsel hayat verileri dışındaki özel nitelikli kişisel verilerin işlenmesinde, açık rızanın istisnası olarak düzenlenen hukuki sebep, *"kanunlarda öngörülen haller"* olarak ifade edilmiştir. Yani sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülmesi halinde veri sorumlularınca hukuka uygun şekilde işlenebilecektir. Örneğin bir işçinin üye olduğu sendika bilgisinin işverence işlenmesi, bu hususa yönelik bir veri işleme faaliyetidir[48].

Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler için ise farklı hukuki sebep belirlemesi yapılmıştır. Her şeyden önce bu veriler de açık rıza hukuki sebebine dayalı olarak işlenebilir. Fakat bu verilere mevzuat sisteminin atfettiği önem ve bu verilerin öğrenilmesi halinde ilgili kişinin uğrayabileceği mağduriyetin ölçüsü gözetildiğinde, bu verilerin açık rıza hukuki sebebine dayalı olarak işlenmesinde ölçülülük sağlanması için veri sorumlularınca titiz davranılması gerekmektedir. Sağlık ve cinsel hayat özel nitelikli kişisel verilerinin işlenmesinde açık rızanın istisnası olan hukuki sebep ise, diğer kişisel verilerden farklı olarak: *"Kamu sağlığının korunması, koruyucu hekimlik, tıbbi 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."* şeklinde KVKK m.6/3'te hüküm altına alınmıştır. Bu belirleme ile sağlık ve cinsel hayat verilerinin işlenmesi oldukça katı şarta bağlanmış ve böylelikle ciddi ölçüde sınırlandırılmıştır. Öyle ki bu kişisel verilerin bazı durumlarda kanunlarda öngörülmesi ve veri sorumlusunun bunları hukuki yükümlülüğü gereği işlemek zorunda olmasına rağmen, anılan şart yerine getirilemediğinden ilgili kişilerden açık rıza alınması gerekmektedir. Örneğin, işveren tarafından iş güvenliği ve işçi sağlığı mevzuatı kapsamında işçiden alınması gereken sağlık verilerinin işlenmesi için, anılan şartın sağlanmaması sebebiyle, veri sorumlusu olan işverenlerce bu hususa ilişkin açık rıza alınması gerekmektedir. Bu durum uygulamada ciddi sorunlara yol açmaktadır. Hal böyle olunca Kanunda sağlık ve cinsel

[48] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler, "Özel Nitelikli Kişisel Verilerin İşlenme Şartları", s. 4, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0ef45a05-ac30-4f35-bc4b-3b2cbefc9864.pdf, Erişim: 28.11.2021; Manav, s. 110.

hayat verilerinin işlenmesi konusunda diğer mevzuatla uyumlu olacak şekilde değişiklik yapılması gerektiği kanaatindeyiz.

2.4.1.3.3. Kişisel verilerin aktarımında açık rıza

Kişisel verilerin aktarılması da bir kişisel veri işleme faaliyetidir. Fakat kişisel verilerin aktarılması faaliyetinin hukuka uygun olarak yapılması hususu Kanunda ayrıca düzenlenmiş ve aktarımda hukuki sebep tespiti ayrıca yapılmıştır. Kişisel veri aktarımında hukuki sebepler verinin aktarılacağı yerin yurt içinde veya yurt dışında bulunması durumuna göre değişiklik göstermekte olup 8. maddede genel olarak aktarım, 9. maddede ise yurt dışına aktarım hükümleri düzenlenmiştir.

Kişisel verilerin aktarımında aranan hukuki sebepler genel olarak kişisel veri işlenmesindeki hukuki sebeplerden farklı değildir. Öncelikle ilgili kişinin açık rızası hukuki sebebi kişisel verinin aktarımında da uygulanabilmektedir. Yani ilgili kişinin açık rızası alınması halinde kişisel verileri aktarıma konu olabilecektir. Burada önemli husus, kişisel verinin işlenmesine ilişkin alınan açık rıza ile aktarımına ilişkin alınan açık rızanın tek beyan ile alınmasının doğru olmadığıdır. Tek bir açık rıza beyanında genel nitelikte kişisel verilerin işlenmesine ve aktarımına ilişkin izin alınması, Kurum tarafından "battaniye rızalar" olarak nitelendirilmektedir[49].

Kişisel veriler üzerinde yapılacak her tür faaliyet için (aktarım gibi) ayrı ayrı açık rıza alınması gerekmektedir[50]. Dolayısıyla kişisel verinin aktarımına ilişkin ayrıca açık rıza alınması halinde kişisel verilerin aktarımı mümkündür. Ayrıca kişisel verilerin aktarımında Kanun, kişisel verilerin işlenmesi şartlarına atıf yapmak suretiyle 5. ve 6. maddesinde sayılan açık rızanın istisnalarına da hukuki sebep olarak dayanılabileceğini hüküm altına almıştır. Özel nitelikli kişisel verilerin aktarımında, kişisel verilerin aktarımına ilişkin yapılan bu atıftan farklı olarak "yeterli önlemler alınmak kaydıyla" hükmü yer almaktadır. Yani veri sorumlusunun kişisel veriyi

[49] Bkz. Kişisel Verileri Koruma Kurumunca yapılan 30.03.2018 tarihli "Açık Rıza Alırken Dikkat Edilecek Hususlar" duyurusu. https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar#:~:text=Belirli%20bir%20konu%20ile%20s%C4%B1n%C4%B1rland%C4%B1r%C4%B1lmayan,edilmekte%20ve%20hukuken%20ge%C3%A7ersiz%20say%C4%B1lmaktad%C4%B1r, Erişim: 08.12.2021.

[50] Kişisel Verileri Koruma Kurumu Resmi Web sitesi. Rehberler, "Açık Rıza", s. 5-6, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf, Erişim: 11.11.2021.

aktarırken açık rıza ve açık rızanın istisnaları olan hukuki sebeplere dayanabilmesi mümkün ve yeterli iken özel nitelikli kişisel veriyi aktarımında ise ayrıca yeterli önlemleri almış olmak şartı bulunmaktadır.

Kişisel verilerin yurt dışına aktarımı hususunda ise Kanun ayrı bir düzenleme yapmıştır. Bu düzenleme Türk veri koruma hukukunun en çok tartışılan düzenlemelerinden biridir. Bu düzenlemede yine öncelikle kişisel verilerin ilgili kişinin açık rızasına dayalı olarak yurt dışına aktarılabileceği belirtilmiştir. Açık rıza aranmaksızın yurt dışına aktarım yapılabilmesi için ise iki şart düzenlenmiş ve bu iki şarttan en az birinin sağlanması gerektiği hüküm altına alınmıştır. Bu şartlardan ilki, aktarılan yabancı ülkede yeterli korumanın bulunması şartıdır. Yeterli korumanın bulunduğu ülkelerin tespitinde ise KVKK m.9/3 gereğince Kurul yetkili kılınmıştır. Bu düzenleme yapılmasına rağmen Kurul halen bu konuda herhangi bir belirleme yapmamış olup bu hususu açık bırakmıştır. Hal böyle olunca bu hükmün ülkemizde uygulanması mümkün olmamıştır. Bu durum yurt dışına aktarım hususunda uygulamada ciddi eleştirileri beraberinde getirmektedir. Ayrıca Kurul'un belirlemeyi neye dayalı olarak yapacağı, bu belirlemeyi yaparken hangi kriterleri gözeteceği gibi sorular da bu konuyu eleştiri odağı haline getirmektedir.

Kişisel verilerin yurt dışına aktarımı için sayılan seçimlik şartlardan ikincisi ise *"yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması"* şartıdır. Bu şart gereği veri sorumluları, kişisel verileri yurt dışına aktarmak için aktaracağı veri sorumlusu yahut veri işleyenden, Kurum tarafından düzenlenen taahhüt metni şablonu ile bir taahhüt almak ve bu taahhüdü Kurul'a sunarak Kurul'un onayını almak zorundadır. Bu taahhüdü her veri sorumlusunun, aktarım yapacağı veri işleyen ve veri sorumlularından tedarik etmesi uygulamada mümkün görülmemektedir. Çünkü kişisel verinin veri işleyen sıfatındaki bir kişiyle paylaşılması durumu da Türk veri koruma hukukunda bir aktarım olarak nitelendirilmektedir. Hal böyle olunca dünyada en çok kullanılan yer sağlayıcılar olan Google, Amazon, Zimbra gibi işletmelerin, Türk kuruluşlarınca kullanılması halinde bu işletmelerden böyle bir taahhüt alınması gerekecek; ancak bunun sağlanması mümkün olamayacaktır. Ayrıca bu taahhüdün alınması durumunda da Kurul'un onayına tabi olması, Kurul'un bu başvurulara yönelik kararlarını oldukça uzun sürede

vermesi gibi durumlar da sürecin uzamasına sebep olmaktadır. Bu durum Türk veri koruma hukukunda ciddi eleştirileri doğurmaktadır. Özetle kanaatimizce, 6698 sayılı KVKK ve ikincil mevzuatında kişisel verilerin yurt dışına aktarımı konusunda ciddi değişiklikler yapılması gerekliliği kaçınılmaz bir hal almıştır.

2.4.2. Kişisel Veri İşleyen Kişi Grupları

Türk veri koruma hukukunda kişisel verileri işleyen kişiler veri sorumlusu veya veri işleyen sıfatını kazanmaktadır. Bu sebeple, bu çalışmada kişisel veri işleyen kişi grupları, veri sorumlusu ve veri işleyen olarak iki grupta ele alınmıştır.

Veri sorumlusu, KVKK m.3'te *"kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak tanımlanmıştır. Bu tanımdan anlaşılacağı üzere veri sorumlusu, himayesinde kişisel veri bulundurmakla birlikte bu kişisel verilerin işlenme sistemini kuran, bu kişisel veriler üzerinde işlenme amacıyla sınırlı olarak tasarruf yetkisi bulunan kişidir. Veri sorumlusu için kanunda yapılan bu tanımda "gerçek ya da tüzel kişi" lafzı kullanılması, kişiliği haiz olmayan oluşumların veri koruma hukuku açısından nitelendirilmesi noktasında sorun yaratmaktadır[51]. Burada önemli olan husus, özellikle tüzel kişi veri sorumlularında veri sorumluluğu sıfatının doğrudan tüzel kişilik üzerinde doğduğudur. Bu sebeple tüzel kişinin mensup, üye, ortak veya yöneticilerinin veri sorumluluğu sıfatı, o tüzel kişiliğin faaliyetleri yönünden bulunmayacaktır.

Veri sorumlusu sıfatı üçüncü kişilere yahut çalışanlara da devredilemez. Veri sorumlusunun tespitinde; toplanan kişisel veri türlerinin, bu verileri toplayıp toplamamaya ilişkin kararın, toplama yönteminin, toplama amacının ve verisi toplanacak kişi grupları ile kişilerin, toplanan verilerin aktarımı hususunun ve kişisel verilerin saklama süreleri ile imha sürecinin kim tarafından yapıldığının tespit edilmesi gerekmektedir[52]. Veri sorumlusu olan tüzel veya gerçek kişi, bu sıfatı haiz olmakla veri sorumlusu adına tanımlanan tüm yükümlülükleri yerine getirme zorunluluğu

[51] Bu durum çalışmamızın önceki bölümlerinde (1.5.1)detaylı olarak irdelenmiş olup tekrara düşmemek adına burada geniş kapsamlı olarak yer verilmeyecektir.
[52] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler, "Veri Sorumlusu Veri İşleyen", s. 2, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf, Erişim: 06.01.2022.

altına girmiş olmaktadır. Hal böyle olunca çalışmamızın devamında[53] yer alacak olan tüm yükümlülüklerin, aksine yasal belirleme olmadığı müddetçe tüm veri sorumlularınca yerine getirilmesi gerekmektedir. Veri sorumlusu sıfatını haiz kişilere; şirketler, tacirler, esnaflar kamu kurumları, oda ve borsalar ile meslek kuruluşları, dernek ve vakıflar ile sendikalar, kat malikleri kurulu örnek olarak gösterilebilir.

Veri işleyen, *"veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* olarak KVKK m.3'te tanımlanmıştır. Bu tanıma göre veri işleyen, himayesinde kişisel veri bulunduran fakat bu kişisel verileri veri sorumlusunun verdiği yetkiyle ve veri sorumlusu namına işleyen tüzel ya da gerçek kişidir. Veri sorumlusu kişisel veri işleme amacını ve yöntemini belirlerken veri işleyenin faaliyeti çoğunlukla veri işleme faaliyetinin teknik kısımlarıyla ilgilidir[54]. Veri sorumlusunun, veri işleyene tanıyacağı yetkinin, onu veri sorumlusu yapacak ölçüde geniş olması halinde veri işleyen sıfatından bahsedilemeyecektir. Veri sorumlusunun; veri toplamada kullanılacak bilişim sistemleri ile diğer metotları, veri saklama yöntemini, uygulanacak veri güvenliği tedbirlerinin detaylarını, aktarım yöntemini, imha sürecinde kullanılacak yöntemleri belirleme yetkisini veri işleyene devredebilmesi mümkündür[55]. Veri işleyen sıfatını haiz kişi grubunun en güzel örneği yer sağlayıcı ve sunucu hizmeti sunan firmalardır.

Bir gerçek veya tüzel kişinin hem veri sorumlusu hem de veri işleyen olabilmesi mümkündür. Örneğin yer sağlayıcı ve sunucu hizmeti sunan bir firma, hizmeti kapsamında himayesi bulunan veriler üzerinde veri işleyen sıfatını haiz iken kendi çalışan ve müşterilerine ait veriler üzerinde veri sorumlusu sıfatını haizdir.

[53] Bkz. 4.3. numaralı başlık.
[54] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler, "Veri Sorumlusu Veri İşleyen", s. 2, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf, Erişim: 06.01.2022.
[55] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler, "Veri Sorumlusu Veri İşleyen", s. 3, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf, Erişim: 06.01.2022.

2.4.3. Kişisel Veri İşleyen Kişi Gruplarının Yükümlülükleri

2.4.3.1. Kişisel verilerin hukuka uygun olarak işlenmesi

Kişisel verilerin hukuka uygun olarak işlenmesi, veri koruma hukukundaki kişi gruplarının başta gelen yükümlülükleri arasındadır. Bu yükümlülük temel anlamda, kişisel veri üzerinde yapılan işleme faaliyetlerinde dayanılacak bir hukuki sebebin mevcut olmasını, işleme amacının mevcut ve meşru olmasını ve en nihayetinde kişisel veri işleme faaliyetinin kişisel verilerin korunmasındaki temel ilkelere uygun olarak gerçekleşmesini gerekli kılmaktadır[56].

2.4.3.2. Aydınlatma yükümlülüğü

Aydınlatma yükümlülüğü, KVKK'nın 10. maddesinde düzenlenmektedir. İkincil düzenleme olarak ise karşımıza Kişisel Verileri Koruma Kurumu'nca hazırlanarak 10.03.2018 tarih 30356 sayılı Resmi Gazetede yayınlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul Ve Esaslar Hakkında Tebliğ çıkmaktadır. Bu düzenlemelere göre veri sorumlusu; kişisel verilerin elde edilmesi sırasında, bizzat ya da temsilcisi veya yetkilendirdiği kişiler aracılığıyla, ilgili kişiyi bilgilendirmekle yükümlüdür. Bu tanım, aydınlatma yükümlülüğünün yerine getirilmesinde dikkat edilmesi gereken hususlara dikkat çekmektedir. Bu hususlardan ilki, aydınlatma yükümlülüğünün kişisel verinin elde edilmesi anında yerine getirilmesidir. İkincisi ise aydınlatma yükümlülüğünün yerine getirilmesi için bilgilendirmenin muhatabının ilgili kişinin kendisi olduğudur. Bu bilgilendirmenin kapsamı; veri sorumlusunun ve varsa temsilcisinin açık kimliği, kişisel verilerin işlenme amaçları, işlenen kişisel verilerin aktarım grupları ve aktarım amaçları, kişisel verilerin toplanma yöntemi, işlemede dayanılan hukuki sebepler, ilgili kişinin KVKK m.11'de düzenlenen haklarıdır. Somut olarak ifade edilmesi gerekirse, veri sorumlularının, kişisel verileri elde ettiği anda, kişisel verinin sahibi olan ilgili kişiye, sayılan unsurların eksiksiz olarak yer aldığı aydınlatma metnini ispatlanabilir vasıta ile sunması gerekmektedir. Aydınlatma metinlerinin hazırlanması ve ilgili kişilere sunulma usulleri hakkında Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul Ve Esaslar Hakkında Tebliğ'e ve Kurumca yayınlanan Aydınlatma

[56] Kişisel verinin hukuka uygun olarak işlenmesi ve kişisel verilerin korunmasındaki temel ilkeler ayrı ayrı başlıklarda (bkz. 4.1.2) detaylıca incelenmiş olduğundan, tekrara düşülmemesi adına bu başlık altında yeniden ele alınmamıştır.

Yükümlülüğü'nün yerine getirilmesi Rehberi'ne[57] uygun hareket edilmesi gerekmektedir.

2.4.3.3. Veri güvenliğinin sağlanması

Veri sorumlusu, himayesinde bulunan kişisel veriler üzerinde, veri güvenliğinin sağlanması yükümlülüğü altındadır. Oldukça geniş kapsamlı bir konu olan veri güvenliği, kişi gruplarının yükümlülüğü olması yanında kişisel verilerin korunması alanının temel amacıdır. Veri güvenliğinin sağlanması yükümlülüğü gereği veri sorumlusunun, himayesinde bulunan kişisel verileri ve uygulamakta olduğu kişisel veri işleme süreçlerini dahili ve harici tüm hukuka aykırı müdahalelerden ari tutması ve zarar görmesini engellemesi gerekmektedir. Bu kapsamda veri sorumlusunun; kişisel verilerin hukuka aykırı olarak işlenmesini ve bunlara hukuka aykırı olarak erişilmesini engellemek ve kişisel verilerin muhafazasını sağlamak amacıyla her türlü idari ve teknik tedbiri alması gerekmektedir[58].

Teknik tedbirden kasıt, bilişim ortamında uygulanması gereken süreç ve prosedürlerdir. Teknik tedbirlere örnek olarak; siber güvenlik önlemleri alınması, yetki ve erişim sınırlamalarına yönelik şifrelemelerin yapılması, sızma testi yapılması, log kaydı tutulması, ağ güvenliğinin sağlanması için gerekliliklerin yerine getirilmesi gösterilebilir. Kişisel verilerin korunması alanını bilişim teknolojileri alanıyla kesiştiren kısım teknik tedbirlerin uygulanmasıdır.

İdari tedbirler, veri sorumlusunun veri güvenliği yükümlülüğünü yerine getirmek adına uygulaması gereken yönetimsel, hukuki ve idari faaliyetleri ifade etmektedir. İdari tedbirlere örnek olarak; veri sorumlusunun personeline farkındalık eğitimi vermesi, personeli gizlilik sözleşmeleri ve disiplin yönergeleriyle bağlı tutması, veri güvenliğine ilişkin periyodik denetimler yapması, yetki ve erişim sınırlamalarına yönelik fiziki ve idari tedbirler alması, güvenlik politika ve prosedürleri hazırlanarak uygulanması gösterilebilir.

---

[57] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler. "Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi", s. 6, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf, Erişim: 02.09.2021.

[58] Toğuz, Ö. (2010). *Data Protection and Intellectual Property in the EU and Turkey*, Middle East University, Unpublished Gratuate Thesis, Ankara, s. 22.

Veri güvenliğinin sağlanması yükümlülüğü açısından veri sorumlusu ve veri sorumlusu adına hareket eden veri işleyenin müştereken sorumlu olduğu, KVKK m.12/2 ile hüküm altına alınmıştır.

2.4.3.4. Kişisel verilerin imhası

Kişisel verilerin imhası konusunda ortaya çıkan en temel sorun, kişisel verilerin saklanma süresidir. Kişisel verilerin saklanma süresi, işlenen kişisel verilere, kişisel verileri işleyen kişi gruplarına ya da ilgili kişilere; bunların tabi olduğu mevzuat düzenlemelerine yahut işlenme amacına göre farklılık arz etmektedir. Tüm kişisel veriler için genel bir saklama süresinin tespit edilebilmesi mümkün değildir. Saklama süresinin tespitinde farklı kriterler söz konusudur. Temel anlamda saklanma süresinin tespitinde yapılması gereken kapsamlı bir mevzuat taramasıdır. Bu mevzuat taramasında öncelikle kapsam, veri sorumlusunun ya da veri işleyenin tabi olduğu mevzuatlar üzerinden belirlenmelidir. Zira veri sorumlusu yahut veri işleyenin kamu kurumu ya da kamu kurumu niteliğinde olması ile özel hukuk tüzel ya da gerçek kişisi olması arasında faaliyet alanları arasında ciddi mevzuat farklılıkları bulunmaktadır. Bu durum da işlenen verilerin saklanma süresini önemli ölçüde etkileyecektir. Örneğin bir kamu kurumu olan veri sorumlusu ya da veri işleyen için, verilerin saklanması hususunda 18.10.2019 tarih 30922 sayılı Resmi Gazetede yayımlanan Devlet Arşiv Hizmetleri Hakkında Yönetmelik ciddi önem arz edecektir. Kamu kurumu niteliğindeki kuruluşlar açısından ise bazen anılan Yönetmelik, bazen ise farklı özel düzenlemeler söz konusu olmaktadır[59]. Özel hukuk tüzel ve gerçek kişilerinin uhdesindeki kişisel verilerin saklanma süresinin tespitinde ise faaliyet alanı ve bu alanın tabi olduğu mevzuatın gözetilmesi gerekmektedir. Örneğin dernekler için Türk Medeni Kanunu, Dernekler Kanunu, Dernekler Yönetmeliği önem arz edecekken kooperatifler için Kooperatifler Kanunu, ticari şirketler için ise Türk Ticaret Kanunu ve ikincil mevzuatı önem arz edecektir. Hatta ticari şirketlerin ya da tacir sıfatına sahip gerçek kişilerin, kişisel verileri saklama süresi, ilgili olduğu ticaret alanına ve iş yerindeki uygulamalarına göre de değişebilecektir.[60] Sonuç olarak bir veri sorumlusu

[59] Örneğin ticaret ve sanayi odaları ve ticaret borsaları için kişisel verilerin saklanma sürelerinin tespitinde: "Ticaret Ve Sanayi Odaları, Ticaret Odaları, Sanayi Odaları, Deniz Ticaret Odaları, Ticaret Borsaları Ve Türkiye Odalar Ve Borsalar Birliğinde Muhafazasına Lüzum Kalmayan Evrak Ve Vesaikin İmhası Hakkında Yönetmelik" önem arz etmektedir.

[60] Örneğin bir imalat şirketinin personeline ait sağlık verilerinin saklanmasında genel olarak iş sağlığı ve güvenliği mevzuatı önem arz ederken, işyerinde kanserojen veya mutajen maddeye maruz kalan

yahut veri işleyenin uhdesindeki kişisel verilerin saklanma süresinin tespiti için evvela iyi bir mevzuat taraması yapılması ve bu doğrultuda saklama sürelerinin tespit edilmesi gerekmektedir. Ardından ise yine tarama sonucu elde edilen tabi olunan mevzuatlar doğrultusunda kişisel verinin ya da kişisel veri içeren belgenin saklanma süreleri ayrı ayrı tespit edilecektir.

2.4.3.5. Sicil kayıt yükümlülükleri

Kişisel Verilerin Korunması Kanunu'nun 16. maddesi ile, veri sorumlularının kayıt ve bildirim yapma zorunluluğu olan Veri Sorumluları Sicili (VERBİS) ihdas edilmiştir. Veri Sorumluları Sicili'ne kayıt yükümlülüğü hususunda istisna ve muaf tutulabilecek kişi gruplarının belirlenmesi ve son kayıt ve bildirim sürelerinin tespiti hususunda Kurul yetkili kılınmıştır. Bu yetki dahilinde Kurul; gerek çalışan sayısı, gerek yıllık mali bilanço, gerekse ana faaliyet konusu olan kişisel veri türlerine göre belli veri sorumlularını VERBİS'e kayıt ve bildirim yapma yükümlülüğünden istisna tutmuştur. Aynı şekilde Kurul, sicil'e kayıt ve bildirim yapmak için süre tayin etmiş, akabinde ise bu süreler defaten farklı sebeplerle ertelemeye maruz kalmıştır. Kurul tarafından, verilen yetki dahilinde Sicil'e kayıt ve bildirim yükümlülüğünde son sürenin sürekli ertelenmesinin ve birçok kişi grubunca halen bu alanın Sicil'e kayıt ve bildirim yükümlülüğünden ibaret sanılması karşında Kurum'un yeterli ve istikrarlı açıklama ve bilgilendirmelerde bulunmamasının kişisel verilerin korunması alınana ciddi zarar verdiği ifade edilmelidir.

2.4.3.6. Başvurulara cevap verme

İlgili kişiler, KVKK m.13'te ve 10.03.2018 tarih 30356 Resmi Gazetede yayınlanan Veri Sorumlusuna Başvuru Usul Ve Esasları Hakkında Tebliğ'de yer alan usullerle KVKK m.11'de sayılan haklarını kullanmak suretiyle veri sorumlusuna başvuru yapma hakkına sahiptirler. Veri sorumlusu bu gibi başvuruları derhal ve en geç 30 gün içerisinde sonuçlandırmak zorundadır. Bu süre içerisinde veri sorumlusunca herhangi bir işlem yapılmaması veya başvurunun haksız olarak reddi, ilgili kişiye, Kurul'a şikayet hakkı vermektedir. Başvuru yolu, şikayet için ön şart olup tüketilmedikçe Kurul'a şikayet hakkı doğmaz. Hal böyle olunca kişisel verilerin

personelinin sağlık verilerinin saklanma süresinin tespitinde: "Kanserojen Veya Mutajen Maddelerle Çalışmalarda Sağlık Ve Güvenlik Önlemleri Hakkında Yönetmelik" önem arz edecektir.

korunması alanında yükümlü kişi gruplarının, ilgili kişilerce kendilerine yapılan başvurulara, derhal ve en geç 30 gün içinde cevap verme yükümlülüğü doğmuştur.

3. KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN MİKROÇİPLER

3.1. Mikroçip Kavramı

Mikroçip kavramı oldukça yeni bir kavram olup "entegre devre yapmak için kullanılan yarı iletken malzemeden küçük bir levha" olarak tanımlanmaktadır. Bir mikroçip (çip, bilgisayar çipi, entegre devre veya IC olarak da adlandırılır), küçük düz bir silikon parçası üzerindeki bir dizi elektronik devredir. Çipteki transistörler, bir akımı açıp kapatabilen minyatür elektrik anahtarları gibi davranır. Mikroçip, bir bilgisayar donanım sistemindeki diğer mikroçiplerle ilgili olarak belirli bir role hizmet eden, paketlenmiş bilgisayar devrelerinin küçük bir yarı iletken modülüdür[61]. Bir mikroçip pirinç tanesi büyüklüğünde de olabilir ve tarayıcılar tarafından okunur.

Mikroçipler transistör denilen ve kırmızı kan hücresinden 200 kat küçük bileşenleri kullanarak çalışırlar[62]. Çip, içerisinde ne kadar transistör barındırırsa o kadar hızlı ve güçlü olur. Bunların imalatı ise fotolitografi makinesi tarafından yapılmaktadır. Bu makine, silikon bir tabakaya lazer ışınını göndermek, suretiyle fotoğraf çekerken olduğu gibi, plakaya transistörün görüntüsünü bırakarak çalışmaktadır. Seneler içerisinde hem çiplerin içerisindeki transistör sayısı artmakta hem de transistörlerin boyutu küçültülmeye devam etmektedir. Bu kadar küçük bir şeyi üretmenin zorluğu aynı zamanda ortam koşullarının üst düzey olmasını gerektirmektedir. Mikroçipler çok küçük boyutlarda oldukları için üretim sırasında odada herhangi bir toz veya deri parçası gibi yabancı bir cismin bulunmaması için çip imalatında görevli kişiler özel bir kıyafet ve ayakkabı giymekte, eldiven takmakta, hava duşu almakta ve üretim odalarındaki hava iki dakikada bir yeni ve temiz havayla değiştirilmektedir[63]. Ülkemizde seri üretim boyutunda mikroçip üretimi yapılmamaktadır. Bu da, kullandığımız birçok cihazın içinde mikroçip bulunması nedeniyle, teknolojik açıdan diğer ülkelerden geri kalmamızın sebeplerinden biridir.

Günümüzde mikroçipler teknolojinin birçok alanında kullanılmakta olup 7 nanometre gibi küçük boyutlarda üretilebilmektedirler. Endüstriyel olarak birçok

---

[61] Teknopedia. "What Does Microchip Mean?", https://www.techopedia.com/definition/8331/microchip, Erişim: 10.09.2020.

[62] Tekno Kampüs. "Mikroçip Nedir?", https://teknokampus.net/mikrocip-nedir-ne-ise-yarar-nasil-uretilir/, Erişim: 08.08.2021.

[63] Tekno Kampüs. "Mikroçip Nedir?", https://teknokampus.net/mikrocip-nedir-ne-ise-yarar-nasil-uretilir/, Erişim: 08.08.2021.

makinenin içerisinde yer almakta olan mikroçiplerin genel kullanımları otomotiv, makine imalatı gibi endüstriyel amaçlı ağır sanayilerdir. Endüstriyel kullanımlarının yanı sıra insan hayatını kolaylaştıran, teknolojik aletlerin işlevselliğini arttıran ve tüm bunları veri akışı sağlayarak yapan mikroçipler hayvanlar ve insanlar üzerinde de kullanılmaya başlanmıştır. Hayvanlar üzerinde kullanım birçok ülke tarafından kabul görmekte olup yasallaşmış ve birtakım düzenlemelere de tabi tutulmuştur. Ancak mikroçiplerin insanlar üzerinde kullanımına gerek gizlilik ve mahremiyet gerekse dini nedenlerle çekinceli yaklaşılmaktadır. Bu nedenle insanlar üzerinde kullanımı henüz yaygınlaşmamış ve düzenleyici kurallara tabi tutulmamıştır.

3.2. Mikroçiplerin Tarihi Gelişimi

Mikroçip yapma fikri ilk kez 1949 yılında Siemens için çalışan mühendis Werner Jacobi'nin mikroçip benzeri bir tasarım için yaptığı patent başvurusunda bu tasarımın, işitme cihazları için kullanılabileceğini ileri sürmesiyle ortaya çıkmıştır[64]. Daha sonrasında tam anlamıyla mikroçipin oluşturulması, ilk kez Jack Kilby ve Robert Noyce isimli iki elektronik mühendisinin ayrı ayrı bu alan üzerine çalışmalarıyla gerçekleşmiştir. Kilby 2000 yılında mikroçipi bularak Nobel fizik ödülünü alırken aynı zamanda bu çalışmasıyla 2009 yılında Elektronik Mühendisliği Dönüm Noktaları Listesi'nde (IEEE Milestone) yerini almıştır[65]. Robert Noyce ise Kilby'den bir süre sonra Kilby'nin tasarımını geliştirerek eksikliklerini gidermiştir[66]. Endüstriyel anlamda mikroçipin icadı bu şekilde gerçekleşmiştir. Mikroçipin icadından önce, bilgisayarlar ve radyolar gibi elektronik cihazlar, oldukça ağır ve hantal yapıda olup çok fazla güç tüketmekte ve büyük miktarda ısı üreten vakum tüpleri veya valfler kullanmaktaydı[67].

Günümüzde en gelişmiş yöntemlerle yapılan endüstriyel mikroçipler Asya kıtasında üretilmektedir. Endüstriyel olarak mikroçip üretimi yapan ülkelerin başında büyük oranda Çin, Tayvan ve daha küçük çapta Güney Kore gelmektedir. Dünyada çipe olan talep o kadar fazladır ki üretim yetişmemektedir. Telefon ve diğer küçük ev

---

[64] Teknopedia. "What Does Microchip Mean?", https://www.techopedia.com/definition/8331/microchip, Erişim: 10.09.2020.
[65] Wikipedia. "Entegre Devre", https://tr.wikipedia.org/wiki/Entegre_devre, Erişim: 08.08.2021.
[66] Wikipedia. "Entegre Devre", https://tr.wikipedia.org/wiki/Entegre_devre, Erişim: 08.08.2021.
[67] WIDEX. "How The Chıp Transformed The Industry", https://www.widexpro.com/en-ca/blog/global/how-the-chip-transformed-the-industry/, Erişim: 08.08.2021.

aletleri için çip ihtiyacının artması özellikle otomotiv sektörünü etkilemiş, otomotivler için yeterli çip üretimi yapılamamış ve otomotiv sektöründe yaşanan çip krizi nedeniyle tüm dünyada otomotiv fiyatları artmıştır.

Deri altı mikroçiplerin keşfi ve gelişimi ise önce hayvanlara kimlik tanımlaması yapılabilmesi için geliştirilen mikroçiplerle başlamıştır. İnsan bedeni üzerindeki kullanımına ilişkin çalışmalar devam etmektedir ve hali hazırda birçok insanın üzerinde mikroçip bulunmaktadır. İnsan bedeni üzerinde mikroçip kullanımına ilişkin yapılan çalışmalara tarihsel süreçte oldukça ilgi kadar tepki de gösterilmiştir. Mikroçip üretimi ve geliştirilmesi konusunda çalışma yapan kişiler, insanoğlunun beyinden ibaret olduğunu, tüm faaliyetlerimizin beynin komutasına bağlı olduğunu ve vücudumuzun sadece itaat eden bir et-kemik sistemi olduğunu düşünmekte ve bu nedenle insan vücudunda teknolojik olarak değişiklik yapmak veya onu endüstriyel hale getirmek konusunda sakınca görmemektedirler. Mikroçiplerle ilgilenenler genelde mühendislerdir, buna karşılık deri altı mikroçiplerle ilgilenenler biohacker[68] ismini almışlardır. İnsan bedeni üzerine mikroçip kullanımı zamanla farklı kişiler tarafından, farklı amaçlarla denenmiştir[69]. Bilindiği kadarıyla deri altı mikroçip faaliyetleri ilk olarak Amerika'da gerçekleşmiş ve dünyaca duyulmuştur. Amerika'da da mikroçipleri faydalı görenler olduğu kadar bunların birçok zararlı etkisi olduğunu ya da gelecekte zararlı etkileri olacağını ileri süren de çoktur.

İyi yönleri olacağını düşünenler; mikroçiplerle önemli tesislere, gizli evrakların bulunduğu alanlara ya da askeri üslere giriş ve çıkışlarda güvenliğin artacağını, acil servislerde insanların tıbbi kayıtlarına hızlıca ulaşılarak hastaya daha hızlı ve uygun müdahalenin yapılabileceğini düşünmekteydi.

Kötü yönleri olacağını düşünenler ise mikroçip kullanımıyla gizliliğin büyük oranda zarar göreceğini ve insanları izlemek için daha iyi bir yol olamayacağını düşünmektedirler. Bu kesime göre insanlar doğuştan özgür yaratıklar olup bu şekilde

[68] Fiziksel ve bilişsel performanslarını artırma umuduyla geleneksel laboratuvar alanları ve kurumların dışında kendi bedenleri üzerinde deney yapanlardır. Vox. "How biohackers are trying to upgrade their brains, their bodies — and human nature" ,https://www.vox.com/future-perfect/2019/6/25/18682583/biohacking-transhumanism-human-augmentation-genetic-engineering-crispr, Erişim: 10.10.2021.
[69] Detaylı bilgi için bkz. 3.3. numaralı başlık.

izlenmemelilerdir. ve İnsanları bu şekilde izlemenin onları etiketlemek olacağı, bunun Orwellian[70] bir düşünce olduğu savunulmuştur[71].

İnsanlara mikroçip takma fikri Amerika'da, etiketlenme korkusunu doğurmuştur. Sadece belli özelliklere sahip kişilere mikroçip takma fikri, bu kişilerin diğerlerinden ayırt edilmesini sağlayacak ve etiket etkisi yaratabilecektir. En başta Alzheimer hastalarına kaybolmamaları için çip takma fikri düşünülmüş ise de bu bütün Alzheimer hastalarını etiketlemek olacak ve kimin ailesinde ve nerede Alzheimer hastası var bu şekilde bilinebilecektir. Daha sonrasında şartlı tahliye edilenler, göçmenler gibi birçok gruba çip takılması gündeme gelmiş ve insanların hepsinin kategorize edilerek elektronik olarak etiketlenmesi sonucu ortaya çıkmıştır[72].

Sadece belli özelliklere sahip bireylere çip takılması fikri bireyin etiketlenmesine yol açarak bireyin, toplumda eşitsizliğe ve ayrımcılığa maruz kalmasının yanı sıra bilinmesini istemediği kişisel verilerinin bu şekilde alenileşmesine neden olabilecektir. Örneğin yüz kızartıcı suçlardan hüküm giyenlere böyle bir uygulama zorunluluğu getirilirse mikroçiplerin x-ray cihazlarında gözükmesi nedeniyle bu durumu öğrenmemesi gerekenler de öğrenmiş olacaklardır. Bu tip bir etiketleme veri gizliliğini de zedeleyerek istenmeyen sonuçlar doğuracaktır. Bu ve buna benzer sebeplerle insanlar üzerinde deri altı mikroçip uygulaması tam olarak güvenilirlik kazanmış değildir.

Mikroçiplerin işverenler tarafından işçilerine zorunlu tutularak baskı aracı haline getirileceğini düşünenler de olmuştur. İşverenler için işe giriş-çıkış takibi, işçinin mikroçipini okuyucuya okutarak kimliğinin ve işe girdiği saatin okuyucuya aktarılmasıyla yapılabilmektedir. Halihazırda Amerika'daki ve İsveç'teki bazı şirketlerde bu şekilde işe giriş-çıkış takibi yapılmaktadır. Ancak bunun işçilere zorunlu tutulması söz konusu olmayıp gönüllük esası ile bu uygulamaya geçildiği dile getirilmektedir. Kanaatimizce bu şekilde bir giriş-çıkış takibi işçiler için herhangi bir baskı oluşturmayacak, işverenler için ise sağlıklı bir takip yöntemi olacaktır.

---

[70] George Orwell'in Bin Dokuz Yüz Seksen Dört adlı romanında anlatılana benzer şekilde, hükümetin insanların hayatlarının her bölümünü kontrol etmeye çalıştığı bir siyasi sistemi tanımlamak için kullanılır. Cambrige Dictionary. "Orwellian", https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/orwellian, Erişim: 11.11.2021.

[71] Özdemir, s. 1.

[72] Todd, L. (2007). USAToday, "Microchips İn Humans Spark Privacy Debate", https://usatoday30.usatoday.com/tech/news/surveillance/2007-07-21-chips_N.htm, Erişim: 11.10.2021

Hristiyan eleştirmenlerin bir kısmı, insanların bir şey satın almak veya satmak için vücutlarına mikroçip yerleştirmelerini "Canavarın İşareti" olarak ifade edip İncil'deki kötülük çağını tanımlayan bir kehanetin gerçekleşmesi olarak görmüşlerdir. Michigan'daki bir Roma Katolik grubu mikroçip faaliyetlerine karşı bir tutum sergileyerek canavarın işaretini alanlara Tanrı'nın gazabının geleceğini, şeytani çipi kabul etmeyi reddedilenlerin ise kurtarılacağını dile getirmiştir[73].

Amerikan Sivil Özgürlükler Birliği'nde Teknoloji ve Özgürlük Programı Üst Düzey Yöneticisi'ne göre polis karakollarını, hastaneleri, doktor muayenehanelerini ve devlet kurumlarını çip okuyucularla donatmak maliyetli olacak, personeli eğitmek zaman alacak ve insanlar vücutlarının herhangi bir yerine çip takılması konusunda çekingen olacaklardır[74]. Gerçekten de mikroçiplerin günümüzde hayatımızın her yerinde yer alabilmesi için oldukça büyük bir yatırım yapılması gerekmektedir. Bu tip teknolojilere yıkıcı teknoloji adı verilmektedir. Yıkıcı teknolojiler; hayata girmesiyle birlikte birçok faaliyeti değiştiren, bireylerin üretimini ve verimliliği artıran, bireylerin yeni şartlara uyum sağlaması için dönüşüm geçirmelerini gerektiren teknolojilerdir. Hiç kuşkusuz mikroçip teknolojisi de bir yıkıcı teknoloji örneği olacaktır. Toplumların bu teknolojiye ayak uydurması, insanların bu fikre alışması ve uyum sağlaması zaman alacaktır[75].

Toplumun geneli için mikroçip uygulaması zaman alacak olsa da bazı kesimleri için daha hızlı olacaktır. Örneğin 2004'te İspanya'nın Barselona kentindeki Baja Beach Club adındaki gece kulübü "Implant Nights" yani "İmplant Geceleri" düzenlemiş ve bu düzenlenen gecelerde kulüp müşterilerine mikroçip enjekte edilmiştir. Kulüp bu uygulama ile müşterilerinin VIP salonlarına girişi ve içecek ödemeleri için nakit para veya kredi kartı olmadan ödeme yapabilmelerini amaçlamıştır. Bu uygulamada çipteki kimlik numarası, kullanıcının mali hesaplarına bağlanmış ve kulüp üyelerinin ödeme bilgileri kulübün bilgisayarlarında saklanmıştır.

[73] Schwartz, O. (2019). "The rise of microchipping: are we ready for technology to get under the skin?", https://www.theguardian.com/technology/2019/nov/08/the-rise-of-microchipping-are-we-ready-for-technology-to-get-under-the-skin, Erişim: 11.10.2021; Todd, L. (2007). USAToday, "Microchips İn Humans Spark Privacy Debate", https://usatoday30.usatoday.com/tech/news/surveillance/2007-07-21-chips_N.htm, Erişim: 11.10.2021.

[74] Todd, L. (2007). USAToday, "Microchips İn Humans Spark Privacy Debate", https://usatoday30.usatoday.com/tech/news/surveillance/2007-07-21-chips_N.htm, Erişim: 11.10.2021.

[75] Barry Steinhardt'ın görüşü uyarınca.

Daha sonrasında dünyanın farklı yerlerindeki gece kulüpleri de bu uygulamaya geçmiştir. Kulüp sahibi, müşterilerinin genelde vücudunda piercing, dövme veya silikona sahip kişiler olduğunu ve bu nedenle mikroçip taşımaya aldırış etmediklerini dile getirmiştir. İnsanlara mikroçip takılmasına hızlı uyum sağlayacak kesimler belki de bu tip yaşama sahip bireyler olacaktır[76].

3.3. Mikroçiplerin Kullanım Alanları

3.3.1. Günlük Hayatta Kullanım Alanları

Mikroçipler; ağırlıklı olarak elektronik ev aletleri, otomotiv endüstrisi, askeri ve sivil havacılık endüstrilerinde, bilgisayarlarda ve cep telefonlarında veri işleme ve iletişim amaçlı olarak yaygın şekilde kullanılmaktadır. Mikroçipler, aynı zamanda GPS (Küresel Konumlama Sistemi) takip cihazlarında, kimlik kartlarında ve hastalıkların hızlı teşhisi ve tedavisi için tıpta da kullanılmaktadır.

Mikroçiplerin kullanım alanlarından biri de araştırma laboratuvarlarıdır. İnsan hayatının kolaylaşması için mikroçip kullanımının önem arz ettiğinin farkında olan araştırmacılar, bu alanda çalışmalar yapmaktadır. Örneğin insan hücresinin mikroçip üzerinde kullanılması bu çalışmalardan biridir. Bu yöntemle insan hücreleri için mikroçiplerde kendi doku ortamlarına benzer bir ortam hazırlanmakta ve ilaç tedavileri denenmektedir. Bu hususta, ileride "Personal Medicine" olarak adlandırılan "Kişisel Tıp" kavramının ortaya çıkacağı/yaygınlaşacağı ve mikroçipler sayesinde direkt kişiye özel tedavi yönteminin bulunmasının amaçlandığı dile getirilmiştir[77]. Bu gibi düşünceler, geçmişten bugüne birçok bilim insanı tarafından dile getirilmiş ve çalışma konusu yapılmıştır.

3.3.2. Mikroçiplerin Hayvan Bedeni Üzerinde Kullanımı

Mikroçiplerin canlılar üzerinde kullanımı, hayvanlarla başlamıştır. Geçmiş zamanlarda hayvanlarda birtakım verilerin alınabilmesi için elektronik etiketleme sistemi yani RFID (Radio Frequency Identification) teknolojisi olarak geçen ve hareketli veya sabit varlıkların kablosuz bir şekilde tanımlanması ve takip edilmesini

[76]Todd, L. (2007). USAToday, "Microchips İn Humans Spark Privacy Debate", https://usatoday30.usatoday.com/tech/news/surveillance/2007-07-21-chips_N.htm, Erişim: 11.10.2021.

[77] Klinik İletişim. "Mikroçipler Aslında Küçük Birer Laboratuvar!", https://www.klinikiletisim.com/mikrocipler-aslinda-kucuk-birer-laboratuvar/, Erişim: 08.08.2021.

sağlayan[78] "Radyo Frekanslı Tanıma" teknolojisi kullanılmıştır. Bu RFID etiketlerinin içerisinde mikroçipler yer almaktadır. Mikroçiplerin içerisinde kendilerini ayırt edici 15 karakterli kod[79] bulundurmaktadır. Hayvanların kulak arkalarına yerleştirilen bu etiketler gönderdikleri radyo dalgaları ile hayvanların hareketlerinin ve sağlıklarının uzaktan takibini kolaylaştırmıştır. Amerika'da 1990'lı yıllarda çiftçiler, sürünün üreme ve yeme alışkanlıklarını takip etmek için sığırların kulaklarına etiket yerleştirmişlerdir[80]. Daha sonrasında birçok çiftlik hayvanına da etiket yerleştirilerek hayvanlara ait verilerin takibi yapılmıştır. Halen bu şekilde takip edilen birçok hayvan bulunmakta ve hayvanlar için RFID etiketlerinin satışını yapan firmalar bulunmaktadır.

Hayvanların vücutlarına mikroçip yerleştirmenin başladığı ilk dönemlerde, insanlara mikroçip enjekte edilmeden önce hayvanlar üzerinde deneyler yapılması ve bu deneylerde kullanılan radyo frekans dalgalarının hayvanlar üzerinde kansere yol açtığını iddia eden hayvan hakları savunucuları mikroçip implantlarına karşı çıkmıştır. Testlerde kullanılan fareler üzerinde yapılan çalışmalarda mikroçipin yerleştirildiği bölgelerde kötü huylu tümörler tespit edilmiş olup bu tümörlerin mikroçip kaynaklı olup olmadığı bilinmemektedir[81].

Günümüzde evcil hayvanlar üzerinde kullanılan mikroçip, derinin altına ve genelde kürek kemiklerinin arasına, herhangi bir anestezi ya da ameliyat gerektirmeden iğneyle yerleştirilebilmektedir. Bu mikroçip, hayvanın sahipliğinin kime ait olduğunu ve kalıcı adresini içermektedir[82]. Bilinenin aksine evcil hayvanın üzerindeki mikroçip hayvanı GPS cihazı gibi takip ederek her an nerede olduğu bilgisini vermez ve hayvanın konumunu göstermez. Bu nedenle bu tür mikroçipler kaybolan hayvanların takibi için kullanılmamaktadır. Bununla birlikte mikroçip

[78] Soteks. "RFID nedir?" , https://www.soteksetiket.com/rfid-nedir/, Erişim: 10.10.2021; Wikipedia. "Radio-frequency identification", https://en.wikipedia.org/wiki/Radio-frequency_identification#Hospitals_and_healthcare, Erişim: 10.10.2021.

[79] 14 karakterli ya da 16 karakterli de olabilmektedir.

[80] Todd, L. (2007). "Microchips İn Humans Spark Privacy Debate", USAToday, https://usatoday30.usatoday.com/tech/news/surveillance/2007-07-21-chips_N.htm, Erişim: 11.10.2021.

[81] Todd, L. (2007). "Chip Implants Linked to Animal Tumors", Washington Post, https://www.washingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997_pf.html, Erişim: 11.10.2021.

[82] Woshoe County. "What is a microchip and how do they work?", https://www.washoecounty.gov/animal/faq/microchip_work.php, Erişim: 11.06.2021.

taşıyan hayvanlar kaybolduklarında bir veteriner kliniğine götürülerek çiplerinin okunması sağlanırsa hayvanın kalıcı adresi gözükeceği için adreslerine teslim edilebileceklerdir.

Mevcut mikroçipler hayvanın sağlık verilerini içermese de birkaç veriyi veri tabanında tutan mikroçipler de bulunmaktadır[83]. Bazı çiftlik hayvanlarına ve atlara yerleştirilen mikroçipler hayvanın vücut ısısı verisini verebilmektedirler. Bu sayede hayvanın sağlığını, diyetini ve herhangi bir hastalığın yayılmasını kontrol etmek için kullanılmaktadırlar[84]. Bu hususta yakalık, tasma ya da etiket gibi yöntemlerin yeterli olmadığı kanısına varılarak çip sistemi geliştirilmiştir.

Mikroçip alanında yapılan deneylerden biri de maymun beynine yerleştirilen çip deneyidir. Tesla ve SpaceX şirketlerinin sahibi Elon Musk'ın uzun zamandır bahsettiği projesi olan Neuralink ile bir maymunun beyninin iki lobuna da çip yerleştirilmiş ve iki farklı bilgisayar oyununu oynaması gözlemlenmiştir. Maymun her iki oyunu da başarılı bir şekilde oynamıştır. Kablosuz şekilde şarj edilebilen ve kafatası içerisine yerleştirilen çipin ileriki sürümlerinde, beyindeki Neuralink'lerden vücut motor/duyusal nöron kümelerindeki Neuralink'lere sinyaller aktarması amaçlanmakta ve böylece, örneğin belden aşağısı felç olanların tekrar yürümelerinin sağlanabileceği ifade edilmektedir[85].

Ülkemizde mikroçiplerin hayvan bedeni üzerinde kullanımına ilişkin yasal düzenleme bulunmaktadır. 26.02.2018 tarihli 30344 sayılı Resmi Gazete ile yürürlüğe giren "Kedi, Köpek ve Gelinciklerin Kimliklendirilmesi ve Kayıt Altına Alınmasına Dair Yönetmelik", evcil hayvanların ve sahiplerinin belirlenebilmesi, hastalıklarının daha etkin kontrolü amacıyla düzenlenmiştir. Hayvanlar üzerindeki mikroçip uygulaması veteriner hekimler tarafından veya veteriner hekim gözetiminde veteriner sağlık teknisyeni/veteriner sağlık teknikeri tarafından yapılmaktadır. Bu yönetmeliğe göre yeni doğan bir evcil hayvan için en geç 3 ay içerisinde bulunduğu yerin il/ilçe

---

[83] AVMA. *"Microchipping FAQ",* https://www.avma.org/resources-tools/pet-owners/petcare/microchips-reunite-pets-families/microchipping-faq, Erişim: 11.09.2020.

[84] RFIDHY Technology. "RFID Hayvan Etiketi İle Geleneksel Hayvan Etiketi Arasındaki Fark Nedir?" https://www.rfidhy.com/tr/what-is-the-difference-between-rfid-animal-tag-and-traditional-animal-tag/, Erişim: 11.10.2021.

[85] Cumhuriyet Haber. "Elon Musk'ın 'Beyin Çipi' Projesi Bir Maymun Üzerinde Test Edildi", https://www.cumhuriyet.com.tr/haber/elon-muskin-beyin-cipi-projesi-bir-maymun-uzerinde-test-edildi-1827168, Erişim: 06.06.2021.

gıda, tarım ve hayvancılık müdürlüğüne mikroçip başvurusu yapılmalıdır. Mikroçip takılan hayvanlar bu konuyla ilgili veri tabanına kaydedilmektedir. Veri tabanında mikroçip numarası, mikroçipin yeri, mikroçipin yerleştirildiği tarih, pasaport numarası, evcil hayvan sahibinin adı, soyadı, T.C. kimlik numarası, adresi, posta kodu, telefon numarası, evcil hayvanın aşılarına dair bilgi, evcil hayvanın ana-baba bilgileri ve ırk bilgileri, doğum tarihi gibi bilgiler yer almaktadır. Bu bilgiler veri tabanında süresiz olarak saklanır. Tarım ve Orman Bakanlığı gerektiğinde veri tabanına kaydetmek için ek bilgi toplayabilir. Veri tabanına erişime ilişkin hükümde ise kişisel verileri içeren kısım için 6698 sayılı Kişisel Verilerin Korunması Kanunu'na atıf yapılmıştır.

Bu yönetmelik gereğince evcil hayvanına mikroçip yerleştirilmesiyle kimliklendirilmesini sağlamayanlar için 5996 sayılı Kanun'da yer alan idari para cezaları uygulanmaktadır. Yine bu Yönetmeliğe göre tüm köpek sahiplerinin 1.1.2021 tarihinden itibaren en geç bir yıl içinde, tüm kedi ve gelincik sahiplerinin ise 1.1.2022 tarihinden itibaren en geç 1 yıl içinde bu düzenlemelere uyması gerekmekte idi.

3.3.3. İnsan Bedeni Üzerinde Kullanımı

Gelecekte robotların mı insanlara yoksa insanların mı robotlara daha çok benzeyeceği kuşkusuz aklımızda yer eden bir sorudur. Bugün hayatımızdaki birçok teknolojik alet insan gücünün yapabildiği birçok işi çok daha hızlı bir şekilde hallederken bilim adamları da ister istemez insanların birçok işini görebilecek robot tipi ev aletleri üretmektedirler[86]. Konuşan çay makinesi, robot süpürge, cam silen robot gibi ev aletleri buna örnek verilebilir. Birçok teknolojik alet ise aynı insanlar gibi konuşabilir, sohbet edebilir ve hatta duygu aktarımında bulunabilir hale gelmiştir.

Robotlar insanlara benzemeye başlamışken bir yandan da insanların robotlara benzediği durumlar ortaya çıkmıştır. Geçmişten beri beyne yerleştirilen bir mikroçiple insanların kontrol edilebildiği senaryosu; dizilerde, filmlerde ve kitaplarda yer almaktadır. Mikroçiplerle insanların kontrol edilebilirliğinin yanı sıra insanların mikroçiplerle birçok şeyi kontrol edebildiği senaryolar da mevcuttur. Birçok bilim kurgu filminde insanların arabalarına binerken, evlerine girerken ve günlük hayattaki

[86] Euronews. "Robotlar insanları işsiz mi bırakacak yoksa yeni iş imkanları mı yaratacak?" https://tr.euronews.com/next/2022/06/22/robotlar-insanlari-issiz-mi-birakacak-yoksa-yeni-is-imkanlari-mi-yaratacak., Erişim: 10.10.2022.

işlerini yürütürken mikroçipleri kullandığının örneği mevcuttur. Gerçekten de bazı ülkelerde deri altına yerleştirilen mikroçiplerin insanlar üzerinde kullanımı başlamıştır.

Mikroçiplerin çalışma sistemi temel olarak RFID teknolojisine sahip çipin NFC(Near Field Communication) yani yakın alan iletişimi ile iletişim kurmasına dayanmaktadır. RFID sistemini oluşturan iki bileşen vardır. Bunlar RFID etiketi ve RFID okuyucusudur. Veriler RFID etiketine yüklenir ve NFC ile RFID okuyucu tarafından okunarak verilere erişim sağlanır. RFID etiketler, içerisinde mikroçip ve anten bulunduran çeşitlerinin yanı sıra mikroçip olmayan basit düzeyde etiketler de olabilirler[87].

Yaklaşık iki pirinç tanesi büyüklüğünde olan deri altı mikroçipler tıbbi bir cam kapsül, bir silikon bilgisayar çipi ve bir bakır antenden oluşmaktadır. Asıl yapı taşı silikon olan mikroçiplerin üretimi çok maliyetli değildir. Çünkü silikonun hammaddesi olan kum, yani silisyum elementi oksijenden sonra dünyada en çok bulunan ikinci elementtir[88].

İlk kez 1998 yılında İngiliz bilim adamı Kevin Warwick tarafından bir radyo frekans tanımlamasıyla günlük işler olan bina içinde kapıları açmak[89], ışıkları yakmak gibi işler için mikroçip kullanılmıştır. Yerleştirildikten dokuz gün sonra deri altından çıkartılan çip, o zamandan beri Londra'daki Bilim Müzesi'nde tutulmaktadır[90].

Yakın bir tarih olan 2005 yılında; implant edilebilir RFID/NFC mikroçip üretimi ve mikroçip üretiminin dünya pazarı için perakende erişilebilirliği konusundaki çalışmalarıyla tanınan bir biohacker ve mikroçip implantı geliştirici olan Amal Graafstra[91], sol elinin baş parmağı ile işaret parmağı arasına RFID teknolojisini içeren bir aktarıcı yerleştirmiştir. Bu aktarıcıyı yapmasındaki etkenin, eve girişi ve arabasını

[87] Berqnet. "NFC Nedir? Nasıl Çalışır? Kullanım Alanları Nelerdir?" https://berqnet.com/blog/nfc, Erişim: 10.10.2022.
[88] Wipelot. https://wipelot.com/rfid-teknolojisi-nedir-ve-is-sagligi-ve-guvenligi-alanlarinda-nasil-kullanilir Erişim: 12.10.2022.
[89] Bkz. Türk Youtuber Tolga Özuygur, derisinin altına çip yerleştirdiği ve bu sayede kapıyı açabildiği bir video çekmiştir. YouTube. "Derimin Altına Çip Taktım (RFID Implantı)" https://www.youtube.com/watch?v=qMODQYqF1wA, Erişim: 12.12.2021.
[90] Wikipedia. "Mikrochip implant (human)" https://en.wikipedia.org/wiki/Microchip_implant_(human)#:~:text=A%20human%20microchip%20implant%20is,body%20of%20a%20human%20being., Erişim: 05.01.2022.
[91] Wikita. "Amal Graafstra" https://wikitia.com/wiki/Amal_Graafstra, Erişim: 10.10.2021

çalıştırmak için sürekli anahtarlarını unutması olduğunu söylemiştir[92]. İlk başta hayvanların kimlik bilgileri için kullanılan çip sistemini incelemiş ve çipi doktorunun yardımıyla derisinin altına yerleştirmiştir. Daha sonra evinin kapısını RFID teknolojisini kullanarak çiple açılabilir hale getirmiştir. Amaal Graafstra, bir gün evine bir arkadaşıyla birlikte gitmiş ve arkadaşı eve çiple girmesine oldukça şaşırarak bu durumu video kaydına almış ve sosyal medyada paylaşmıştır. Viral olan video kaydı ile Amal Graafstra meşhur olmuş ve profesyonel sıfatla bu alanda çalışmalarına devam ederek 2013'te Dangerous Things adlı firmayı kurmuştur[93]. Amal Graafstra, Dangerous Things adlı firması ile mikroçip teknolojisini geliştirmek için çalışmalar yapmanın yanı sıra mikroçip satışı da yapmaktadır. Mikroçiplerin fiyatları 90-210 dolar arasında seyretmektedir[94]. Firma müşterilerine, mikroçip uygulamasının herhangi bir resmi düzenleyici kurum tarafından insan vücuduna implantasyon ve kullanım için onaylanmadığını bildirmektedir. Satın alınan mikroçipler enjektörü ve frekans tanımlayıcılarıyla birlikte gelmektedir[95].

Amal Graafstra'nın bir diğer şirketi olan VivoKey Technologies'de aynı şekilde mikroçip üretimi yapmayı ve mikroçipler ile kişilerin verilerini işleyerek kişilerin hayatlarını kolaylaştırmayı amaçlamaktadır. Ancak Amaal, VivoKey ile Dangerous Things şirketinde ürettiği çiplerden daha gelişkin çipler üretmeyi amaçlamıştır. VivoKey Technologies'de; sadece gündelik hayatı kolaylaştırmak için değil, mikroçip sayesinde karşı tarafa kimlik bilgilerini aktarmak gibi faaliyetleri de yerine getiren mikroçipler üretmeyi başarmışlardır. VivoKey Identy programı ile kişinin güvenilir kriptobiyografik dijital kimliği oluşturulmaktadır[96]. Bu programa (VivoKey API) entegre uygulamaları açarak mikroçipi telefona okutmayla kimlik verileri uygulamaya aktarılabilmektedir. Kimlik verilerinin bu şekilde aktarılması durumunda kişisel verilerin işlenmesi gündeme gelecektir.

---

[92] YouTube. "Biohacking - the forefront of a new kind of human evolution: Amal Graafstra at TEDxSFU" https://www.youtube.com/watch?v=7DxVWhFLI6E, Erişim: 10.10.2021.

[93] Wikipedia. "Dangerous Things", https://en.wikipedia.org/wiki/Dangerous_Things, Erişim: 10.10.2021.

[94] Dangerous Things. https://dangerousthings.com/, Erişim: 10.10.2021; BraveNewCoin. "Biohacking: Implants That Can Store A Private Key", https://bravenewcoin.com/insights/biohacking-implants-that-can-store-a-private-key, Erişim: 10.10.2021.

[95] YouTube. "Unboxing xSIID NFC chip implant with LED", https://www.youtube.com/watch?v=mm7jEMuNBxs, Erişim: 10.10.2021.

[96] VivoKey. "Vivokey Ecosystem", https://www.vivokey.com/ecosystem, Erişim: 10.10.2021.

VivoKey Technologies mikroçiple ödeme yapabilme sistemini de geliştirmiştir[97]. Banka hesabını mikroçipe entegre etmekle veya VivoKey üzerinden ayrı bir hesap açıp bu hesaba para aktarmakla ödeme sistemi kullanılabilmektedir.

Temassız ödeme sistemleri de RFID/NFC teknolojisini kullanarak çalışmaktadır. Mikroçipler ile kartlara, şifrelere gerek olmaksızın bir yaşam amaçlanmaktadır. Bu sayılanlar gibi birçok faaliyetin yanı sıra elektronik mühendisi ve biohacker olan Brian McEvoy omuza yerleştirilecek bir mikroçip ile yön bulma duygusunun geliştirilebileceğini iddia etmektedir. McEvoy, kuzey yönüne göre mikroçipin titreşim vererek yönümüzü her daim saptamamızı sağlayacak bir teknoloji üzerine çalışmaktadır[98].

Dsruptive Subdermals isimli İsveç menşeili bir şirket, şirketin genel müdürü olan Hannes Sjöblad[99]'ın vücuduna yerleştirilmiş olan mikroçip aracılığıyla Covid-19 aşı sertifikalarının okunabilirliğini test etmiştir[100]. Aynı zamanda mikroçip taramasıyla QR kod alınabildiğini de göstermiştir[101]. Sjöblad halen mikroçip partileri düzenleyerek insanları mikroçip kullanımına teşvik etmektedir. İsveç'te oldukça yaygınlaşan mikroçip teknolojisi devlet desteği de almış ve ulusal demiryolu ağında kullanılmaya başlanarak çip bilet kavramını doğurmuştur. İsveç vatandaşları mikroçiplerine kayıtlı bilet bilgileri ile trene binebilmektedirler.

---

[97] YouTube. "comprar en maquina vending con implante chip sin llevar dinero bodyhacker" https://www.youtube.com/watch?v=tLWzTIvRIkk, Erişim: 10.10.2021; Dangerous Things. "X-Series Implantable Transponder FAQ", https://forum.dangerousthings.com/t/x-series-implantable-transponder-faq/28#faq-checkpoints, Erişim: 10.10.2021.

[98] CNN Edition. "Forget wearable tech, embeddable implants are already here", http://edition.cnn.com/2014/04/08/tech/forget-wearable-tech-embeddable-implants/index.html, Erişim: 12.10.2021.

[99] Stephen S./ Penny T. (2018). "The technology getting under your skin: Swedish biohacker says bio-implants movement growing globally", News, https://www.abc.net.au/news/2018-08-28/swedish-biohacker-says-bio-implants-movement-growing-globally/10170326, Erişim: 10.10.2021.

[100] Dsruptive Subdermals. "Biohackinfo News (English)", https://dsruptive.com/media/ Erişim: 12.10.2021; Biohackinfo, "The world's first implantable vaccine passport is here and it can monitor pandemics in real time", https://biohackinfo.com/news-dsruptive-temperature-microchip-implant/, Erişim: 12.10.2021.

[101] Wikipedia, "Mikrochip implant (human)", https://en.wikipedia.org/wiki/Microchip_implant_(human)#:~:text=A%20human%20microchip%20implant%20is,body%20of%20a%20human%20being., Erişim: 06.01.2022.

İsveç, insanlar üzerinde mikroçip implantının sayısal oranında dünyada başı çekmektedir. İsveç'te işçilerin giriş çıkış kayıtlarını yani puantaj kayıtlarını tutmak için mikroçip teknolojisini kullanan şirketler de bulunmaktadır[102].

İsveç merkezli mikroçip üretim şirketi olan bir diğer şirket Biohax da; çalışanlarına kapıları açmak, yazıcıları el işaretiyle hareket ettirmek için mikroçip enjekte etmeyi teklif etmektedir. Biohax şirketi aynı zamanda birçok tanınmış Birleşik Krallık şirketine de hizmet sunmaktadır[103]. Biohax İtalya'nın başındaki yetkili Eric Larsen, İtalya'da hastanelerden, tıp merkezlerinden, diğer sağlık kuruluşlarından ve sağlık bakanlığından çip kullanımı için onay beklediklerini açıklamıştır[104]. Yine bir İngiltere firması olan BioTeq'de mikroçipler üzerine çalışma yürütmekte ve mikroçiplerin bir ödeme aracı olarak kullanıma başlamasını amaçlamaktadır.

Amerika Birleşik Devletleri'nin Ohio eyaletinin Cincinati şehrinde City Watcher isimli bir şirket 2006 yılında çalışanlarına mikroçip yerleştiren dünyadaki ilk şirket olmuştur. Şirket bina içerisindeki erişim ve yetki ayrımını sağlamak ve birtakım verilerin güvenliği amacıyla yüksek güvenlik önlemleri kapsamında bu yolu tercih etmiştir[105].

Deri altı mikroçip üretiminde ismi çok duyulan şirketlerden biri olan VeriChip firması da mikroçip kullanımını daha çok sağlık üzerine teşvik etse de nükleer santraller gibi yüksek güvenlik önlemleri alınması gereken yerler için de mikroçip kullanımını pazarlamıştır[106].

---

[102] Dünya Haber. "3 Bin İsveçli Neden Çip Takıyor?", https://www.dunya.com/sektorler/teknoloji/3-bin-isvecli-neden-cip-takiyor-haberi-425296, Erişim: 12.12.2021.

[103] Kardo, K.İ./ Arnab, P./ Nicolai, O. (2019). "Adoption Of Human Microchip Implants For Business Organizations", Aalborg University, Doktora Tezi, https://projekter.aau.dk/projekter/en/studentthesis/adoption-of-human-microchip-implants-for-business-organizations(4ae5f3a0-db6c-476d-b904-d040559227d4).html, Erişim: 12.10.2021; Dünya Haber. "3 Bin İsveçli Neden Çip Takıyor?", https://www.dunya.com/sektorler/teknoloji/3-bin-isvecli-neden-cip-takiyor-haberi-425296, Erişim: 12.12.2021.

[104] Chadwick, L./ Wasserman R. (2021). "Will microchip implants be the next big thing in Europe?", https://www.euronews.com/next/2020/05/12/will-microchip-implants-be-the-next-big-thing-in-europe, Erişim: 12.12.2021.

[105] Lawn&Landscape. "Ohio Employer Implants Employee Microchip" https://www.lawnandlandscape.com/news/ohio-employer-implants-employee-microchip/, Erişim: 01.10.2021

[106] Forbes. (2022). "Chip Shot", https://www.forbes.com/forbes/2002/1223/076.html?sh=3b52aa1d11ee, Erişim: 01.10.2021.

VeriChip şirketi, on yıldan fazla bir süredir hayvanlar için RFID etiketleri satmakta ve dünya çapında yaklaşık 2.000'i insanlara implante edilmiş 7.000 mikroçip satmıştır[107]. VeriMed adını verdikleri program çerçevesinde ürettikleri mikroçipler ile hastaların sağlık bilgilerini alarak tıbbi geçmişlerini mikroçiplere işleyen şirket, birçok hastaneye de çip okuyucu dağıtmış ve mikroçip kullanımını yaygınlaştırmayı amaçlamıştır. Şirket hastaların kimlik etiketleri ve hastane bilezikleri gibi görünüşlerini etkileyen ürünleri kullanmaktansa deri altı mikroçip kullanımını tercih edilebileceğini savunmaktadır.

VeriChip şirketinin çip sisteminin kabul görmesine kadar geçen sürede Amerika'da doktorların insanlara implant yerleştirme yetkisi bulunmamaktadır. Yasadışı yollarla bu tip faaliyetleri yapan doktorların lisanslarına ise el konulmuştur. 2004 yılında Amerikan Gıda ve İlaç Dairesi (FDA) insan bedeni üzerinde VeriChip'in mikroçipinin kullanılmasına onay vermiştir[108].

Amerikan Gıda ve İlaç Dairesi (FDA) çipi onayladıktan sonra VeriChip şirketi mikroçipin vücutta hareket ederek çıkarılmasının zorlaşabileceğine, MR cihazlarıyla uyumsuz olabileceğine, yanıklara neden olabileceğine, enjeksiyon işleminin yeterince steril gerçekleştirilmemesi durumunda vücutta enfeksiyona neden olabileceğine veya vücudun çipi reddetmesi gibi bazı olası sonuçlara ilişkin uyarılarda bulunmuştur. Bu tip yan etkiler arasında MR makinelerine giren çipin patlayacağı şeklinde oluşan korku bir internet mitine dönüşmüştür. Mythbusters isimli Amerikan yapımı bir televizyon şovu, 87.bölümünde bir domuzun derisine mikroçip enjekte ederek çipin, MR cihazının güçlü mıknatısıyla iletişime geçerek patlayıp patlamayacağını test etmiştir. Bununla da sınırlı kalınmamış ve programda Kari Byron isimli kadın sol koluna enjekte edilmiş bir çip ile MR makinesine girmiştir[109]. Testin sonucunda hem domuz etinin içerisindeki mikroçipe hem de Kari Byron'un kolundaki mikroçipe herhangi bir

---

[107] Todd, L. (2007). USA Today, "Microchips İn Humans Spark Privacy Debate", , https://usatoday30.usatoday.com/tech/news/surveillance/2007-07-21-chips_N.htm, Erişim: 11.10.2021; Molly, M. (2007). "Human-İmplantable RFID Chips: Some Ethical And Privacy Concerns", Healthcare IT News, https://www.healthcareitnews.com/news/human-implantable-rfid-chips-some-ethical-and-privacy-concerns, Erişim: 11.10.2021.

[108] Zor, S. (2014). "Bir Mikroçipim Olsa: RFID", Açık Bilim, http://www.acikbilim.com/2014/10/dosyalar/bir-mikrocipim-olsa-rfid.html, Erişim: 11.10.2021.

[109] Zor, S. (2014). "Bir Mikroçipim Olsa: RFID", Açık Bilim, http://www.acikbilim.com/2014/10/dosyalar/bir-mikrocipim-olsa-rfid.html, Erişim: 11.10.2021; YouTube. "MythBusters The RFID CHIP IMPLANT!", https://www.youtube.com/watch?v=IDq_LBH_ZYs, Erişim: 11.10.2021.

şey olmamıştır ve böylelikle mikroçiplerin MR cihazında patladığına ilişkin mit çürütülmüştür.

Mikroçipler, deneme çalışmaları ve kullanımlarıyla birlikte birçok projede de kullanılmak istenmişlerdir. Örneğin 2017 yılında Dünya Olimposlular Birliğinin Başkanı sporcularda uyuşturucu ve doping kullanımının mikroçip ile kolayca denetlenebileceğini ileri sürerek sporculara mikroçip uygulanmasını teklif etmiştir[110]. Ancak bu uygulama yürürlüğe girmemiştir.

Parkview Hastanesi Klinik Araştırma Merkezi'nde tıbbi direktörü, bir kişinin hayati değerlerini sürekli olarak izleme becerisine sahip prototipler geliştirmek için mikroçip geliştiricilerle birlikte çalışmaktadır[111]. Bu çalışma hem doktorların hem de hastaların gerçek zamanlı olarak doğru tıbbi verilere erişmesine izin verme potansiyeline sahiptir. Sağlık verilerinin mikroçiple işlenmesi için yapılan çalışmalar gerçekten de devrim niteliğindedir. 50 yıl içerisinde deri altı mikroçiplerle kişinin her sabah kendisine sağlık taraması yapabileceği fikrine sahip olan araştırmacılar mevcuttur[112]. Mikroçiplerin sinyal verici olacağı ve duşa kabinlerin MR tarayıcısı olduğu bu senaryoda; her sabah duşta kan basıncı, tansiyon, oksijen seviyesi gibi değerler ölçülecek ve kişiye özel reçete yazılacaktır. Yine kan seviyesinin ölçülmesiyle eksik vitamin ve mineral değerleri tespit edilecek ve bireye özel vitamin karışımları hazırlanacaktır. Bununla da kalmayıp mikroçiplerin beyin dalgalarıyla iletişime gireceği ve sabahları alarm kurmak yerine çipin insanları uyandıracağı ya da kahve makinesine kahve yapması için sinyal göndereceği düşünülmektedir. Özellikle sağlık verilerinin bu denli işlenerek insan yararına kullanılması uzun vadede doktora gidilmesini azaltacak ve sağlık hizmetlerinde ciddi anlamda sadeleşmeye sebep olacaktır.

Mikroçiplerin insan bedeni üzerinde kullanımına ilişkin en kapsamlı çalışmalardan birisi de kontrollü ilaç salınımı yapan mikroçiplerdir. Bu mikroçipler 2

[110] Kelner M. (2017). "Call for athletes to be fitted with microchips in fight against drug cheats" https://www.theguardian.com/sport/2017/oct/10/call-for-athletes-to-be-fitted-with-microchips-fight-against-drug-cheats, Erişim: 15.10.2021.
[111] Thomas. "The Future of Microchip Implants in Humans", https://www.thomasnet.com/insights/the-future-of-microchip-implants-in-humans/, Erişim: 15.10.2021.
[112] Ryan, P. (2021). "Future of healthcare: microcihp implants and no trips to the doctor by 2050", https://www.thenationalnews.com/uae/health/future-of-healthcare-microchip-implants-and-no-trips-to-the-doctor-by-2050-1.1248262, Erişim: 17.10.2021.

cm eninde ve 5 cm boyutunda olup vücudun içerisine yerleştirilmektedirler. Bu mikroçipler içerisinde doz doz ayrılmış ilaçlar bulundurmakta ve belli zaman aralıklarıyla ilaç salınımı yaparak ilacı vücut dokusuna karıştırmaktadırlar[113]. İlaç salınımı yapan mikroçiplerin diyabet gibi sürekli ilaç kullanımını gerektiren hastalıklarda kullanılması düşünülmektedir.

Ağızdan veya damar yoluyla alınan ilaçlarda vücutta ilaç oranı önce yüksekken zamanla düşmektedir. Oysa ilaçlar vücutta etkili olduğu miktar aralığı kadar kullanılmalıdırlar çünkü ancak böylelikle fazla kullanılan ilaç yan etkiye neden olmamakta ve fazladan ilaç kullanımının önüne geçilebilmektedir[114]. Bunun yanı sıra ilaçların vücutta belli bir bölgede etki göstermeleri hedeflenir. Sadece etkiye girmesi gereken bölgeyle etkiye giren ilaç vücudun diğer sağlıklı hücrelerinde yan etkiler göstermeyecek ve hedeflenen tedaviyi sağlayacaktır. Bu alanda 2012 yılında ilk başarılı insan deneyi gerçekleştirilmiştir[115]. Bu deneyde menopoz sonrası kemik erimesi(osteoporoz) yaşayan 8 kadına 4 ay içerisinde 20 farklı günde ilaç salınımı yapan bir mikroçip implant edilmiştir. Bu implantın içinde paratroid hormonu bulunmaktadır ve karın bölgesine basit bir cerrahi işlemle yerleştirilen mikroçip belli aralıklarla ilaç salımı yapmaktadır[116]. Deney sonunda içerisindeki ilaç biten çip geri çıkartılmıştır.

MicroCHIPS şirketi tarafından üretilen bu çip, üç metrelik bir mesafe içerisinde kendine özgü bir frekansta yetkili bir dış cihazla iletişim kurarak kablosuz olarak anında salım veya zamanlama ayarı yapabilmektedir. Çipin üzerinde 20 adet ilaç içeren mikro rezervuar bulunmaktadır. Bu mikro rezervuarların üzerinde de platin ve titanyumdan yapılmış bir zar bulunmaktadır. Cihaz üzerinde titanyum bulunmasının olumsuz etkilere yol açabileceği düşünülmüşse de cihaz bu deney öncesinde

---

[113] Zaki, M./Patil S./Baviskar D./Jain D. (2012). "Implantable Drug Delivery System: A Review" , department of Pharmaceutics, Institute of Pharmaceutical Education, https://sphinxsai.com/2012/pharm/pharm/pt=40(280-292)jm12.pdf, Erişim: 05.10.2021.

[114] Tüylek, Z. (2017). "İlaç Taşıyıcı Sistemler Ve Nanoteknolojik Etkileşim", İnönü Üniversitesi Elektronik ve Otomasyon Bölümü Biyomedikal Teknolojisi, Bozok Tıp Dergisi 7(3); 89-98, s. 90, http://tipdergisi.bozok.edu.tr/dosyalar/Eylul2017/95-104.pdf, Erişim: 11.10.2021.

[115] Farra, R./Sheppard, N./ Langer, R./MCcabe, L./ Neer, R./ Anderson, J./ Santini, J./Cima, M. (2012). "First-in-Human Testing of a Wirelessly Controlled Drug Delivery Microchip", Science Translational Medicine, https://www.science.org/doi/10.1126/scitranslmed.3003276, Erişim: 07.10.2021.

[116] Youtube. "Implanted microchip may help trat osteoporosis", https://www.youtube.com/watch?v=Ap47khjw5n8&t=37s, Erişim: 07.10.2021.

biyouyumluluk testlerinden geçmiştir[117]. Başarılı olunmuş bu deneyle sağlık için mikroçip kullanımı doktora gitmeden tedavinin mümkün olduğunu göstermiştir. Bu deneyle aynı zamanda bireyin ilaç alımını unutma, reddetme veya doz aşımı gibi faktörlerinde gerçekleşmesinin önüne geçilmiştir.

Direkt olarak etki yapılmak istenen dokuya yakın olarak yerleştirilen mikroçip böylelikle vücudun yan etki gösterme ihtimalini azaltmaktadır. Bu mikroçipler aynı zamanda biyolojik olarak duyarlı salınım yapmaktadırlar. Yani sürekli olarak temas ettiği dokudan elde ettiği verilere göre ilaç salımını ayarlayabilmektedirler. Uzaktan erişim sağlanabilen bu cihazların bir kolaylığı da hastanın doktoru, hastanın durumunu içeriden takip edebilecek ve verileri cep telefonundan görebilecektir[118].

İnsan bedeni üzerinde mikroçip uygulaması halen daha dünyanın birçok yerinde tepki ile karşılanmakta ve birçok yasal mevzuatta da herhangi bir hüküm ve koşullara tabi tutulmamıştır. Örneğin Avustralya'nın Sydney şehrindeki bir bio-hacker, yerel ulaşım kartının çip kısmını kesip biyo-uyumlu bir plastikle kaplayarak deri altına yerleştirmiştir[119]. Ancak toplu taşımayı kullanırken görevli memurlar, bio-hacker'ın ulaşım kartı ibraz etmemesi sebebiyle hakkında tutanak tutmuşlardır. Bunun üzerine olay mahkemeye taşınmış ancak mahkemeden de olumlu sonuç alınamamıştır. Bio-hacker'ın avukatı çip ile ödeme yapılmasının temassız ödeme seçenekleri arasında olduğu savunmasını yapsa da mahkemenin hakimi konuya ilişkin yasanın gelecekte teknolojinin gelişmesi ile kapsamının genişleyebileceğini ancak bugün için günün yasalarına uyulması gerektiğinin ifade etmiştir.

Söz edilen tüm örneklerde de görüldüğü gibi mikroçiplerin barındırabildiği verilerin herhangi bir sınırı yoktur. Deri altı bir mikroçipe kredi kartı bilgilerini yükleyip ödeme yapabilir, ya da mikroçipi bir ödeme sistemine entegre edip yerel

---

[117] Sharma, S./Nijdam, A./Sinha, P. (2006). "Controlled-release Microchips", https://www.tandfonline.com/doi/full/10.1517/17425247.3.3.379, Erişim: 08.10.2021; Prescott, J./Lipka, S./ Baldwin, S. (2006). "Chronic, Programmed Polypeptide Delivery From An İmplanted Multireservoir Microchip Device", Nature Biotechnolohy, https://www.nature.com/articles/nbt1199, Erişim: 08.10.2021.

[118] Zor, S. (2014). "Bir Mikroçipim Olsa: Kontrollü İlaç Salımı", Açık Bilim, http://www.acikbilim.com/2014/11/dosyalar/bir-mikrocipim-olsa-kontrollu-ilac-salimi.html, Erişim: 08.10.2021; Eltorai, A./ Fox, H./ McGurrin, E./ Guang, S. (2016). "Microchips in Medicine: Current and Future Applications*",* https://www.hindawi.com/journals/bmri/2016/1743472/, Erişim: 08.10.2021.

[119] Lily, M. (2018). "Sydney Bio-Hacker Who İmplanted Opal Card İnto Hand Fined For Not Using Valid Ticket", https://www.abc.net.au/news/2018-03-16/opal-card-implant-man-pleads-guilty-transport-offences/9555608, Erişim: 11.10.2021.

ulaşım kartı gibi de kullanabilmek mümkündür. İçerisine ad, soyad, telefon numarası, adres gibi bilgileri yükleyip hızlı bir şekilde kimlik paylaşımı da yapılabilmektedir. Sağlık verileri kapsamında kan grubu, hastalık geçmişi gibi özel nitelikli kişisel verilerinde yüklenebilmesi mümkündür. Henüz mikroçip kullanımı yaygınlaşmadığı veya devlet otoriteleri tarafından tam anlamıyla kabul görmediği için mikroçip kullanımını düzenleyen hukuk kuralları bulunmamaktadır[120]. Bu nedenle mikroçipler ile hangi tip kişisel verilerimizin alınabileceği, ne şekilde paylaşılabileceği, aktarımının nasıl olacağı vb. gibi hususlarda belirlilik yoktur. Ancak hiç kuşkusuz mikroçip kullanımı yaygınlaşırsa ve devlet otoriteleri tarafından da tanınırsa bu konuda düzenlemeler getirilecektir.

3.4. Mikroçiplerin Kullanımı Esnasında Kişisel Verilerin Korunması

3.4.1. Mikroçipler İle Kişisel Verilerin İşlenmesi

Mikroçiple veri işleme kişilerin doğrudan tasarrufunda olan bir işleme tipidir. Bir kameranın uzaktan görüntü alıp kişinin görüntü verisini işlemesinden farklıdır. Mikroçip sahibi kişi çipin içerisinde yer alan verilerinin tipini değiştirebileceği gibi sınırını daraltıp genişletebilmektedir[121].

Kişisel verilerin kaydedildiği ortam, otomatik (dijital) veya veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan (analog) olabilmektedir. Mikroçiplerle veri işleme bu açıdan incelenecek olursa internet bağlantılı bir veri tabanından veri işleme faaliyeti yürütüleceği için otomatik (dijital) yollarla veri işleme gerçekleşecektir. Kişisel Verileri Koruma Kurumu'nun öngördüğü teknik tedbirler gereğince bu internet veri tabanının yurtiçi menşeili olması gerekmektedir. Aksi takdirde çip içerisindeki kişisel verilerin yurtdışına aktarımı söz konusu olacaktır[122].

Tüm kişisel veriler, paylaşılmadıkça, bireyin beyninde bir düşünce formundadır. Mikroçiplerle veri işleme faaliyeti, bireyin bu düşüncelerinin veri işleme faaliyetiyle çipe aktarımı şeklinde gerçekleşecektir. Bu nedenle birey burada kullandığı mikroçipe

---

[120] Lohrmann D. (2023). "From Progress to Bans: How Close Are Human Microchip Implants?", https://www.govtech.com/blogs/lohrmann-on-cybersecurity/from-progress-to-bans-how-close-are-human-microchip-implants, Erişim: 20.03.2023.

[121] Coldiron R. (2021). "Here's How to Update Your Pet's Microchip Information" , https://www.marthastewart.com/8136232/how-update-pet-microchip-information#:~:text=Visiting%20the%20Registry's%20Site,information%20or%20call%20the%20registry. Erişim: 02.02.2022.

[122] Aktarıma ilişkin detaylı bilgi Üçüncü Bölüm'ün 2.2. numaralı başlığında verilmiştir.

hangi verilerinin aktarılacağını tercih edebilecektir[123]. Bu tercihi yaparken birey oldukça dikkatli olmalı ve gerekmedikçe mikroçiple kişisel veri işlenmemesini sağlamalı ve işleme faaliyetini basit düzeyde tutmalıdır.

Ad, soyad, adres, iletişim bilgisi gibi veriler herkesin hemen her gün en çok paylaştığı kişisel verilerdir. Kanaatimizce mikroçiplerle kişisel veri işleme faaliyeti yürütüldüğü takdirde bu faaliyetin veri sağlayıcısı olarak ya devlet altyapısı kullanılacak ya da aracı nitelikte özel şirketlerden yararlanılacaktır[124]. Bu çalışmada da bu ihtimale yönelik olarak veri işleme faaliyeti ele alınmıştır.

Kimlik verileri, iletişim verileri gibi kişisel veriler, devlet altyapısında devletin işleyişi gereği bulunurken, çipler için veri işleme faaliyeti aracı nitelikte özel şirketler aracılığıyla yürütülecekse bu kişisel verilerin aracı şirketlerle paylaşılması gerekecektir. Daha sonra şirketler işledikleri kişisel verileri mikroçipe yükleyecek ve birey bu verilerini aktarmak için mikroçipini kullanabilecektir. Devlet altyapısının kullanılması durumunda ise devlet, verileri tekrar almasına gerek kalmadan işleyebilecektir[125].

Özel nitelikli kişisel verilerin yani kişinin 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 verilerinin mikroçiple işlenmesi durumunda, her bir özel nitelikli kişisel verinin veri işleme prosedürü farklı olacaktır. Kanaatimizce mikroçiplerle özel nitelikli kişisel veri işleme, sağlık bilgileri ile sınırlı kalmalıdır. Sağlık verilerinin de veri ihlaliyle karşı karşıya kalınmaması için ciddi güvenlik önlemleri çerçevesinde saklanması gerekmektedir[126]. Sağlık bilgisi haricindeki özel nitelikli kişisel verilerin bireyin yararı amacına kullanımı oldukça zor olduğu gibi mahiyetleri gereği de çip içerisinde sürekli güncel olarak tutulmaları mümkün olmayacaktır.

[123] Coldiron, Erişim: 02.02.2022
[124] Jones C. (2023). "4 Thıngs That Wıll Defıne Government Data Storage In 2023 And Beyond", https://redriver.com/storage/government-data-storage, Erişim: 02.02.2023.
[125] Jones, Erişim: 02.02.2023.
[126] Tükel, R. "Kişisel Sağlık Verileri Korunmalıdır!", http://www.tipdunyasi.dr.tr/2017/06/kisisel-saglik-verileri-korunmalidir/, Erişim: 02.02.2022.

Irk, etnik köken bilgisinin mikroçiple işlenmesi durumunda kişi ya bu bilgilerini aracı şirketle paylaşmış olmalı ya da devlet altyapısında bir yerde bu veriler kaydedilmiş olmalıdır. Bu veriler zorunlu olmadıkça işlenmemelidir. Irk ya da etnik köken bilgisinin, mikroçip ile yapılacak herhangi bir işlemde kullanılması oldukça düşük bir ihtimal olduğu için bu tip verilerin mikroçip veri tabanı içerisine girmesinde bir yarar yoktur. Ölçülülük ilkesi[127] gereğince de mikroçipte buna ilişkin veri bulundurulmaması uygundur.

Siyasi düşünce, felsefi inanç, din, mezhep gibi kişisel veriler sonradan değişebilecek kişisel veriler olup her an paylaşımları mümkün değildir. Kişinin bu tip kişisel verilerini de mikroçipe yüklemesine gerek yoktur; çünkü bunların aktarımını gerektirecek bir durumun söz konusu olması düşük ihtimaldir. Kişi bu bilgileri gerektiğinde mikroçip kullanarak aktarmak yerine direkt söyleyerek de aktarabilir. Üstelik bunlar ve bunlar gibi birçok kişisel veri bireyler tarafından gün içerisinde sürekli aktarım halindedir. Her bir verinin mikroçiple aktarılması mümkün olmayacaktır[128].

Kanun; sağlık ve cinsel hayata ilişkin kişisel verilerin ancak kamu sağlığının korunması, koruyucu hekimlik tıbbi 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 işlenebileceğini ifade etmiştir. Mikroçiplerin kullanılmak istemesinin temelinde yatan sebeplerden biri de kişinin tıbbi geçmişine ve sağlık bilgilerine hızlıca ulaşılmasının istenmesidir. Kişinin sağlık bilgilerinin mikroçiplere aktarılması devlet veya özel hastaneler aracılığıyla gerçekleşecektir. Örneğin kişi bir tedavi almak için hastaneye gidecek, çipiyle hasta girişi yapılacak ve yine tedavisi sonucunda alması gereken ilaçları çipine işlenecektir. Kişi, eczaneye gittiğinde çipini okutarak kendisi için yazılmış olan reçetedeki ilaçları temin edebilecektir. Bu durum özellikle ilaç almakta zorlanan yaşlılar, konuşma zorluğu olanlar için kolaylık sağlayacaktır. Burada devlet hastaneleri, özel hastaneler ve

[127] Erdinç G. (2020). "Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi" Kişisel Verileri Koruma Dergisi , C.2, S.1, https://dergipark.org.tr/tr/download/article-file/1195495, Erişim: 02.02.2022.

[128] By Mıchelson Found Anımals Foundatıon. "5 Things You Didn't Know About Microchips", https://www.foundanimals.org/5-things-didnt-know-microchips/, Erişim: 05.12.2022.

eczaneler yetkili kurum ve kuruluş olarak kişinin sağlık bilgilerini işleyecek ve mikroçipe aktaracaklardır. Bu verilerin güvenliği ise bu kuruluşlara ait olacaktır[129].

Ülkemizde sağlık bilgilerinin aktarımı için dahi mikroçip kullanımı bulunmamaktadır. Sağlık bilgilerinin mikroçipe işlenmesi mikroçip kullanımının bulunduğu ülkelerde aracı nitelikte özel şirketler aracılığıyla yapılmaktadır. Örneğin VeriChip şirketi halihazırda sattığı mikroçiplerin içerisine kişinin sağlık bilgilerini de işlemekte ve anlaşmalı hastanelere de çip okuyucu dağıtmaktadır. Bu çipler VeriChip şirketinin veri tabanını kullanmaktadır[130].

Gömülü Biyo-Sensör Sistemi adını verdikleri bir patente sahip olan VeriChip şirketi ve Receptors şirketi, bireyler için vücuttaki glikoz seviyesini gerçek zamanlı olarak ölçebilen bir biyo-algılayıcı olan bir prototip mikroçip geliştirmişlerdir[131]. Health link (sağlık bağlantısı) adını verdikleri bir bağlantı kişinin kişisel sağlık verilerinin kaydının bağlantısıdır. Health link, çip sahibini kişisel sağlık kayıtlarına[132] bağlayan güvenli, özel bir çevrimiçi veri tabanı kullanmaktadır. Bu bağlantı sayesinde kişi çipini okuttuğunda doktorlar, hemşireler veya acil müdahalede bulunan diğer sağlık görevlileri bireyin hayati tıbbi verileri ve acil durum iletişim verilerine ulaşmaktadır.

Bir şeyleri satın almak ya da satmak için de mikroçiplerin kullanıldığı düşünüldüğünde ödeme bilgileri ve alışveriş geçmişi verileri de çipler aracılığıyla işlenecektir. Son dönemde marketlerde kasiyersiz kasa uygulamasına geçildiği sıklıkla görülmektedir. Mikroçiple ödeme yapıldığı durumda bu tip ödeme uygulamaları hız kazanacaktır. Birçok ödemenin mikroçip aracılığıyla yapılması insanların kolayına gidecek ve mikroçiple ödeme faaliyeti artacaktır[133]. Bu da bir yerde kayıt dışı ekonominin önüne geçilmesine de katkı sağlayacaktır. Devletler kayıt dışı ekonominin önüne geçilmesi amacıyla dahi bu tip bir ödeme sistemini kabul etmeye sıcak bakacaklardır.

---

[129] Ömür, R. (2018). "Kişisel Sağlık Verilerinin Korunması ve Hastanelerin Sorumluluğu", YÜHFD, C.XV, No:1, s. 133-180, s. 163, http://law.yeditepe.edu.tr/sites/default/files/yuhf_dergisi_v.14.pdf, Erişim: 09.10.2021.

[130] Zor, Erişim: 05.04.2022.

[131] VeriChip. "GlucoChip" , http://www.verichipcorp.com/products_glucochip.html, Erişim: 12.10.2021.

[132] Güven, s. 6; Hakeri H. (2019). "Sağlık Hukuku", 2.Baskı, Seçkin Yayıncılık, Ankara, s. 348-349.

[133] Latham, K. (2022). "The microchip implants that let you pay with your hand", https://www.bbc.com/news/business-61008730, Erişim: 04.11.2022.

Mikroçipin bir banka hesabı ile entegre çalışması halinde parayı direkt olarak çipi okutarak harcamak mümkün olacaktır[134]. Dangerous Things şirketi talep edilmesi durumunda çipi bir banka hesabına entegre etmektedir. Sadece aktif banka hesapları değil Bitcoin cüzdanı yani kripto para hesabı da çiple entegre edilebilmektedir. Polonyalı- İngiliz girişimi olan Walletmor isimli şirket bunu sağladığını ve bu şekilde ödemenin yayılacağını iddia etmektedir[135].

Son dönemde tüm dünyayı sarsan Covid-19 salgını ödeme alışkanlıklarını da oldukça değiştirmiştir. Banka kartları ve kredi kartlarındaki temassız ödeme uygulaması Covid-19 dönemi uygulamaları ile yaygınlaşmıştır. Ödeme seçenekleri gibi birçok faaliyeti temassız gerçekleştirme fikri insanları daha güvende hissettirmiştir. Mikroçiplerle günlük hayatta birtakım faaliyetleri yerine getirecek olmak bu temassız dünyaya hizmet edecektir. Halihazırda İngiltere'de bu şekilde ödeme yapılabilmektedir. Temel anlamda banka kartları ve kredi kartları da RFID teknolojisi ile çalışmaktadır. Bu sefer ödeme (pos) cihazına yaklaştırılacak olan banka kartı veya kredi kartı değil mikroçip olacaktır[136]. Teorisyenlerin ve distopya severlerin üzerine konuştuğu konulardan biri olan nakit parasız yaşam da mikroçiplerin yaygınlaşması ile gerçekleşebilecek bir senaryodur.

Kişisel dijital veri pazarının bu gibi uygulamalarla genişleyerek 2025 yılına kadar 500 milyon dolar değerinde olması beklenirken 2028 yılına kadar 5 milyar doları bulacağı tahmin edilmektedir[137].

3.4.2. Mikroçipler İle İşlenen Kişisel Verilerin Saklanması ve Korunması

Kişisel verilerin saklanması fiziksel saklama ve dijital saklama olmak üzere iki şekilde gerçekleşebilmektedir. Fiziksel saklama kağıda yazılı belgeler ve dokümanların saklanmasını ifade ederken dijital saklama ise telefon, bilgisayar gibi

---

[134] Grauer, Y. (2018). "A practical guide to microchip implants", Arstechica, https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/, Erişim: 15.10.2021.

[135] Notes From Poland. "World's first payment chip that can be implanted under skin launched by Polish-British startup", https://notesfrompoland.com/2021/04/14/worlds-first-payment-chip-implanted-under-skin-launched-by-polish-british-startup/, Erişim: 13.12.2021.

[136] Latham, Erişim: 04.11.2022.

[137] Fortune Business Insights. (2023). The global digital transformation market is projected to grow from $2.27 trillion in 2023 to $8.92 trillion by 2030, at a CAGR of 21.6% during the forecast period... Read More at:- https://www.fortunebusinessinsights.com/digital-transformation-market-104878, Erişim: 17.03.2023.

teknolojik aletler içerisindeki saklama faaliyetini ifade eder. Fiziksel olarak saklanan belgeler saklama sürelerine göre arşivlenerek evrak arşivinde saklanmalıdır. Aynı şekilde dijital olan belgeler de saklama sürelerinin sonuna kadar veri ihlallerinden korunacak şekilde dijital ortamda güvenli bir şekilde saklanmalıdır[138]. Mikroçipler ile işlenen veriler için saklama faaliyeti bir dijital saklama çeşididir. İnternet bağlantısı olmadan internet veri tabanına ulaşım mümkün olmayacağı için mikroçip internet olmadan herhangi bir veri akışı sağlamayacak ve tek başına herhangi bir kişisel veri sızıntısına sebep olamayacaktır.

İnternet veri tabanına bağlı şekilde hizmet veren mikroçiplerin güvenliği için veri tabanına hizmet veren internet sunucusunun bilgilerine bakmak gerekmektedir. Sunucu güvenilir olmalı ve veri sızıntılarına karşı gerekli yazılım ve donanıma sahip olmalıdır. Mikroçiplerin devlet veri tabanına bağlı olduğu senaryoda çiplerdeki kişisel verilerin güvenliğini tehdit edebilmek için günümüzde aktif bir şekilde kullanılan e-devlet sisteminin veri tabanının tehdit edilmesi gerekmektedir. Bireyin devlet altyapısında bulunan tüm verileri elbette mikroçipe işlenmeyecek, ancak çipin veri tabanına herhangi bir sızıntı olması durumunda kişi hakkında devletin sahip olduğu diğer verilere de ulaşılacaksa bu durumda her ne kadar doğruluk ve güncellik için devlet alt yapısını kullanmak daha makul görünse de devlet alt yapısı bu denli büyük bir veri sızıntısı tehlikesi düşünüldüğünde kullanılmamalıdır. Bu durumda bugün veri bankası[139] olarak hizmet gören şirketler gibi mikroçip veri dağıtım şirketi ya da mikroçip veri işleme şirketi gibi şirketler kurulursa, bu şirketler aracılığıyla çiplere veri işleme faaliyetinin düşünülmesi gerekmektedir.

Veri işleme, saklama, koruma ve imha prosedürlerinin aracı nitelikte özel şirketlerin elinde olması durumunda çip sahipleriyle yapılan kullanım sözleşmeleriyle bu şirketlerin verilerin saklanması ve korunmasına ilişkin sorumlulukları doğacaktır. Kanaatimizce veri işleme faaliyetinin aracı nitelikte özel şirketler aracılığıyla

[138] Kara, İ. (2019). "Dijital Verilerin İmha Süreçlerinin Tanımlanması Ve Uygulama Yönünden Değerlendirilmesi", https://dergipark.org.tr/tr/download/article-file/901385, Erişim: 12.12.2022.

[139] Yerel veya uzaktan bilgi alımını kolaylaştıracak şekilde düzenlenen ve uzun bir süre boyunca birçok sürekli sorguyu işleyebilen bilgi deposudur. Wikipedia. "Veri Bankası", https://en.wikipedia.org/wiki/Data_bank, Erişim: 02.01.2022; Uygun, M. (2010). "Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Koruması", Yayımlanmamış Yüksek Lisans Tezi, Ankara, s. 11; Uncular, s. 51.

yapılacak olması daha olasıdır. Devlet tamamen bu altyapıyı üstlenmeyecek ve özel şirketler aracılığıyla yürütülmesini düzenleyici kurallar koyacaktır.

Kişisel verilerin korunmasına yönelik tedbirler alınması ve bunların korunmasının bu denli önem arz etmesinin temelinde bilinçsizce ve rıza dışı veri ticareti faaliyetinin kontrol altına alınması gerekliliği yatmaktadır[140]. Çiplerle veri işleme faaliyeti başladığında hiç şüphesiz özel şirketler ticari menfaatleri için bu işleme faaliyetine dahil olmak isteyecek ve bireylerin verilerini öğrenmek için çaba gösterecektir.

Veri işleme faaliyetinin hem devlet hem de aracı nitelikte özel şirket alt yapısı ile gerçekleştiği düşünülürse -ki kanaatimizce tercih edilecek sistem bu olacaktır- verilerin doğruluğu ve güvenliği[141] devlet altyapısı ile desteklenirken özel şirketler de çiplerle veri işleme faaliyetinden uzak kalmayacak ve sektör bu şekilde gelişecektir. Hem özel sektörün hem de devletin yer aldığı bir altyapı sisteminde her veri tabanı, kendi himayesinde barındırdığı verinin güvenliğini sağlamakla sorumlu olacaktır.

3.4.3. Mikroçipler İle İşlenen Kişisel Verilerin İmhası

Kanun'a göre saklama süresi dolan kişisel verilerin imha edilmesi gerekmektedir. Bir verinin saklama süresi çoğu zaman mevzuatta öngörülmekte, mevzuatta öngörülen süre yok ise veri sorumlusu tarafından tayin edilen süre kadar olmaktadır[142]. Mikroçipler ile işlenen kişisel veriler, kişi mikroçip sahibi oldukça kişinin himayesinde taşınmaya devam edecektir. Mikroçiplerin içerisindeki kişisel veriler saklama veri tabanında süresiz bir şekilde kalacaktır. 10 yıllık kullanım süresi dolan bir mikroçip çıkartılarak bilgileri ve ID numarası yeni mikroçipe aktarılmalı ve mevcut mikroçip imha edilmelidir. Bu imha ile o mikroçipe hiçbir şekilde erişilememeli ve çip tekrar kullanılamaz hale getirilmelidir.

Devlet altyapılı bir sistem geçerli ise mikroçiplerin imhası resmi bir şekilde devlet eliyle gerçekleştirilmelidir. Kişi kendi mikroçipini çıkartmaya çalışmamalı, çip

[140] Türkiye Gazetesi, (2022). "İnternette karanlık ticaret! Türkiye'de her gün 50 milyon dolarlık işlem yapılıyor: Instagram hesabı çalma, kredi sicili düzeltme...", https://www.turkiyegazetesi.com.tr/ekonomi/internette-karanlik-ticaret-turkiyede-her-gun-50-milyon-dolarlik-islem-yapiliyor-instagram-hesabi-calma-kredi-sicili-duzeltme-907887, Erişim: 08.10.2021.
[141] Yücedağ N. (2019). "Kişisel verilerin korunması kanunu kapsamında genel ilkeler", Kişisel Verileri Koruma Dergisi, C.1, S.1, https://dergipark.org.tr/tr/download/article-file/737938, Erişim: 08.10.2021.
[142] Yücedağ, Erişim: 08.10.2021.

steril bir ortamda doktor ya da hemşire tarafından cerrahi olarak çıkartılmalıdır. Çıkartılan mikroçip için Kanun'a uygun bir imha tutanağı tutulmalı ve bu tutanak saklanmalıdır[143]. İmha edilen mikroçip yerine kişinin yeni mikroçipi enjekte edilmelidir. Altyapının aracı nitelikte özel şirketlerle desteklenmesi durumunda bu faaliyetleri aracı şirketler yerine getirecektir.

Mikroçipler imha edilirken veri imha yöntemleri kullanılabilir. Yüksek manyetik alana maruz bırakmak (de-manyetize etme) bunlardan biridir[144]. Bu yöntem aracılığıyla manyetik medya özel bir cihazdan geçirilir ve yüksek bir manyetik alana maruz bırakılarak üzerindeki veriler okunamaz hale getirilir[145]. Çıkartılan mikroçip özel bir manyetik alana maruz bırakılarak bu şekilde imha edilebilir. Bir diğer yöntem fiziksel olarak yok etmektir. Mikroçipler tıbbi cam kapsül, bakır anten ve silikon bilgisayar çipinden oluşmaktadır[146]. Sadece fiziksel olarak bu silikon bilgisayar çipinin imhası verilerin imhası için yeterli olacaktır. Çipin dışındaki tıbbi cam kapsül ve bakır anten tekrar kullanılabilecektir. Bilgisayar çipinin imhası öğütmek, toz haline getirmek, eritmek, yakmak işlemlerinden birisinin yerine getirilmesi ile de gerçekleşebilecektir.

Bir diğer veri imha yöntemi üzerine yazmadır. Bu imha yönteminde amaç, manyetik medya ya da optik medya üzerine 7 kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin özel yazılımlarla kurtarılabilmesinin önüne geçmektir. Mikroçipler bakımından bunun yapılabilmesi için mikroçipin içerisindeki bilgisayar çipinin çıkartılarak verilerin üzerine yazma yapılmalıdır[147].

---

[143] Kişisel Verileri Koruma Kurumu. (2018). Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf, Erişim: 19.05.2022.

[144] Kişisel Verileri Koruma Kurumu. (2018). Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf, Erişim: 20.05.2022.

[145] Kişisel Verileri Koruma Kurumu. (2018). Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf, Erişim: 20.05.2022.

[146] Uralstk. "İnsan vücudundaki bir çip nasıl belirlenir. İnsanlara kim cips koyar? Parçalamanın avantajları ve dezavantajları", https://uralstk.ru/tr/a-healthy-lifestyle/kak-opredelit-chip-v-tele-cheloveka-kto-stavit-lyudyam-chipy/, Erişim: 19.12.2022.

[147] Hürriyet. (2019). "Tamamen silinmesi istenen verinin üzerine yeni veri yazılmalı", https://www.hurriyet.com.tr/teknoloji/tamamen-silinmesi-istenen-verinin-uzerine-yeni-veri-yazilmali-41108551, Erişim: 19.12.2022.

Veri imha yöntemlerinden bir diğeri olan anonimleştirme mikroçipler için söz konusu olmayacaktır[148]. Çünkü mikroçipler sadece üzerinde bulunduğu bireyin verilerini taşıdığı için anonimleştirme faydasız olacaktır.

3.5. Mikroçipler İle Veri İşlemenin Kişisel Verilerin İşlenmesinin Temel İlkelerine Göre Durumu

Kişisel verilerin hukuka uygun olarak işlenebilmesi için uluslararası ve ulusal mevzuatta ve uygulamada benimsenen birtakım temel ilkelere uygun davranılması gerekmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde kişisel verilerin işlenmesine ilişkin usul ve esaslar, 108 sayılı Sözleşmeye ve 95/46/EC sayılı Avrupa Birliği Direktifine uygun şekilde düzenlenmiştir[149]. Bu ilkelerin her biri, tüm veri işleme faaliyetleri için azami önem ihtiva etmekte olup veri koruma hukukunun da temelini oluşturmaktadır. Bu bağlamda otomatik olan ya da otomatik olmayan yollarla yapılan tüm veri işleme faaliyetlerinin bu ilkelere uygun olması gerekmektedir.

Kanun'da kişisel verilerin işlenmesinde sayılan genel (temel) ilkeler şunlardır: Hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Mikroçiplerle işlenecek kişisel verilerin işlenmesi süreçlerinde de bu ilkelere riayet edilmesi gerekliliği kaçınılmazdır. Zira mikroçiplerle işlenecek kişisel veriler hususunda en çok tartışılacak konulardan biri, bu işleme faaliyetinin, kişisel verilerin işlenmesine ilişkin temel ilkelere uygunluğunun denetimidir.

Tüm kişisel veri işleme faaliyetleri, bu sayılan ilkelere uygun olacak şekilde yapılmalıdır[150]. Mikroçiplerle kişisel veri işleme faaliyetinin de kanuna uygun bir

---

[148] Kişisel Verileri Koruma Kurumu. (2018). Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf, Erişim: 20.05.2022.

[149] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Yayınlar, Rehberler, "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler", https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf, Erişim: 14.11.2021.

[150] Develioğlu, H.M. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü*, İstanbul: Oniki Levha Yayınevi, s. 44.; Çekin, M. S. (2018). *6698 Sayılı Kişisel Verilerin Korunması Kanunu*, İstanbul: Oniki Levha Yayınevi, s. 42.

şekilde yapılabilmesi için, sayılan tüm bu ilkelere uygun şekilde yapılması gerekmektedir.

Günümüzdeki mikroçip kullanımlarında henüz tam anlamıyla veri işleme faaliyeti gerçekleştirilmemektedir. Daha çok kapı açmak, arabayı çalıştırmak gibi basit gündelik işlemler için kullanılan mikroçipler bakımından kişisel veri işleme faaliyeti söz konusu değildir. Çünkü bu çipler, sadece kendilerine has bir barkod ile okuyucu tarafından aktif edilerek çalışmaktadırlar. Çipi taşıyan bireye ait herhangi bir kişisel veri bu tip çiplerde yer almamaktadır. Ancak sağlık verilerinin yer aldığı mikroçiplerde kişisel veri işleme faaliyeti söz konusudur[151].

Kişisel veri içeren mikroçipler, içerisine veri yüklenebilen ve okuyucudan geçtiğinde karşı tarafa çipin sahibi ile ilgili bilgi verebilen çipler olmalıdır. Çipte bulunan kişisel veriler, sadece çipin içine yüklü olabileceği gibi bir internet veri tabanında da saklanabilir. Örneğin öğrencilerinde deri altı mikroçip olan bir okulda, öğrenciler çipi okuyucuya okuttuğunda öğrencinin adı, soyadı, öğrenci numarası gibi bilgilerini çip verebilmelidir. Günlük hayatta kullanılan birtakım kartların üzerindeki çipler de kişisel verileri içermektedir. Örneğin Türkiye Cumhuriyeti kimlik kartlarının yenilenmesi ve çipli haline geçilmesinden sonra eski nüfus cüzdanının arkasında yer alan önceki soyadı, medeni hali, kan grubu, dini, doğum yeri, kayıtlı olduğu yer (ili, ilçesi, cilt, hane, sıra no), veriliş nedeni, veriliş tarihi bilgileri, yeni kimlik kartlarında çipin içerisinde yer almaktadır[152]. Bu gibi kart üzerinde bulunan çiplerin işleme faaliyeti sınırlıdır ve devlet, kamu kurumu gibi otoritelerin kontrolünde veri işleme faaliyeti yapılmaktadır.

Basit düzeyde faaliyet gösteren ve içerisinde kişisel veri barındırmayan çipler için burada bahsedilecek düzenlemeler söz konusu değildir. Burada bahsedilecek düzenlemeler, içerisinde bir kişiye ait ayırt edici bir bilgiyi işleyebilen mikroçipler için geçerli olacaktır. Henüz işleyişi, kapasitesi ve mevcut teknoloji mikroçiplerle bu denli veri işlenmesine imkan vermese de bu çalışmada, gelecekte mikroçiplerle kişilerin

[151]Bilim ve Gelecek. (2017). "Sürekli sağlık gözlemi yapan mikroçip", https://bilimvegelecek.com.tr/index.php/2017/07/01/surekli-saglik-gozlemi-yapan-mikrocip/, Erişim: 05.06.2022.

[152] Türkiye Cumhuriyeti İçişleri bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü. "Türkiye Cumhuriyeti Kimlik Kartı", https://www.nvi.gov.tr/tc-kimlik-karti, Erişim: 07.11.2022.

tanıtıldığı ve birçok faaliyetin gerçekleştirildiği durumda, mikroçiplerle kişisel veri işleme hususunda nelere dikkat edilmesi gerektiğine değinilecektir[153].

3.5.1. Hukuka ve Dürüstlük Kuralına Uygun Olma

Hukuka uygunluk, genel olarak hukuk normlarına ve evrensel hukuk ilkelerine uygunluğu kapsadığı için, kanuna aykırı bir veri işleme faaliyeti, hukuka aykırılığa neden olacaktır. 6698 sayılı Kanun'a aykırı şekilde veri işlenmesi bu ilkeye aykırılık teşkil edecektir. Hukuka uygunluk kavramı, hukuk dilinde, mevzuata ve hukuk ilkelerine uygun olanı ifade etmek için kullanılmaktadır[154]. Hukuk sisteminin sonuç bağladığı bir olgunun mevzuata ve hukuk ilkelerine uygun olması haline hukuka uygunluk denmektedir. Hukuka uygunluktan kasıt elbette yalnızca veri koruma hukukuna uygunluk değil, kişisel veri işleme faaliyetlerinde genel hukuk norm, mevzuat ve ilkelerine uyumluluktur. Bu açıdan hukuka uygunluğu mevzuata uygunluktan ibaret olarak görmemek gerekmektedir. Mevzuatın yanı sıra temel hukuk ilkelerine de uygun bir veri işleme faaliyeti hukuka uygun olabilecektir.

Dürüstlük kuralı, kişisel veriler işlenirken hakkın kötüye kullanılması yasağına uyulmasını gerektirmektedir. Dürüstlük kuralı çerçevesinde hakkın amacına aykırı hareket edilmemelidir. Dürüstlük kuralı doğruluk kuralını ifade etmektedir[155]. Türk hukukunda dürüstlük kuralı, Türk Medeni Kanunu'nun 2. maddesinde: *"Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır"* şeklinde anılmaktadır. Bu haliyle dürüstlük kuralı, hukukun her alanına temas eden bir ilkedir.

Mikroçipler her bir bireyin deri altında olup sadece o kişiye ait bilgiler içerdiği için veri sahibi olan ilgili kişinin kendisi tasarruf yetkisini tam olarak haiz olacaktır. Kişisel veriler mikroçiplerle işlenirken kişinin hangi verilerinin çipe yükleneceği hususunda kişi aydınlatılmalı ve rızası hilafına hakkın kötüye kullanılmasıyla veri işleme yapılmamalıdır. Gereğinden fazla hiçbir kişisel veri çipe yüklenmemelidir[156]. Veri sahibi kişi de günlük hayatta kullanmasını gerektirecek verilerden başka verilerini

[153] Schwartz, Erişim: 11.10.2022.
[154] Eren, F. (2015). *Borçlar Hukuku Genel Hükümler,* 19. Baskı, Yetkin Yayınları, Ankara, s. 601.
[155] Eren, s. 19.
[156] Kişisel Verileri Koruma Kurumu. "İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık)", https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik-, Erişim: 19.12.2022.

mikroçipe yüklememeli ve verilerini koruması gerektiğinin bilincinde olmalıdır. Kişisel veriler mikroçiplerle işlenirken bu işlemenin hukuka uygun olmasına ve dürüstlük kuralına uygun olmasına dikkat edilmesi gerekmektedir.

Dürüstlük kuralı Medeni hukuk kapsamında yer almakla birlikte tüm hukuk dalları için geçerli bir ilkedir[157]. Hukuka ve dürüstlük kuralına uygun veri işleme ilkesi oldukça geniş kapsamlıdır. Hatta bu ilkenin diğer ilkeleri de kapsadığı söylenebilir. Zira sayılan diğer ilkelere uygun bir veri işleme faaliyetinden bahsedilebilmesi için bu ilkeye uygunluk şarttır[158]. Dolayısıyla bu ilkenin tüm yönleriyle kavranması, temel ilkelere uygunluk denetiminin yapılması bakımından önem arz etmektedir. Hukuka ve dürüstlük kuralına uygun veri işleme ilkesinin "hukuka uygunluk" ve "dürüstlük kuralına uygunluk" şeklinde bölünerek incelenmesi faydalı olacaktır.

Doktrinde dürüstlük ilkesinin dört temel fonksiyonunun bulunduğundan bahsedilmektedir[159]. Bu fonksiyonlardan ilki somutlaştırma fonksiyonudur. Somutlaştırma fonksiyonu, tarafların hak ve sorumluluklarının açıkça belirlenmesine, somutlaştırılmasına hizmet eder. Bu haliyle kişisel veri işleme faaliyetinde veri sorumlusunun sorumluluklarının ve ilgili kişinin haklarının açıkça belirlenmesi, somutlaştırma fonksiyonuyla ilgilidir.

Dürüstlük ilkesinin fonksiyonlarından bir diğeri, tamamlama fonksiyonudur[160]. Kişisel veri işleme faaliyetinde tamamlama fonksiyonu, veri sorumlusunun asli yükümlülüklerini yerine getirmek için yapmakla ödevli olduğu yan yükümlülüklerle ilgilidir. Bu haliyle tamamlama fonksiyonunun özellikle veri sorumlusunun veri güvenliğini sağlama yükümlülüğüyle doğrudan ilgili olduğu söylenebilir.

Dürüstlük ilkesinin sınırlama fonksiyonu bulunmaktadır[161]. Bu fonksiyon, hakkın sınırlarına ilişkindir. Kişisel veri işleme faaliyeti düşünüldüğünde veri sorumlusunun işlemiş olduğu kişisel veriler üzerinde sınırsız tasarruf yetkisi olmadığı anlaşılmaktadır. Bu haliyle dürüstlük ilkesinin sınırlama fonksiyonu, kişisel veri

[157] Oğuzman, M.K./Barlas, N. (2018). *Medeni Hukuk*, 24. Bası, Vedat Kitapçılık, İstanbul, s. 262-263.
[158] Dülger, Kişisel Verilerin Korunması Hukuku, s. 42.
[159] Eren, s. 19.
[160] Eren, s.19.
[161] Eren, s.19.

işlemede temel ilkelerden olan "İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması" ilkesiyle bazı yönlerden örtüşmektedir.

Dürüstlük ilkesinin fonksiyonlarından sonuncusu düzeltme fonksiyonudur[162]. Düzeltme fonksiyonu, hukukun diğer alanlarında uyarlama kavramını doğuran fonksiyondur. Dürüstlük ilkesinin veri koruma hukukuna etkisi oldukça fazladır. Nitekim Kişisel Verileri Koruma Kurulu'nun vermiş olduğu kararlara bakıldığında dürüstlük ilkesine uygunluğun kişisel verilerin işlenmesinde ciddi bir denetim kriteri halini aldığı görülecektir[163].

Sonuç olarak kişisel verilerin korunması alanında kişisel verilerin işlenmesinde hukuka ve dürüstlük kuralına uygun olma ilkesi önem arz etmektedir. Her veri işleme faaliyetinin, kendi içinde bu ilkeye uygun olması gerekmektedir. KVKK m.4/2-a bendinde düzenlenen bu ilke "Hukuka ve Dürüstlük Kuralına Uygunluk" şeklinde adlandırılmışken GDPR bu ilkeyi "Hukuka Uygunluk, Adalet ve Şeffaflık" olarak adlandırmaktadır.

Hukuka ve dürüstlük kuralına uygun veri işleme ilkesi, mevzuata uygunluktan ibaret değildir. Bu ilke gereği veri işleme faaliyetinde, mevzuata uygunluğun yanı sıra kişisel verinin sahibinin çıkarlarının ve makul beklentilerinin dikkate alınması ve bu uğurda zarara uğratılmaması gerekmektedir. Yine bu doğrultuda kişisel veri sahibinin öngöremeyeceği faaliyetlerde bulunulmaması, öngörülemeyecek durumların meydana gelmesinin önlenmesi için gerekli tedbirlerin alınması da veri işleme faaliyetinin hukuka ve dürüstlük kuralına uygun olması ilkesinin gereklerindendir.

---

[162] Eren, s.19.

[163] Örneğin Kişisel Verileri Koruma Kurulu'nun 20.04.2021 tarih 2021/389 Karar numaralı kararında; kişisel veri işlemede açık rızanın istisnaları olarak sayılan kişisel veri işleme hukuki sebeplerine dayanılabilecek durumlarda, yine de açık rıza alınarak açık rıza hukuki sebebine dayanılması, hakkın kötüye kullanılması ve dürüstlük ilkesine aykırılık doğuracak unsur olarak yorumlanmış ve veri sorumlusuna yaptırım uygulanmıştır. Bkz. https://www.kvkk.gov.tr/Icerik/6967/2021-389, Erişim: 10.11.2021; Yine örneğin veri sorumlusuna ilgili kişi tarafından yapılan başvurunun veri sorumlusunca reddedilmesi durumunda ret gerekçesinin eksik ve hatalı olması durumu da Kişisel Verileri Koruma Kurulunun 06.02.2020 tarih 2020/86 Karar numaralı kararında yer alan *"Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ kapsamında ilgili kişi tarafından yapılan bir başvuruyu dürüstlük kuralına uygun olarak sonuçlandırmadığı dikkate alınarak, bundan böyle Tebliğ kapsamında ilgili kişiler tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri alması hususunda Şirketin talimatlandırılmasına"* ifadeleriyle dürüstlük ilkesine aykırı görülmüştür. Bkz. https://www.kvkk.gov.tr/Icerik/6732/2020-86, Erişim: 05.09.2021.

Hukuka ve dürüstlük kuralına uygun veri işleme ilkesinin bir sonucu olarak veri sorumlusu, ilgili kişilerce KVKK m. 11'e dayalı olarak yapılan başvuruları uygun şekilde yanıtlamalı veya gereğini yapmalıdır. Şayet böyle bir talebin reddedilmesi söz konusu olursa bu ilke gereği ret kararı gerekçelendirilmeli ve bu kararla ilgili kişi zarara uğratılmamalıdır. Kişisel verileri koruma hukuku açısından kişisel verileri rızası dışında işlenen veri sahibi ya da kişisel verileri ile ilgili veri sorumlusunun veri güvenliği sağlayamaması durumunda zarara uğrayan kişi yine bu zararını Türk Borçlar Hukukunda yer alan haksız fiil hükümleri ile tazmin edebilecektir[164].

Veri sorumlusu, veri işlemeye yönelik süreçlerini alınabilecek en az veri ile en yüksek verimi elde edecek şekilde planlamalıdır. Gerçekten veri koruma hukukunun uygulanabilirliğinin temelinde, alınan verinin azaltılması vardır[165]. Bu uğurda veri sorumlusu, işleyeceği kişisel veriler üzerinde etkin ve verimli bir gereklilik denetimi yapmalıdır[166]. Bu denetimi yaparken gerekliliğin tespitinde salt kişisel verinin işlenme ihtiyacının değil ilgili kişinin menfaatlerinin de göz önünde bulundurulması gerekliliği, bu konunun hukuka ve dürüstlük kuralına uygun olma ilkesiyle bağlantısını ortaya çıkarmaktadır.

Veri sorumlusu, kişisel verilerin işlenmesi esnasında, ilgili kişiyi aydınlatmakla yükümlüdür[167]. Aydınlatma yükümlülüğünün doğuşu, kişisel verinin hukuka ve dürüstlük kuralına uygun işlenmesi ilkesinin bir sonucudur. Zira aydınlatma yükümlülüğü doğrudan dürüstlük ilkesinin somutlaştırma fonksiyonuna hizmet etmektedir. İlkenin GDPR metnindeki isminde yer alan "şeffaflığın" sağlanması, aydınlatma yükümlülüğünün yerine getirilmesiyle mümkün olmaktadır. Bu durum da aydınlatma yükümlülüğünün hukuka ve dürüstlük kuralına uygun veri işleme ilkesinden doğduğunu göstermektedir[168].

---

[164] Badur E./ Kurt Konca N. (2022). "Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini Ve Görevli Mahkeme", İnönü Üniversitesi Hukuk Fakültesi Dergisi, C.13, S.2, 476-490, s. 482, https://dergipark.org.tr/en/download/article-file/2585121, Erişim: 22.12.2022.

[165] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler. "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler", s. 3, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf, Erişim: 06.09.2021.

[166] Lambert, P.B. (2017). "The Data Protection Officer: Profession, Rules and Role", New York, CRC Press Taylor&Francis Group, s. 194.

[167] Uygun, s. 64; Küzeci, s. 217-218; Akgül, s. 163; Akdağ, s. 77.

[168] Benzer görüş için bkz. Dülger, Kişisel Verilerin Korunması Hukuku, s. 267.

Veri sorumlusunun hukuka ve dürüstlük kuralına uygun veri işleme ilkesine riayet etmiş sayılması için işlemiş olduğu kişisel verileri işleme amacına uygun şekilde kullanması, işlenme amacı dışında yahut ilgili kişilere zarar verecek şekilde kullanmaması, mevzuatta öngörülen yahut işlendikleri amaç gereği muhafaza edilmesi gereken sürelerle muhafaza edip sonrasında imha etmesi gerekir[169]. Bunlar veri sorumlusu için birer yükümlülük olmakla birlikte aynı zamanda hukuka ve dürüstlük kuralına uygun veri işleme ilkesinin dolaylı sonuçlarıdır.

Kişinin çipinde yüklü kişisel verileri için kişisel veri ve özel nitelikli kişisel veri aktarım farklılığının sağlıklı olabilmesi için RFID okuyucularının farklı özelliklere sahip olması gerekmektedir[170]. Örneğin bir kamu kurumu ile kimlik bilgileri paylaşılmak istendiğinde çipte yüklü sağlık verileri veya paylaşılmaması gereken diğer kişisel veriler kamu kurumu tarafından görülmemelidir. Ancak bir hastaneye gidildiğinde hastanedeki okuyucular sağlık verilerine erişebilmelidir. Bu ayrım belki de kişilerin iki farklı mikroçip taşıması ile çözülecektir. Sol eldeki mikroçipte kimlik, iletişim gibi kişisel veriler yer alırken, sağ eldeki çipte sağlık verilerine ilişkin kişisel veriler yer alabilecektir[171]. Böylelikle "Hukuka uygun olma ve dürüstlük ilkesi" gereğince kişisel verinin sahibinin çıkarlarının ve makul beklentilerinin dikkate alınması ve bu uğurda zarara uğratılmaması sağlanmış olacaktır.

3.5.2. Doğru ve Gerektiğinde Güncel Olma

KVKK m. 4/2-b ve GDPR m. 5/1-d maddelerinde, işlenen kişisel verilerin doğruluğu ve gerektiğinde güncel olması ilkesine yer verilmiştir. Bu ilke, veri sorumlusunun/kontrolörün, işlemiş olduğu verilerin doğruluğunu ve güncelliğini sağlama yükümlülüğünü doğurmaktadır.

Kişisel verinin, bir gerçek kişiye ait ve onu tanımlamaya yarayan bilgiler olarak kabul edilmesi halinde o verinin tanımlamış olduğu ya da ait olduğu kişi için doğru olması gerektiği şüphesizdir[172]. Doğru olmayan kişisel veriler, veri sorumlusunun bu

[169]Saka, R./Çağlayan, R./Koca, M. (2020). *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası*, Seçkin Yayıncılık, Ankara, s. 70.
[170] Pontius N. (2023). "What is RFID? Types of RFID Tracking Tags, Their Uses, Disadvantages and How They Compare to Barcode Labels", https://www.camcode.com/blog/what-is-rfid/, Erişim: 16.03.2023.
[171] Eltorai, A./ Fox, H./ McGurrin, E./ Guang, Erişim: 04.10.2022.
[172] Voigt/Bussche, s. 92.

ilke ile farklı yükümlülüklerini ihlal etmesine yahut farklı yaptırımlarla karşılaşmasına sebep olacaktır. Gerçekten bir kişiden alınan bilginin ona ait olmaması durumunda ilgili kişi, kişisel verisini paylaşarak elde etmek istediği menfaatten mahrum kalacaktır. Bu durumun varlığı doğrudan kişisel verinin doğru ve gerektiğinde güncel olma ilkesiyle bağdaşmamaktadır. Bunun yanı sıra bir kişiden alınan bilginin, o kişiye değil farklı bir kişiye ait kişisel veri olması durumunda riskin boyutu artmakta ve türü değişmektedir. Zira bu durumda işlenen kişisel verinin kullanılması, örneğin o vasıta ile ait olduğu sanılan kişi ile iletişime geçilmesi durumunda iki ayrı veri güvenliği ihlali meydana gelecektir. Bunlardan birincisi, işlenmiş olan kişisel verinin gerçek sahibinin kişisel verisinin hukuka aykırı olarak kullanılmış olması iken ikincisi ise bu vasıta ile yapılan bildirimlerde yer alan bilgilerin, varması gereken ve vardığı sanılan kişiye değil üçüncü bir kişiye ulaşacak olmasıdır. Bu da kişisel verinin hukuka aykırı olarak paylaşılması ve veri güvenliğinin ihlali anlamını taşıyacaktır. Bu sebeple veri sorumlusu için, işlemiş olduğu verinin doğruluğunu sağlamak büyük önem arz etmektedir[173].

Kişisel verinin toplandığı anda doğru olması ile güncel olması farklıdır. Zira kişisel verinin toplandığı anda doğru olması ve fakat sonradan değişebilmesi her zaman mümkündür. Bu durumda veri sorumlusunun bu tip değişiklikleri geciktirmeden uygulayarak verilerin güncelliğini sağlaması veya sağlamaya elverişli vasıtalar oluşturması gerekmektedir. Güncelliğin sağlanması için, güncelliği sarsılarak değişikliğe uğrama ihtimali bulunan verilerin, sistem ve süreç dahilinde yenilenmesi için gerekli alt yapıyı kurmak, bu ilke gereği, veri sorumlusunun yükümlülükleri arasındadır[174].

Doğru ve gerektiğinde güncel olma ilkesi tersten yorumlandığında veri sorumlusunun doğru veya güncel olmadığını bildiği kişisel verileri uhdesinde bulundurmama ve kullanmama yükümlülüğünü ortaya çıkarmaktadır. GDPR'da da veri işleme amacına aykırı yahut doğru olmayan verilerin gecikmeksizin silinmesi veya düzeltilmesi için gerekenin yapılması gerektiği hüküm altına almıştır[175].

[173] Yücedağ, s.51, Erişim: 12.05.2022.
[174] Kişisel Verileri Koruma Kurumu. (2018). "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf, s.13, Erişim: 05.06.2022.
[175] Dülger, Kişisel Verilerin Korunması Hukuku, s. 294.

Verinin işlenmesi aşamasında verinin doğruluğundan emin olmak veri sorumlusunun yükümlülüğüdür. Fakat kişisel verinin doğrudan ilgili kişiden alınması ya da bilgisi dahilinde üçüncü kişilerce paylaşılması durumunda ilgili kişi de paylaşmış olduğu kişisel verinin doğru ve güncel olmasını sağlamalıdır. İlgili kişi, kasten veya yanlışlıkla bu ödeve aykırı davranması durumunda, doğru olmayan bir bilgiyi veri sorumlusu ile paylaşmasından doğan zararlarını veri sorumlusundan talep edemeyecektir. Zira hukukun en temel ilkelerinden biri olduğu üzere; "Kimse dürüstlük kuralına aykırı olarak elde ettiği hakka dayanamaz" (Nemo auditur turpitudinem suam allegans)[176].

İlgili kişi, paylaşmış olduğu kişisel verinin doğru olmasını sağlamakla birlikte kişisel verilerindeki değişiklikleri de veri sorumlusuna iletmelidir. Bu ilgili kişi için KVKK m.11/1-d fıkrası ile tanınmış bir hak ve yapılması lazım gelen bir gereklilik olarak ortaya çıkarken veri sorumlusu için bu bildirimin yapılmasının vasıtalarını yani iletişim kanallarını ilgili kişilere sunmak ve bu tip bildirimleri uygulamak bir yükümlülüktür. Başka bir deyişle veri sorumlusu, ilgili kişilere, kişisel verilerinin değişmesi durumunda kendisine bildirmeleri için bir iletişim kanalı sunmak zorundadır[177]. KVKK m.11/1-d uyarınca ilgili kişilerce yapılan bu bildirimlerin de veri sorumlusunca ivedi olarak yerine getirilmesi gerekmektedir. Şunu da belirtmek gerekir ki, veri sorumlusunun değişikliğin kendisine bildirilmediği gerekçesiyle güncel olmayan kişisel veriyi kullanması hukuka aykırı olacaktır. Veri sorumlusu, kişisel veriyi kullandığı anda kişisel verinin doğru ve güncel olup olmadığını denetlemek zorundadır. Kurul; bir banka olan veri sorumlusunun, ilgili kişiye ait kredi kartını adres bilgisinin doğru ve güncel olmaması sebebiyle başkasına teslim etmesi durumunda, bankanın ilgili kişi tarafından değişikliğin kendisine bildirilmediği savunmasına karşılık, kuryenin kartın teslimi esnasında yeterli kontrolü yapmamasını veri sorumlusunun verinin doğru ve güncel olması için gereken tüm çabayı göstermemesi şeklinde yorumlamıştır[178].

[176] Prof. Dr. İlhan Helvacı Dersleri. Türk Medeni Kanunu. http://www.ilhanhelvacidersleri.com/turk-medeni-kanunu/turk-medeni-kanunu-madde-2, Erişim: 05.06.2022.
[177] Küzeci, s. 214.
[178]Kişisel Verileri Koruma Kurulu'nun 16.01.2020 tarih 2020/32 Karar numaralı kararı. https://www.kvkk.gov.tr/Icerik/6700/2020-32, Erişim: 15.10.2021.

Kişisel verilerin her durumda doğru ve güncel olması, aynı zamanda veri güvenliğinin sağlanmasının gereklilikleri arasındadır. Mikroçiplerde doğru veri barındırılması, kişiye ait bilgilerin doğruluğunu yine kişinin denetlemesi ile gerçekleşecektir. Bir internet veri tabanı üzerine kişi bilgilerini girecek ve daha sonra bu bilgiler mikroçipe yüklenecekse, kişi veri tabanına girdiği bilgilerin doğruluğundan kendisi sorumlu olacaktır[179]. Aynı zamanda mikroçip içerisindeki bilgilerin de güncel olması gerekmektedir.

Mikroçip veri tabanına ulaşım, kişinin sadece kendisi için tahsis edilmiş bir sistem olmalıdır. Mikroçiplerin herkes tarafından veri akışı için kullanıldığı bir senaryoda, bu veri akışının veri tabanına sahip olup bu hususta tasarruf yetkisi olan ya devlet ya da aracı nitelikte özel şirketler olacaktır. Bireyler ülkemizde olduğu gibi bir e-devlet alt yapısından bilgilerini çekebilecek ya da aracı nitelikte özel şirketlerle paylaştıkları verilerini çiplerine yükleyebileceklerdir. Veri akışının güvenliği ve kişisel veriler için doğruluğu ve güncelliği sağlamanın en iyi yolu, e-devlet gibi bir sistemle kişinin üzerindeki mikroçipin entegre çalışmasıdır. Bu şekilde entegre çalışan mikroçip geliştirilirse verilerin doğruluğu ve güncelliği devlet altyapısı tarafından desteklenecek ve bu hususta şüpheye yer olmayacaktır[180]. Şu anda da birçok resmi belge doğrulanabilir barkodlu bir şekilde e-devlet üzerinden temin edilmektedir. Bu barkodlu doğrulama sistemi çiplere de getirilebilir ve e-devlet üzerinden alınan bir evrak çipin okunması ile okuyucuya yansıtılacak şekilde tasarlanabilir. Örneğin işe girişte istenilen tüm evraklara işveren, işçinin mikroçipini okuyarak e-devlet sistemi üzerinden ulaşabilir. Bu uygulama, evrakta sahteciliğin önüne geçilmesine de fayda sağlayacaktır. Aynı zamanda böylelikle internet veri tabanı ile eşgüdümlü hareket eden mikroçip içeriği, en güncel verilere ulaşılmasına imkan tanıyacaktır. Bir başka örnek, kişinin boşanması ve medeni halinin değişmesi durumunda e-devlet üzerinden güncelleme yapılacağı için kimlik kartı değişikliği yapmasına gerek olmayacak ve soyadı, medeni hali çip üzerinden de değişecektir[181].

---

[179] Uncular, s. 63.

[180] Aşıkoğlu, İ.Ş. (2018*). Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri.* İstanbul Üniversitesi Hukuk Fakültesi Özel Hukuk Yüksek Lisans Tezleri Dizisi No:5, İstanbul, On İki Levha Yayıncılık, s. 166.

[181] European Union Agency for Fundamental Rights and Council of Europe. (2018). "Hanbook of European Data Protection Law", Luxembourg: Publications Office of the European Union. http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition, s. 128, Erişim: 22.12.2022.

3.5.3. Belirli, Açık ve Meşru Amaçlar İçin İşleme

Belirli, açık ve meşru amaçlar için işleme ilkesi, kişisel verinin işlenme amacı ve hukuki sebebiyle ve bu amaç ve hukuki sebebin ilgili kişiye bildirilmesiyle alakalıdır. Gerçekten veri sorumlusu, tüm kişisel veri işleme faaliyetlerinde, KVKK m. 5, 6, 7 ve 8. maddelerinde sayılan hukuki sebeplerden birine dayanmak ve bir işleme amacına sahip olmak zorundadır. Bu açıdan veri sorumlusu, veri işleme için var olan hukuki sebebi doğru şekilde tespit etmelidir. Bununla birlikte veri işleme amacını da belirlemelidir[182].

Veri işleme amacının sınırlı sayıda olması mümkün değildir. Birçok farklı amaçla kişisel verilerin işlenmesi söz konusu olabilecektir. Bu konuda önemli olan veri işlemenin belirli bir veri işleme amacına dayalı olması, bu amacın ilgili kişi açısından açık ve anlaşılabilir olması ve meşru olmasıdır. Tüm bunlar değinmekte olduğumuz belirli, açık ve meşru amaçlar için işleme ilkesini meydana getirmektedir[183].

Belirli amaçlar için işleme ilkesi, kişisel verinin işlenmesi esnasında işlemeyi gerektiren amacın ne olduğunun bilinmesini ifade etmektedir. Burada önemli olan her şeyden önce bir amaca sahip olmaktır. Bu amacın ne olabileceği hususunda herhangi bir sınır yoktur. Belirli amaçlar için işleme ilkesi, amaçsız olarak kişisel veri işlemenin önüne geçecektir. Buradan kasıt hiçbir amacın olmaması yanında sonsuz amaca hizmet eden bir veri işleme faaliyetinin de mümkün olmadığıdır. Gelecekte işe yarayabilecek olması, şimdilik bilinmese de gelecekte farklı amaçlar için kullanılabilme durumunun bulunması, bir zararı olmayacağından verinin himayede tutulması gibi sonsuz amaçlar veya veri sorumlusunun salt istekleri gibi amaçsız durumlar ile kişisel veri işlenmesi, belirli amaçlar için işleme ilkesiyle bağdaşmayacaktır[184]. Bunun yanı sıra belirli amaçlar için işleme ilkesine uygun davranılabilmesi için, veri işleme amacı ile işlenen kişisel verinin de birbirine uyumlu olması gerekmektedir[185].

---

[182] Akgül, s. 128.
[183] Yücedağ, s. 53.
[184] Privacy Internatiol. (2018). "The Keys to Data Protection:A Guide For Police Engament on Data Protection", United Kingdom, s. 27, https://privacyinternational.org/sites/default/files/2018-03/Data%20Protection%20COMPLETE.pdf, Erişim: 15.10.2021; Başalp, s. 37; Küzeci, s. 203.
[185] Dülger, Kişisel Verilerin Korunması Hukuku, s. 122.

Açık amaçlar için işleme ilkesi, kişisel verinin işlenme amacının ilgili kişilerce anlaşılabilir olmasını ifade etmektedir. Muğlak ya da çok ağır hukuk diliyle ifade edilen kişisel veri işleme amaçları, açık amaçlar için işleme ilkesiyle bağdaşmaz. Aydınlatma yükümlülüğü kapsamında veri sorumlusu, işlemiş olduğu kişisel verilerin işlenme amaçlarını ilgili kişilerle paylaşmak zorundadır. Bu da amacın açık olması ilkesi ile bağlantılı bir durum olarak ortaya çıkmaktadır[186].

Meşru amaçlar için işleme ilkesi, kişisel verilerin işlenme amacının hukuka uygun ve ilgilisini zarara uğratmayacak bir amaç olmasını ifade etmektedir. KVKK, kişisel verilerin işlenmesi için gerekli hukuki sebeplere ilişkin olarak sınırlı sayı ilkesini benimsemişken kişisel veri işleme amaçlarında tam aksine, örnek minvalinde dahi amaç yazmamayı tercih etmiştir. Kişisel verilerin işlenmesi amaçlarını sınırlamak mümkün değildir. Bu anlamda zikredilebilecek tek sınır, amacın meşru olması sınırıdır. Belirlenmiş açık amacın hukuka, hukukun temel ilkelerine aykırı olmaması ve ilgili kişinin çıkarlarıyla tamamen ters düşmemesi gerekmektedir. İşlenen kişisel verinin, veri sorumlusunun sunmuş olduğu hizmetle bağlantılı olması ve sunmuş olduğu hizmet için gerekli olması da meşru amaçlar için işleme ilkesinin gereklerindendir[187].

Her veri sorumlusu, hangi verileri hangi amaçlarla işlediği konusunda doğru tespiti yaptıktan sonra bu konuda ilgili kişiyi açık bir şekilde aydınlatmalıdır. İlgili kişi olarak anılacak kişi, kişisel verilerini vücudunun altındaki bir mikroçipte tutan kişiyi ifade ederken, veri sorumlusu ise çipteki kişisel verileri işleyecek okuyucuya sahip gerçek kişi veya tüzel kişidir[188].

Mikroçiplerle veri işlenirken oluşabilecek sorun çip sahibinin, karşı tarafın hangi verilerini okuyucu aracılığıyla alıp almadığı olabilir. Sadece kimlik bilgilerinin işlenmesinin yeterli olduğu bir işleme faaliyetinde, kimlik bilgilerinin yanı sıra iletişim bilgilerinin de işlenmesi mümkündür. Bu durum ilgili kişinin rızası hilafına gerçekleşebilir ve kişi bunun farkında olmayabilir. Bu ilke gereğince mikroçiplerden

[186] Yücedağ, s. 53.
[187] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler. "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler", s. 8, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf, Erişim: 10.10.2021.
[188] Işık, O. (2022). "Kişisel Verilerin Korunması Kanunu Kapsamında Veri Sorumlusu Olarak Sosyal Güvenlik Kurumu", Erciyes Üniversitesi Hukuk Fakültesi Dergisi, 17 (2) , 263-362, s. 275, https://dergipark.org.tr/tr/pub/eruhfd/issue/73314/1195339, Erişim: 26.03.2023.

alınacak veriler hangi amaç için işlenecekse o hususta çip sahibine aydınlatılma yapılması gerekmektedir. Kişiden habersiz mikroçipinden bilgisi dışında bir veriyi almak, veri sorumluları açısından sorumluluk doğuracaktır[189].

Her veri sorumlusu kendi faaliyetleri kapsamında işlediği amaçlar için kişisel verileri işleyebilecektir. Örneğin kişinin adına fatura kesilmesi için sadece adı, soyadı, kimlik numarası, adresi bilgilerinin işlenmesi gerekirken anne adı, baba adı gibi kişisel veriler de işlenirse meşru amaç kapsamında işlemenin dışına çıkılmış olacaktır[190].

3.5.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması

İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi, kişisel verilerin işlenmesi için gerekli hukuki sebeple ve kişisel veri işleme amaçlarıyla alakalı olan bir diğer ilkedir. Burada yine kişisel verinin işlenme amacının tespiti, bu amaç doğrultusunda kişisel verinin kullanımının sınırlanması ve bu amacın işlenen kişisel veriyle bağlantılı ve dengeli olması durumlarının incelenmesi gerekecektir.

İşlendikleri amaçla bağlantılı ve sınırlı olma ilkesi, kişisel veri işlerken sahip olunması gereken bir hukuki sebebin ve amacın mevcudiyetini gerekli kılar. Yalnızca soyut, genel, geleceğe yönelik, sınırı belirsiz amaçların bulunduğu koşullarda kişisel veri işlemenin mümkün olmaması, temelini bu ilkeden alır.

İşlenen veri, işleme amacı için gerekli olduğu ölçüde hukuka uygun kabul edilecektir. Bu doğrultuda işlendikleri amaçla bağlantılı ve sınırlı olma ilkesi; kişisel verilerin yalnızca gerektiği kadar işlenmesini, gerekmeyen verilerin arındırılmasını; yani veri minimizasyonunu[191] veya veri asgarileştirmesini[192] karşımıza çıkarmaktadır.

İşlendikleri amaçla bağlantılı ve sınırlı olma ilkesi, kişisel verinin işlendiği amaç için gerekli olması yanında işlendiği amaç uğruna kullanılabilmesini ifade etmektedir. Buradan hareketle öncelikle kişisel verinin yeterli, ilgili ve işlenme amacına göre gerekli olanlarla sınırlı olması, bu ilkenin yarattığı bir durumdur. Ardından ise bu

---

[189] Küzeci, s. 220.
[190] Korkmaz, İ. (2016). "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", Türkiye Barolar Birliği Dergisi (124), s. 96, http://tbbdergisi.barobirlik.org.tr/m2016-124-1571, Erişim: 12.05.2023.
[191] Carey, P. (2018). Data Protection Principles, "Data Protection:A Practical Guide to UK and EU Law", 5. Bası, Oxford, Oxford University Press, s. 35; Voigt/Bussche, s. 90.
[192] Dülger, Kişisel Verilerin Korunması Hukuku, s. 282; Kuner, C. (2007). "Europen Data Protection Law: Corporate Compliance and Regulation, Second Edition", Oxford, Oxford University Press, kn.2.30.

işleme amacı, artık veri sorumlusu için bağlayıcı bir amaç halini alacaktır. Böylece bir kişisel veri, veri sorumlusunca hangi amaçla işlenmiş ise o amaç için kullanılabilecektir. Bu amacı aşan kullanımlar için ayrıca hukuki sebep tespit edilmesi ve bu doğrultuda gerekli aydınlatmanın da yeniden yapılması gerekecektir[193].

Kişisel verilerin korunması hukukunda "ne kadar az veri o kadar az sorumluluk" düşüncesi hakimdir. Bu ilkeye göre işlenen bir kişisel veri, işleme amacının dışına çıkıyorsa veya işleme amacının sınırlarını aşıyorsa işlenmemelidir. Geleceğe yönelik ihtimallere binaen bireylerin kişisel verileri işlenmemelidir. Kişisel veriler, her halükarda alınıp ihtiyaç olduğunda kullanılabilecek veriler değildir. Muhtemel ihtiyaçlara yönelik veri işlemesi yapılmamalı, veriyi işleme amacı için gerekli olmayan veri işlemeden kaçınılmalıdır[194].

Mikroçiplerle kişisel veri işlenirken de amaçla bağlantılı olma ve amaçla sınırlı olma unsuruna dikkat edilmelidir. Mikroçiplerle veri işlemede amaçla bağlantılı olma ilkesine uygunluk çip okuyucularının denetimi ile gerçekleşecektir. Okuyucu mikroçipten gereğinden fazla veri almamalı, aldığı verileri ise amacına uygun olarak işlemelidir. Okuyucuların denetimini okuyucuların sahibi olan gerçek veya tüzel kişi veri sorumlusu gerçekleştirmelidir. Kurum tarafından bir şikayet üzerine veya resen yapılan denetimde de Kurum okuyucuları denetlemelidir[195].

Okuyucuların aldığı ve daha sonra veri sorumlusunun işlediği kişisel verilerin veri sorumlularının aldığı amaca yönelik kullanılmaması, hukuka aykırı bir işlem olacak ve veri ihlalini doğuracaktır. Böyle bir durumun veri sorumlusunun bilgisi dışında gerçekleşmesi durumunda veri sorumlusu, veri sahibi ilgili kişiye bu konuda bilgi vermeli ve Kurum'a da veri ihlali başvurusu yapılmalıdır. Ancak amaçla bağlantılı olarak işlenmeyen verilerin tespiti oldukça zordur. Veri sorumlusu ilgili kişinin verilerini hangi amaçla işlediğine aydınlatma metninde yer vermek zorundadır. Amaçla bağlantılı olmadığının tespiti, aydınlatma metni incelenerek ve çip okuyucuları denetlenerek sağlanmalıdır[196].

---

[193] Kuner, s. 62; Korkmaz (Kişisel Verilerin Korunması), s. 99; Şimşek, s. 44.
[194] Akgül, s.158; Kuşkonmaz E. M. (2013). *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması,* Yüksek Lisans Tezi, İstanbul, s. 93.
[195] Saygı, S. (2020). "6698 Sayılı Kanun'un Sistematiğinde Yargısal Başvuru Yolları", Kişisel Verileri Koruma Dergisi, C.2, S.2, s.44, https://dergipark.org.tr/tr/download/article-file/1106037, Erişim: 25.04.2023.
[196] Ömür, s.136.

Uygulamada veri sorumlularının bu ilkeye aykırı davranması, genelde veri ticareti olarak ortaya çıkmaktadır. Kişiye hizmet sağlamak amacıyla alınan kişisel veriler, kişinin rızası olmadan reklam ve pazarlama şirketlerine satılmaktadır. Örneğin ilgili kişinin telefon numarasını paylaşmadığına emin olduğu bir işletmeden mesaj gelmesi, telefon numarasının rızası dışında o işletmenin eline geçtiğini gösterir ve buradan da rıza kapsamında verilen bir verinin amaçla bağlantılı olmadan işlendiğini anlaşılmaktadır[197].

Kişisel verilerin, işlenme amacıyla ölçülü olarak işlenmesi ilkesi kişisel verilerin korunması alanının getirdiği en temel ölçütlerden biridir. Bu ilkeye göre veri sorumlusu tarafından işlenen kişisel verinin önemi ile işlenme amacının vadettiği önem arasında bir kıyas yapılmalı ve işlenen kişisel veri, nitelik itibarıyla, işleme amacına nazaran çok daha önemli olarak belirlenmemelidir. Bugüne kadar kişisel verilerin işlenmesi ve aktarımı farklı yöntemlerle yapılmıştır. En basit haliyle dil ile, diğer karmaşık hallerde ise kullandığımız cihazlarla kişisel veri paylaşımı yapılabilmektedir. Kişisel verileri işlerken ve paylaşırken dikkat edilmesi gereken kişisel verinin işlendiği veya paylaşıldığı amaçla kullanımının ölçülülüğüdür. Özetle kişisel veri işleme faaliyeti yapılırken işlenme amacıyla ölçülü olarak hareket edilmeli ve bu ikisi arasında makul bir denge kurulmalıdır[198].

Ölçülülük ilkesindeki ölçünün ne şekilde tespit edileceği hususunda mevzuatta katı bir düzenleme bulunmamaktadır. Ölçülülük, somut durumun özelliklerine göre Kurul tarafından yayınlanan rehber ve ilke kararlar ile Kurul kararları veya doktrin görüşleriyle şekillenebilecek bir olgudur. Bilhassa özel nitelikli kişisel verilerin işlenmesinde ölçülülük üzerine Kurul tarafından verilen bazı kararlar yol gösterici niteliktedir[199]. Ölçülülüğün şekillenmesiyle kişisel verilerin korunması alanının ülkemizde gelişme göstermesi söz konusu olacaktır. Mikroçiplerle işlenen kişisel

---

[197] Kaya, M. (2015). Elektronik Ortamda (Elektronik Haberleşme-İnternet-Sosyal Medya) Kişilik Hakkının Korunması, Ankara, Seçkin Yayıncılık, s. 139.

[198] Bayındır, s. 82.; Develioğlu, s. 47.

[199] Bkz. "Bir havayolu taşımacılık şirketinin (veri sorumlusu), sunduğu sadakat programını kullanan ilgili kişinin kullanıcı adı ve parola bilgilerini değiştirme talebi karşısında ilgili kişiden arkalı önlü kimlik görüntüsü talep eden veri sorumlusu" hakkında Kişisel Verileri Koruma Kurulu'nun 01.10.2019 tarihli ve 2019/294 sayılı Kararı. https://www.kvkk.gov.tr/Icerik/6556/2019-294, Erişim: 20.11.2021; Bkz. "Belediyede memur olarak görev yapan ilgili kişinin, veri sorumlusu bünyesinde işe giriş çıkış takibinin biyometrik veri işlenerek yapılması" hakkında Kişisel Verileri Koruma Kurulu'nun 01.12.2020 tarihli ve 2020/915 sayılı Kararı. https://www.kvkk.gov.tr/Icerik/6872/2020-915, Erişim: 20.11.2021.

veriler üzerinde de temel ilkeler bağlamında yapılacak olan değerlendirmede, en temel kriterlerden biri kuşkusuz ölçülülük ilkesi olacaktır.

Ölçülülük kapsamında veri sorumlusu, amacı çerçevesinde ölçülülük ilkesine uygun olarak ilgili kişiden minimum düzeyde veri talep etmeli ve kişinin rızası olsa bile aşırı miktarda veri işlememeli veya paylaşmamalıdır[200].

6698 sayılı Kanun'da yer alan ölçülülük ilkesi, GVKT'deki veri minimizasyonu ilkesine karşılık gelmektedir. GVKT'de veri minimizasyonu, Tüzüğün 5. 75addesinin (1)/c bendinde *"işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlıdır"* şeklinde tanımlanmıştır. Bu ilkeye göre veri sorumlusu, amaçlarına ulaşmak için gereğinden fazla veri işleme faaliyetinden kaçınmalı ve işleyeceği kişisel verinin işlenmesinin, amacına ulaşmak için şart olup olmadığını araştırmalıdır[201]. Ölçülülük ilkesinde veri işleme faaliyeti ile veri işleme amacı arasında bir denge olmalıdır.

Kişisel Verileri Koruma Kurulu'nun 27.02.2020 tarihli ve 2020/167 sayılı kararı[202], ölçülülüğe aykırı faaliyetten dolayı verilmiş bir karardır. Kurul bu kararında müşterilerinin giriş ve çıkış takiplerini biyometrik veri olan parmak izi ve avuç içi izi alımı ile yapan bir spor salonunun; ilgili kişinin biyometrik verilerinin işlenmesini ölçülülük ilkesi ışığında, minimum düzeyde veri talep etme ilkesine aykırı bulmuş ve idari para cezası uygulamıştır[203].

Kurul 01.12.2020 tarihli ve 2020/915 sayılı kararında[204] da benzer bir hüküm vermiştir. Bu kararda; bir ilçe belediyesinin personel giriş ve çıkış takipleri için personelin parmak izini aldığı, personelin işten ayrıldıktan sonra parmak izinin silinmesini talep ettiği ancak belediyeden olumsuz dönüş alması nedeniyle Kurum'a yaptığı başvuru incelenmiştir. Kurul, burada da parmak izi verisinin işlenmesini yani bir özel nitelikli kişisel veri türü olan biyometrik veri işlenmesini personelin giriş ve

---

[200] Şimşek, s.99.
[201] Erdinç, G.H. (2020). "Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi", Kişisel Verileri Koruma Dergisi, Cilt: 2, Sayı:1 s.13.
[202] KVKK. "Kurul Kararları", 27.02.2020 tarihli ve 2020/167 sayılı karar, https://kvkk.gov.tr/Icerik/6738/2020-167, Erişim: 11.11.2021.
[203] Dede, R. (2022). Kişisel Verilerin Korunması Kanunu Bakımından Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati, Altınbaş Üniversitesi Lisansüstü Eğitim Enstitüsü Kamu Hukuku Yüksek Lisans Tezi, s. 51.
[204] KVKK. "Kurul Kararları", 01.12.2020 tarihli ve 2020/915 sayılı kararı, https://kvkk.gov.tr/Icerik/6872/2020-915, Erişim: 11.11.2021.

çıkış takibini yapmak amacıyla kullanılmasını ölçülülüğe aykırı bulmuş ve yaptırım uygulamıştır[205].

Ölçülülük ilkesi kanaatimizce kişisel veriler işlenirken Kanun'un en dikkat edilmesi gereken ilkelerindendir. Daha önceki başlıklarda değinildiği gibi dünyanın çeşitli ülkelerinde personelin giriş ve çıkış takibi, personelin deri altı mikroçipleri ile sağlanmaktadır. Mikroçiplerle personel giriş ve çıkış takibi yapmanın, ölçülülük ilkesi açısından değerlendirilmesi gerekmektedir[206].

Parmak izi verisinin kullanımıyla mikroçip kullanımı kıyaslanacak olursa parmak izi verisi, özel nitelikli kişisel verilerden olup her birey için ayırt edici nitelikte olduğundan, hassas şekilde koruma gerektirmektedir. Mikroçiplerde ise bu ortaya ID numarası olarak çıkacaktır. Her mikroçipin kendine has 14-15-16 karakterli kodu da parmak izi gibi bireylere ait ayırt edici bir unsur olacaktır. Ancak mikroçip ID numarası kimlik verisi gibi bir veri tipi olduğu için hassas veri olarak nitelendirilemeyeceğinden, bu verinin veri sorumlusu tarafından işlenmesi kanaatimizce ölçülülük ilkesine aykırılık teşkil etmeyecektir. Üstelik giriş ve çıkışta mikroçipin okunması ile alınan veriler kişinin adı, soyadı gibi kimlik verisi olacak, özel nitelikli kişisel verisi olmayacaktır[207].

Uygulamada işverenlerin büyük çoğunluğu personel giriş ve çıkış takiplerini parmak izi verisi alarak yapmakta ve bu uygulamayı daha verimli görmektedir. Bunun sebebi parmak izini kullanan personelin giriş ve çıkışlarda işvereni aldatamayacağıdır. Çünkü parmak izi kullanabilmek için mutlaka tam zamanında kendisinin işe hazır olması gerekmektedir. Oysa kart sistemi veya şifre sistemi gibi takip sistemlerinde personelin yerine bir başka personel, personeli giriş veya çıkış yapmış gibi gösterebilmektedir. Mikroçiple giriş ve çıkış yapılması durumunda her kişinin kendi deri altı mikroçipi olacağı için personeller birbirlerini giriş veya çıkış yapmış gibi gösteremeyeceklerdir[208].

Mikroçiple giriş ve çıkış takibi yapılmasıyla işverenler parmak izi verisini işlemeye gerek duymayacak ve ölçülülük ilkesi ihlal edilmeyecektir. Aynı zamanda

[205] Saygı, s.51.
[206] Yücedağ, s.59.
[207] Küzeci, s. 281; Işık, s. 311.
[208] Manav, s. 111; Sevimli, A. (2006). *İşçinin Özel Yaşamına Müdahalenin Sınırları,* İstanbul, s. 113.

mikroçiple giriş ve çıkış sistemi kartlı sistem gibi kolayca suiistimal edilebilir bir sistem olmayacaktır. Hem işverenler için önem arz eden personelin verimliliği zedelenmeyecek hem de personelin biyometrik verileri alınmayarak ölçülülük ilkesine aykırılık teşkil edecek bir durum oluşmayacaktır[209].

3.5.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme

Veri koruma hukuku ile ülkemiz hukukunda ve kuruluşların işleyişinde "imha" kavramı önem kazanmıştır. Kişisel verilerin imhası, ülkemizde, 28.10.2017 tarih 30224 sayılı Resmi Gazete'de yayınlanan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"te tanımlanmıştır. Bu tanıma göre kişisel verilerin imhası, *"Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi"* anlamını taşımaktadır. Bu tanımda yer alan silme, yok etme ve anonim hale getirme kavramlarının üzerinde durulmalıdır. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'te silme: *"Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi"*; yok etme, *"kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi"*; anonim hale getirme, *"kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi"* olarak tanımlanmıştır. Kişisel verinin imhası denildiğinde bu uygulamalardan herhangi birinin yapılmasını anlamak gerekmektedir[210].

Mevzuatın bu düzenlemesiyle artık veri sorumlusu ya da veri işleyenler tarafından işlenen kişisel verilerin, belli sürelerin dolmasıyla imha edilmesi bir zorunluluk halini almıştır. Öyle ki, anılan sürelerin dolmasıyla kişisel verinin işlenmesindeki hukuki sebep son bulacak ve artık o verinin işlenmeye devam edilmesi yahut himayede tutulması hukuka aykırı hale gelecektir[211]. Bu doğrultuda kişisel

[209] Süzek, S. (2018). *İş Hukuku,* İstanbul, s. 400.
[210] Erarslan, s. 117; Demirezen, 59.
[211] Kaya/Taştan, s. 49.

verinin ileride tekrar gerek duyulabileceği ihtimaline yahut farklı gerekçelere binaen saklanması doğru olmayacaktır[212].

Bu ilke doğrultusunda kişisel veriler, veri sorumlusu yahut veri işleyenler tarafından, tabi olduğu mevzuat gereği saklanması gereken süre kadar; mevzuatta böyle bir süre belirtilmemişse işleme amacıyla bağlantılı olan süre kadar saklanmak ve ardından imha edilmek zorundadır[213]. Kişisel verilerin veri sorumluları veya veri işleyen uhdesinde belirli sürelerle saklanması, çoğunlukla farklı yasalar kapsamında bir yükümlülük olarak ortaya çıkmaktadır. Kişisel verilerin korunması alanında bu saklama sürelerinin sona ermesiyle birlikte kişisel verilerin imha edilmesi de bir yükümlülük halini almıştır[214].

Veri sorumlusunun, kişisel verileri himayesinde barındırırken, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik seviyesini oluşturmak için gerekli her türlü idari ve teknik tedbirleri alması gerekmektedir. Veri sorumlusu kişisel verileri mevzuatta öngörülen süre kadar tutmalı, öngörülen bir süre yok ise işleme amacı için gerekli olan süre kadar saklamalıdır. Kişisel veriler, işleme amacının gerektirdiğinden daha uzun süre tutulmamalı, saklama süresi dolan kişisel veriler imha edilmelidir[215].

Bir deri altı mikroçipin ömrü ortalama 10 yıldır. 10 yıl sonra mevcut mikroçip çıkartılarak bilgiler yeni mikroçipe aktarılır ve yeni mikroçip tekrar deri altına enjekte edilerek çip kullanımına devam edilebilmektedir. Bu 10 yıllık süreç boyunca ilk takılmış olan mikroçipten verilere ulaşılabilecektir. Kişinin mikroçipinin bağlı olduğu internet veri tabanındaki bilgileri, veri tabanının devlet altyapısı olması durumunda süresiz, aracı nitelikte özel bir kuruluşun altyapısı olması durumunda ise kuruluşun kişisel verileri saklama ve imha politikasına göre belirlenecektir. Aracı nitelikte özel kuruluş, bireylerin kişisel verilerini ne kadar süre ile saklayıp ne şekilde imha ettiğini saklama ve imha politikası ile mikroçip ve kişisel veri sahibi ilgili kişiye aktaracaktır[216].

---

[212] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler", s. 13,https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf, Erişim: 06.11.2021.
[213] Küzeci, s.215; Yücedağ, s. 60.
[214] Saka, R./Çağlayan, R./Koca, M., s. 38.
[215] Mikroçiplerle işlenen kişisel verilere ilişkin imhanın nasıl yapılacağına yukarıdaki başlıkta değinmiştik. Bkz.: I. Bölüm 4.3. numaralı başlık.
[216] Manav, s. 333; Orak, s. 65; Küzeci, s. 388; 100 Soruda Kişisel Verilerin Korunması Kanunu, s.40.

Mikroçip içerisindeki kişisel veriler, işlendikleri amaç için gerekli olan süre kadar saklandıklarında kişinin ölümüne kadar saklanmış olacaklardır. Kişi öldükten sonra o mikroçiple veri işleme faaliyetine son verilmeli ve mikroçip imha edilmelidir. Aksi takdirde kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesine aykırılık oluşacaktır[217].

Ölen kişilerin kişisel verileriyle ilgili kurul 18/09/2019 tarihli ve 2019/273 sayılı kararıyla ölen kişinin yakınlarının bu veriler üzerinde bir talebi olamayacağını açıklığa kavuşturmuştur[218]. Bu nedenle günümüzde ölen kişinin kişisel verileriyle ilgili bir imha prosedürü mevcut değilken mikroçipler ile bu sağlanabilecektir

[217] Uçak, M. (2021). "Kişisel Verilerin Ölümden Sonra Korunması", İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi, C. VI, S. 10, s. 97-123, s. 119.
[218]KVKK. "Kurul Kararları", 18/09/2019 tarihli ve 2019/273 sayılı kararı. https://www.kvkk.gov.tr/Icerik/6710/2019-273, Erişim: 05.06.2022.

4. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNDA UYGULAMA SORUNLARI VE MİKROÇİPLERİN KULLANIMINDA KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN YAŞANABİLECEK SORUNLAR

4.1. Kişisel Verilerin Korunması Hukukunda Uygulama Sorunları

Kişisel verilerin korunması hukukunun mikroçipler açısından uygulanmasının gerek özel hukuk gerçek ve tüzel kişilerinin gerekse kamu kurumları ile kamu kurumu niteliğindeki kuruluşların işleyişinde ciddi değişikliklere yol açması kaçınılmazdır. Veri sorumlusu veya veri işleyen sıfatını haiz gerçek ya da tüzel kişiler, kişisel verilerin korunması hukukunun getirdiği yükümlülüklere ve yeniliklere uyum sağlayabilmek için gerek bilişim altyapısı ve teknik konularda gerekse hukuki alt yapı ve idari konularda bir dizi yenilik veya değişiklik yapmak durumundadır[219]. Zira emredici normlar ihtiva eden kişisel verilerin korunması hukukunun gereklerine riayet etmeyen bu kişilerin karşılaşabileceği ağır yaptırımlar ve buna karşılık veri sahibi kişi gruplarının da ciddi mağduriyeti söz konusu olabilecektir[220].

Her yenilik şüphesiz bir değişimi gerektirecektir. Bu değişimler de her zaman kolaylıkla gerçekleşebilir değildir. Öyle ki bazı değişimlerin tam manasıyla uygulanmasında alt yapı eksiklikleri sebebiyle ciddi bir zaman gerekebilecek iken bazı değişimlerin uygulanması ise mevcut altyapı itibariyle imkansız yahut aşırı derecede güç bir hal alacaktır. Tüm bunların çaresi şüphesiz mevzuatın uygulanmasının alt yapı eksiklerinin giderilmesiyle eş güdümlü olarak kısım kısım gerçekleşmesi, bu konuda yerel otoritelerin hummalı ve istikrarlı bir çalışma yürüterek değişimde kilit rol oynamasıdır. Aksi halde değişimi icap eden yükümlülük sahiplerinin yerel otoriteler tarafından yalnız başına bırakılması, bu konuda gerek mevzuat gerekse alt yapı eksikliğinin ülke çapında ciddi anlamda hissedilmesi gibi durumlar, kişisel verilerin korunması hukukunun hem uygulanmasında hem de gelişim göstermesinde ciddi engel teşkil edecektir[221].

Bu başlık altında kişisel verilerin korunması hukukunun ülkemizde karşılaştığı ve karşılaşması muhtemel uygulama sorunları, alt yapı eksikliği ve yerel otoritelerin

[219] Korkmaz, (Kişisel Verilerin Korunması) s. 134; Kuşkonmaz, s. 116; Küzeci, s. 245.
[220] Badur/Konca, s. 482.
[221] Korkmaz, (Kişisel Verilerin Korunması) s. 83.

hatalı uygulamaları değerlendirilecek ve mikroçiplerle kişisel veri işlenmesi perspektifinden anlatılmaya gayret edilecektir.

Ülkemizin kişisel verilerin korunması hukuku ile tanışma sürecinin, uygulayıcı ve yükümlülük sahibi kişi grupları açısından, ani ve henüz alt yapısı hazırlanmadan gerçekleşmesi; uygulanmasını zorlaştırmış ve beklenen gelişimin sağlanmasının önünde engel teşkil etmiştir. Bunun yanı sıra kişisel verilerin korunması hukukunun ülkemizdeki denetçisi ve yegane uygulayıcısı konumunda olan yerel otorite Kişisel Verileri Koruma Kurumu'nun, bu hukukun uygulanmasında yer yer eksik, yer yer ise hatalı uygulamalara yol açması ve bu alanın aydınlatılması için gerekli ve verimli çalışmayı yapmamış olması, bu hukukun gelişiminde büyük engellerden bir diğeridir[222].

4.1.1. Alt Yapı Eksikliği

Kişisel verilerin korunması hukukunun ülkemizde uygulanmasını zorlaştıran sebeplerin başında alt yapı eksikliği gelmektedir. Öncelikle kişisel verilerin korunması hukuku ile yükümlülük altına giren kişi gruplarının tabi olduğu mevzuatın, kişisel verilerin korunması hukuku için gerekli düzenlemeleri içermemesi, bazı yönleriyle bu hukukun uygulamasını zorlaştırması, belirsiz ve soyut hale getirmesi ve hatta çelişkilere yol açması gibi sebepler hukuki alt yapı eksikliğinin mevcut olduğunu göstermektedir. Çalışmamızın önceki kısımlarında ifade edildiği üzere kişisel verilerin korunması hukukunun teknik alanla ilişkisi yadsınamayacak kadar geniştir. Hal böyle olunca yükümlü kişi gruplarının ciddi teknik donanıma sahip olması zorunludur. Fakat bu teknik donanım için öncelikle sağlıklı ve sağlam bir teknik alt yapının gerek ülke çapında gerekse yükümlü kişi grupları özelinde bu mevzuat çalışmaları yapılmadan önce gerçekleştirilmesi gerekmekte idi. Böyle bir alt yapı çalışmasının yapılmamış olması, kişi gruplarının yükümlülüklerini yerine getirmesi önünde ciddi bir engel olan teknik altyapı eksikliğini göstermektedir. Hukuki ve teknik altyapı eksiklikleri yanında, yükümlü kişi grupları, bu kişi gruplarının personeli ve devlet otoritelerinde gerekli kurumsal bilincin ve eğitim düzeyinin yetersiz olması, kişisel verilerin getirdiği

[222] Dülger. M.V. (2016). "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, C. 3, S. 2, 101-167, s. 115.

yeniliklerin anlaşılmasını ciddi anlamda zorlaştırmış ve böylelikle uygulanması önünde de ciddi bir engel teşkil etmiştir[223].

4.1.1.1. Hukuki altyapı eksikliği

Türk Hukukunda, neredeyse tüm hukuk alanlarının gelişimi sürecinde, ihdas edilen mevzuatın öncesinde tabi olunan diğer mevzuatta gerekli değişikliklerin yapılması, ihdas edilecek olan mevzuata yönelik diğer mevzuatın öncelikle hazırlanması gibi çalışmaların eksik yapılması, sürekli karşılaşılan bir sorun halini almıştır. Çoğunlukla ihdas edilen mevzuatın, evvelki mevzuatla eş güdümlü yürütülebilmesi adına, mevzuatın ihdasından sonra uygulanması sürecinde vaziyetin farkına varılarak süreç içinde kısım kısım değişiklikler yapılması kaçınılmaz olmakta ve bu durum da mevzuatın yükümlü kıldığı kişi gruplarını zor duruma sokmaktadır. Kişisel verilerin korunması hukuku açısından da aynı durumla karşı karşıya kalındığı yadsınamaz bir gerçektir. Kişisel verilerin korunması hukukunun yükümlü kıldığı kişi gruplarının tabi olduğu mevzuatın, bu hukukun doğuşundan önce, bu hukuka hizmet edecek gerekli düzenlemelerinin yapılmamış olması, uygulamada belirsizliklere ve çelişkilere yol açmıştır[224]. Kişisel verilerin korunması hukukundaki hukuki alt yapı eksikliği özellikle; kişisel verilerin saklama sürelerinin tespitinde yükümlü kişi gruplarının tabi olduğu mevzuatın düzenleme içermemesi, açık rıza hukuki sebebinin uygulamasının sözleşmeler hukukunun temel prensipleri ile çelişmesi, sağlık verilerinin işlenmesinde Kanunda belirlenen hukuki sebepler ile bazı mevzuatın emirlerinin uyumlu olmaması durumlarında kendisini ciddi şekilde göstermektedir. Çalışmamızın konusu olan mikroçiplerle kişisel verilerin işlenmesi durumunun gerçekleşmesi halinde ise buna uygun hukuki düzenlemelerin yapılması gerekecektir.

Kişisel verilerin, veri sorumlusu ve veri işleyenler himayesinde belirli sürelerle saklanıp akabinde imha edilmesinin bir gereklilik ve yükümlülük olduğu çalışmamızın birçok kısmında ifade edilmiştir. Bu ifadelerde, veri sorumlusu ve veri işleyenlerin, himayelerindeki kişisel verileri, kanunlarda öngörülen sürelerle yahut böyle bir süre yok ise işlendikleri amaç için gerekli olan süre kadar muhafaza edip akabinde imha

[223] Yürük, Z. (2023). Kişisel Verilerin İhlalinden Doğan Özel Hukuk Sorumluluğu, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı Tezli Yüksek Lisans, s. 141-142.
[224] Dülger, Kişisel Verilerin Korunması Hukuku, s. 114.

edilmesi gerekmektedir[225]. Burada öncelikle ifade etmek gerekir ki "işlendikleri amaç için gerekli olan süre" kavramı, son derece soyut ve belirsiz olup uygulamada farklı yorumlarla farklı yönde faaliyetlerin doğmasına sebep olacaktır. Oysa kişisel verilerin korunması hukuku ile amaçlananın bu olmadığı kabul edilmelidir. Nitekim Türk veri koruma otoritesi olan Kişisel Verileri Koruma Kurumu ve bu otorite içerisindeki karar mekanizması olan Kişisel Verileri Koruma Kurulu'nun "işlendikleri amaç için gerekli olan süre"yi nasıl ve neye göre belirleyeceği hususunda netlik bulunmamaktadır. Gerçekten bir veri sorumlusunca, mevzuatta saklama süresi belirtilmemiş bir kişisel verinin uzun bir süre saklanması, Kurul'un ise bu veriyi daha kısa süre saklamanın makul olacağı yönünde bir kanaatte bulunması durumunda ihlal doğacak ve bu ihlalde veri sorumlusunun yorum niteliğindeki bu tutumu ile bir kusuru bulunmayacaktır. Hal böyle olunca kişisel verilerin korunması hukuku açısından ciddi bir sorun ortaya çıkacaktır. Bu sebeple uygulamada "işlendikleri amaç için gerekli olan süre" olgusuna dayanmaktan mümkün mertebe uzaklaşılmasının daha sıhhatli olacağı kanaatindeyiz. Bu durum mikroçiplerin kullanıma başlamasıyla daha da zorlaşacaktır. Çözümün sağlanabilmesi için ise hukuk alanlarındaki temel mevzuat yahut ikincil mevzuatın bilgi, belge ve verilerin saklanması hususunu ihtiva etmesi gerekmektedir.

Kişisel verilerin korunması hukukunun ülkemizde uygulanmasından sonra ihdas olan mevzuatta çoğunlukla bu tip netlik kazanmamış hükümlere rastlanmaktadır. Hal böyle olunca veri sorumluları tarafından kişisel verilerin saklanma süresinin tespiti ciddi zorluk arz etmektedir. Kamu kurumu olan veri sorumlularında bu sorunun görece daha az hissedildiği söylenebilir. Nitekim 18.10.2019 tarih 30922 sayılı Resmi Gazete'de yayımlanan *"Devlet Arşiv Hizmetleri Hakkında Yönetmelik*"te birçok bilgi ve belgenin saklanma süresinin tespit edilmiş olması bu sorunu tümüyle ortadan kaldırmamış olsa da asgari düzeye indirmektedir[226]. Aynı şekilde odalar ve borsalar için Ticaret ve Sanayi Odaları, Ticaret Odaları, Sanayi Odaları, Deniz Ticaret Odaları, Ticaret Borsaları ve Türkiye Odalar ve Borsalar Birliğinde *"Muhafazasına Lüzum Kalmayan Evrak ve Vesaikin İmhası Hakkında Yönetmelik"* ile bu sorun ciddi anlamda çözüme kavuşmaktadır. Fakat bu iki düzenlemede dikkati çeken şey saklama sürelerinin birçok bilgi ve belge için süresiz olarak belirlenmiş olmasıdır. Elbette bu

[225] Yücedağ, s. 60.

[226] KVKK. Kurul Kararları. 28.06.2018 Tarihli ve 2018/69 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/5366/2018-69, Erişim: 12.02.2023.

durum bir Devlet hafızası ve Devlet kimliği oluşması maksadıyla doğmuştur. Fakat kişisel verilerin korunması karşısında anılan maksatların ciddi bir kıyas ile her bilgi, belge ve kişisel veri için ayrı ayrı ve ihtimamla yapılması şarttır. Anılan kişi grupları haricindeki veri sorumluları için ise, saklama sürelerinin tespiti için tüm alan ve faaliyetlere ilişkin mevzuatı taraması, bir hüküm varsa uygulaması, yok ise işleme amacı için gerekli süreyi belirlemesi gerekmektedir. En başta bunca mevzuatın taranıp tüm faaliyet ve süreçler için gerekli saklama sürelerinin tespit edilmesinin ne kadar zor olacağı ortadadır. Kişisel verilerin imhasını da bir yükümlülük olarak tanımlayan kişisel verilerin korunması hukukunun, saklama süreleri hususunda daha belirli, daha kolay erişilebilir bilgiye sahip bir sistem kurgulaması ve bu uğurda gerek yeni bir mevzuat çalışması gerekse eski mevzuatta uyarlama yapması gerektiği kanaatindeyiz. Saklama sürelerinin tespiti hususunun imha yükümlülüğü için vazgeçilmez nitelikte olması, imha yükümlülüğünün ise kişisel verilerin korunması hukukunun yapı taşlarından olması sebebiyle bu hukuki alt yapı eksikliğinin mutlaka giderilmesi gerekmektedir.

Kişisel verilerin korunması hukukunun hukuki altyapı eksikliklerinden birisi kişisel verilerin işlenmesinde ve aktarımında hukuki sebeplerden biri olan "açık rıza" konusundadır. Açık rıza ile ilgili çalışmamızda yapılan açıklamalarda, Kanun ve ilgili mevzuat ile Kurul kararlarına uygun bir açık rızadan bahsedilebilmesi için hem faaliyet hem de kişisel veri türleri bazında ayrı ayrı açık rıza alınması gerektiğinden bahsedilmiş idi[227]. Bu durum için şöyle bir somut örnek verilebilir: Özel nitelikli kişisel verileri işleyen ve bu kişisel verileri işleyiş gereği gerek yurt içine gerekse yurt dışına aktaran bir kuruluşun, diğer hukuki sebeplere dayanamadığı durumlar özelinde kişisel verilerin işlenmesi için ayrı, özel nitelikli kişisel verilerin işlenmesi için ayrı, kişisel verilerin yurt içine aktarımı için ayrı, kişisel verilerin yurt dışına aktarımı için ayrı, özel nitelikli kişisel verilerin yurt içine aktarımı için ayrı, özel nitelikli kişisel verilerin yurt dışına aktarımı için ayrı açık rıza alması gerekmektedir. Ayrıca açık rıza almak gerekliliğinden kasıt, ilgili kişinin, açık rıza vereceği her bir hususa ilişkin ayrıca onay vermesi, bu hususların tek bir imza ya da onay kapsar şekilde toplanarak "battaniye rıza" durumunun meydana getirilmemesidir[228]. Yani bu şirketin

[227] Bkz. yukarıda I. Bölüm 4.1.2.8.
[228]KVKK. Kurul Kararları. 27.02.2020 tarihli ve 2020/173 sayılı karar özeti. https://www.kvkk.gov.tr/Icerik/6739/2020-173.

uygulamada, ilgili kişilerden alacağı açık rıza hukuken bir sözleşme olarak değerlendirildiğinde, altı maddeli bir sözleşmenin her maddesinin ayrı ayrı imzalanması veya onaylanması anlamına gelecektir. Bu durumun sözleşmeler hukuku ile bağdaşır bir yönünün bulunmadığı kabul edilmelidir. Zira sözleşmeler hukukunda asıl olan, tüm şartların yazılı olduğu bir metnin en sonda imzalanması ya da onaylanması ile o metindeki her maddenin geçerlilik kazanmasıdır. Hatta maddelerden birinin hukuka aykırı olması durumunda kısmi geçersizliğin söz konusu olması da sözleşmeler hukukunda kabul edilmektedir. Hal böyle olunca kişisel verilerin korunması hukukunun bu konuda sözleşmeler hukukunun temel prensipleriyle çeliştiği kabul edilmelidir. Kurum'un görüşü olan her bir rıza için ilgili kişinin ayrı ayrı imza atması gerekliliği, sözleşmeler hukukundan farklıdır[229].

Açık rıza beyanlarının, orantılılık ilkesi yahut diğer sebeplerle Kurul tarafından geçersiz kabul edilmesi, uygulamada çok karşılaşılan bir durumdur. Bu durumun çok fazla olması ise sözleşmeler hukukunun temel prensibi olan "irade özgürlüğü" ile bağdaşmayan niteliktedir. Bir an için açık rıza beyanlarının genel işlem koşulu olarak düşünülmesi halinde dahi genel işlem koşulu niteliğindeki sözleşme yahut beyanları onaylayan kişinin kimliği, taraflar arasında kurulan hukuki ilişkinin genel işlem koşullarının geçerliliği için irdelenmesi gereken hususlarındandır. Oysa kişisel verilerin korunması hukukunda bu neviden herhangi bir inceleme yapılmaksızın orantılılık yahut diğer sebeplerle açık rıza beyanlarının geçersiz sayılması yine kabul edilemeyecektir. İzah edilen sebeplerle, kişisel verilerin korunması hukukunun, açık rıza uygulamasında sözleşmeler hukukunun temel prensipleriyle çeliştiği ortadadır. Bu durumun düzeltilmesi adına, açık rıza konusunda gerek mevzuatın gerekse Kurul görüşlerinin ciddi bir yapılandırmadan geçmesi gerektiği kanaatindeyiz.

Kişisel verilerin korunması hukukundaki hukuki alt yapı eksikliklerinden bir diğeri de sağlık verileri üzerinde toplanmaktadır. İş güvenliği ve işçi sağlığı mevzuatı gereği, işveren niteliğindeki tüm şahıs ve kuruluşların, işçilerinden bazı sağlık verilerini alması gerekmektedir. Alınan sağlık verilerinin niteliği işverenin durumuna göre değişmekle birlikte değişmez olan husus işverenlerin sağlık verisi işlemesinin

[229] Sözleşmeler hukukunda bir sözleşmenin tüm hükümlerinin kabulü, tarafların tüm hükümlerin en sonunda yer alacak şekilde tek imza atması ile sağlanabilecektir. Bu şekilde imza atan taraflar sözleşmenin üst metninde yer alan tüm hükümleri kabul, beyan ve taahhüt etmiş olacaklardır.

kaçınılmaz oluşudur[230]. Kanunda düzenlenen sağlık verilerinin işlenmesi şartlarına bakıldığında, şayet işveren sağlık verilerinin işlenmesi konusunda yetkili kılınmış, sır saklama yükümlülüğü altında bulunan bir veri sorumlusu değilse, işçinin sağlık verilerini ancak açık rızası dahilinde işleyebilecektir. Başka bir deyişle farklı bir kanunda alınması emredilen sağlık verilerinin Kanun gereği açık rıza hukuki sebebine dayanılarak alınması gerekecektir. Bu durumun tutarsızlığını gidermek amacıyla uygulamada, işçi sağlık dosyalarının işveren himayesinde değil de işyeri hekimi himayesinde kalması durumunda, işyeri hekiminin Kanunda sayılan yetkili kişilerden olması sebebiyle açık rızaya gerek olmadığından, işçi sağlık dosyaları işveren himayesinde değil de işyeri hekimi himayesinde tutulmaktadır[231]. Bu uygulama her ne kadar açık rıza gerekliliğini ortadan kaldırsa da işverenler bu uygulamaya sıcak bakmamakta ve haklı olarak, bu bilgi ve belgelerin kendi himayesinde de bulunmasını istemektedir. Hal böyle olunca sağlık verilerinin işverenlerce işlenmesinde açık rıza hukuki sebebine dayanılacaktır. Kanunların bu konudaki çelişkisi bir yana, bu konu aynı zamanda işverenleri mağdur edebilecek bir durum olarak da ortaya çıkmaktadır. Zira işverenlerin, tüm işçilerinden sağlık verilerinin işlenmesine ilişkin bir beyana imza alması çok kolay bir çalışma değildir. Gelişen teknoloji ve bilgiye erişimin kolaylaşması sebebiyle işçiler, haklarının bilincinde ve zarara uğratılma konusunda sürekli endişe içindedir. Dolayısıyla kendilerine uzatılan evrakları imzalamaya çekinmekte ve çok defa bundan imtina etmektedir. Böyle bir durumda imzadan imtina eden işçinin sağlık verilerinin işveren himayesinde bulunmaması iş güvenliği ve işçi sağlığı mevzuatına, bulunması ise kişisel verilerin korunması mevzuatına aykırı olacaktır[232]. Yani işçinin bu tutumu işveren için doğacak idari yaptırımları kaçınılmaz hale getirecektir. Bu tutarsızlık ve kanunlar arası çelişkinin derhal düzenlenmesi, sağlık verilerinin işlenmesi hususunun çağın gereklerine ve diğer mevzuat hükümleri uygun olarak değiştirilmesi gerektiği kanaatindeyiz.

[230] Manav, s. 103; Aydın, U. (2002). İş Hukukunda İşçinin Kişilik Hakları, Eskişehir, s. 225.
[231] Özdemir, M./Yılmaz, M./Kaya, H. (2022). "Kişisel Sağlık Verilerinin 6698 Sayılı Kanun Çerçevesinde Korunması", 19 Mayıs Sosyal Bilimler Dergisi, C.3, S.1, 85-96, s.90, dergipark.org.tr/tr/pub/19maysbd, Erişim: 12.04.2023.
[232] Manav, s. 108.

4.1.1.2. Teknik altyapı eksikliği

Kişisel verilerin korunması hukukunun yapıtaşlarından biri teknik tedbirler ve bilişim ortamında veri güvenliğinin sağlanmasıdır. Veri sorumlularınca, bilişim ortamında muhafaza edilen kişisel verilerin, hukuka aykırı bir şekilde dışarıya aktarılmasının ve yetkisiz bir şekilde erişimin engellenmesi gerekmektedir. Hal böyle olunca veri sorumlusu ve veri işleyenlerin ciddi bir teknik altyapıya sahip olmaları gerekmektedir. Veri sorumluları ve veri işleyenlerin teknik altyapısı yanında ülkemizin de bu ihtiyaca hizmet edebilecek bir altyapıya sahip olması gerekir. Gerek kişisel verilerin korunması hukuku gereği yükümlülük altında bulunan kişi gruplarının gerekse ülkemizin tam manasıyla teknik tedbirleri uygulayacak ve siber güvenliği sağlayacak altyapıya sahip olmaması kişisel verilerin korunması hukukunun uygulanmasında teknik altyapı eksikliği olarak ortaya çıkmaktadır[233].

Kişisel verilerin korunması hukuku gereği yükümlülük altında bulunan kişi gruplarının tümü, çalışmamızda izah edilen teknik tedbirleri eksiksiz olarak uygulamak zorundadır. Zira bu hususstaki küçük bir eksikliğin dahi veri güvenliğinin ihlali sonucunu doğurması kuvvetle muhtemeldir. Fakat ülkemizdeki bu kişi grupları düşünüldüğünde hepsinin bu tedbirleri uygulayarak tam güvenliği sağlaması mümkün görünmemektedir. Ülkemizdeki tacirler ve ticari şirketlerin, dernek ve vakıfların ve hatta kamu kurumlarının birçoğunda henüz anti-virüs altyapısı bile bulunmazken, bu grupların, ağ güvenliğini eksiksiz sağlayabilmesi, yerel bilişim sistemlerine ilişkin gerekli güvenliği sağlaması, hataların erken tespitine yönelik log kayıt sistemlerini (işlem kaydı sistemi) ihdas etmesi sanıldığı kadar kolay olmayacaktır[234]. Her şeyden önce bu faaliyetlerin tam manasıyla uygulanması ciddi bir mali yük doğuracaktır. Bu mali yükün tüm bu gruplarca kaldırılabilmesi beklenemez. Mali yükün kaldırılamaması yanında bu uygulamaların tam manasıyla yapılabilmesi için gerekli bilinç düzeyinin de bu gruplarda tam olarak yerleşmediği açıktır. Hal böyle olunca kişisel verilerin korunması hukuku gereği yükümlülük altında bulunan kişi gruplarının teknik altyapı eksikliği sebebiyle bu yükümlülükleri tam olarak uygulaması mümkün gözükmemekte ve bu durum da kişisel verilerin korunması hukukunun uygulamadaki

[233] Küzeci, s. 245.
[234] Kuntoğlu, Ö.F. (2021). "Elektronik Ticarette Kişisel Verilerin Korunması". Bilişim Hukuku Dergisi 3, no: 1, 176-229, s. 208.

beklentileri karşılamasında ve gelişmesinde bir engel olarak ortaya çıkmaktadır[235]. Bu engelin aşılabilmesi için Devlet otoritesinin bu konuda kişi gruplarını desteklemesi gerekmektedir. Bu desteğin mali açıdan yürütülebilmesi için teşvik programlarının açılması, bilinç açısından yürütülebilmesi için ise eğitim ve farkındalık çalışmaları ile denetimlerin düzenlenmesi gerektiği kanaatindeyiz.

Kişisel verilerin korunması hukukunun gereklerinin, ilgili gruplarca yerine getirilmesi için ülkemizin de altyapı geliştirme çalışmalarını hızlandırması zorunludur. En basit örnekle, kişisel verilerin yedeklenmesi ve depolanması hususunda faydalanılan yer sağlayıcıların büyük çoğunluğunun ve en güvenilir denebilecek olanlarının (Google, Amazon, Zimbra vb.) yurt dışı menşeli olması, bu yer sağlayıcılarda yapılan yedekleme ve depolama faaliyetlerinin kişisel verilerin yurt dışına aktarımını doğurması durumu karşısında ülkemizde bu yer sağlayıcıların sağladığı güveni, kaliteyi ve niteliği sağlayan yer sağlayıcılarının bulunmaması veya az olması ciddi bir teknik altyapı eksikliğidir[236]. Bu durumun giderilmesi için ülkemizde gerek yeni yer sağlayıcı hizmeti sunan firmaların ihdası gerekse mevcut firmaların güçlendirilmesi gerekmektedir. Bu çalışmanın da yine Devletçe açıklanacak teşvik programları, eğitimler ve yönlendirmeler ile ivme kazanabileceği kanaatindeyiz. Bunun yanı sıra ülkemizde sınırlı internet hızı kullanılması, bu alanın uygulanmasını ve gelişmesini tehdit eden bir teknik alt yapı eksikliğidir. İnternet hızının tüm ülke genelinde arttırılması için uydu sistemleriyle ilgili çalışmaların hızlandırılması gerekmekte iken, bilhassa organize sanayi bölgeleri başta olmak üzere, veri sorumlusu ve veri işleyen kişi gruplarının bulunduğu alanlardaki internet erişiminin, bu bölgelerdeki kullanıcılar için internette olabilecek en yüksek hıza ulaşılabilmesinin sağlanması için gerekli alt yapı çalışmalarının yapılması gerekmektedir.

[235] Şeşen, Y./Kuzcuoğlu, A.H. (2021). Veri ve Bilgi Güvenliği Bağlamında İstihbarat Faaliyetleri, Lamre Journal, C.2, S.2, s. 98-99.
[236] Selvan, E. (2023). Veri Diplomasisi Ve Uluslararası Veri Güvenliği Politikaları, T.C. Milli Savunma Üniversitesi Atatürk Stratejik Araştırmalar Ve Lisansüstü Eğitim Enstitüsü Stratejik İletişim Anabilim Dalı Stratejik İletişim Programı Yüksek Lisans Tezi, s. 61.

4.1.1.3. Kişi gruplarının altyapı eksikliği

Kişisel verilerin korunması hukukunun uygulanabilmesi için, bu hukukun yükümlü kıldığı kişi gruplarının ve devlet otoritelerinin kendilerini bilinç düzeyi ve teknik altyapı açısından geliştirmesi şarttır.

Kişisel verilerin korunması hukuku ile yükümlülük altına giren kişi gruplarında bu hukukun gereklerini yerine getirmek hususunda ciddi bir dirençle karşılaşılmaktadır. Bu direncin sebebi, her konuda olduğu gibi yeni doğan bir alanın uygulanmasının bilinmemesi ve bu alan uygulanırken farklı alanlar özelinde hata yapılmasından korkulmasıdır. Ülkemizdeki şahıs, kurum ve kuruluşların birçok konuda belli alışkanlıkları vardır. Bu alışkanlıkların en başta gelenleri; birim ve departman kavramları ile yetki ayrımının kurulmaması, personele tam güven ve yetki sınırlarının sürekli ihlaline göz yummak, belge ve bilgilerin imhasında çekinmek, mevcut düzeni değiştiren uygulamaları dışlamak, mali yük getirecek tüm faaliyetlerden uzak durmak olarak ifade edilebilir. Bu alışkanlıklar, kişisel verilerin korunması hukukunun getirdiği yükümlülüklerin uygulanmasında ciddi engellerdir. Her şeyden önce bu kişi gruplarında belli bir birim ve departman kültürünün olmaması, yetki ve erişim sınırlarının uygulanmasını imkansız hale getirmektedir[237].

Kişisel verilerin korunması hukuku, güvenilmeyen personele karşı kişisel verilerin korunmasını değil yetkisiz personele karşı korunmasını emrettiğinden, personel ile olan ilişkilerin güvene dayalı olmaktan ziyade yetkiye dayalı olması gerekmektedir. Ülkemizde bir belge ya da bilginin imha edilmesi ise korkulan ve uzak durulan bir durumdur. Hal böyle olunca kişisel verilerin saklanma süreleri bir yana, belge ve bilgiler okunamayacak hale gelene kadar saklanması gibi bir alışkanlık da bu kişi gruplarında hakimdir. İmha etmek konusunda ise "fotokopisini çekip öyle imha etmek" gibi bir uygulama bile meydana çıkmıştır. Saklama süresi dolan bir kişisel verinin imhası bir zorunluluktur[238]. Bu zorunluluk gereği saklama süresi dolan kişisel verinin tüm suret ve nüshaları ile bilişim ortamındaki yansımalarıyla birlikte imha edilmesi gerekmektedir[239]. Bu duruma karşı bir dirençte bulunulması, ciddi bir eksiklik olarak karşımıza çıkmaktadır. Bunun yanı sıra kişi gruplarında mevcut düzeni

[237] Korkmaz, (Kişisel Verilerin Korunması) s.85-88.
[238] Yücedağ, s.61.
[239] Kara, s. 54-56.

değiştirme korkusu da kişisel verilerin korunması hukukunun uygulanmasını zorlaştırmaktadır. Uygulanacak yetki-erişim sınırları ile yükümlü kişi gruplarının işleyişinde bazı değişiklikler olması kaçınılmazdır. Mevcut düzen bu duruma uygun değilse değiştirilmesi gerekecek olup buna karşı gösterilecek direnç kişisel verilerin korunması hukukunun uygulanmasını olumsuz etkileyecektir. Son olarak da yükümlü kişi gruplarının yükümlülüklerini yerine getirmek için bazı harcamalar yapması kaçınılmaz olacaktır. Fakat kişi gruplarının somut menfaat elde edemeyeceği konular için mali bütçe ayırmak ve bu doğrultuda harcama yapmak gibi bir alışkanlığının pek bulunmadığı da bir gerçektir. Bu nedenle kişisel verilerin korunması hukukunun uygulanması da zorlaşmaktadır. Kişisel verilerin korunması hukukunun uygulanmasına karşı oluşan bu kurumsal direncin kırılabilmesi için yapılması gerekenlerin; yerel otoritelerin bu konudaki eğitici faaliyetlerini arttırması, yerel otoritelerin denetimlerini arttırarak bu uygulamanın kaçınılmaz olduğunu kişi gruplarına bildirmesi, devlet kurumlarının bu konuda örnek uygulamalar yapması ve hakim konumdaki kişi gruplarının diğer kişi gruplarına yönelik farkındalık sağlamak veya denetim yapmak gibi çalışmalar yürütülmesi gerekmektedir[240].

Kişisel verilerin korunması hukukunun uygulanmasının önündeki engellerden biri de personel direncidir. Kurumsal direncin yanında bir de yükümlü kişi gruplarının personelince bu yükümlülüklerin uygulanmasına karşı direnç uygulanmaktadır. Bu direnç sebepleri ve çözümleri itibariyle kurumsal dirençle büyük oranda örtüşmektedir. Yükümlü kişi gruplarının personeli; mevcut iş düzeninde devam etmeyi ve değişiklik yapmamayı istemekte, yetki ve erişim sınırlarını personeller arası ayrım olarak görmekte, bu yükümlülükler kapsamındaki tüm uygulamayı prosedür yükü olarak görmekte ve mevzuatı kabullenmemektedir. Bu eksikliklerin aşılabilmesi için öncelikle kurumsal direncin ortadan kaldırılması, akabinde ise yükümlü kişi gruplarının personelleri üzerinde ciddi bir denetim yapmasının sağlanması gerekmektedir.

Devlet otoriteleri, her konuda olduğu gibi kişisel verilerin korunması hukukunun uygulanmasında da diğer yükümlü kişi grupları için örnek ve yol gösteren olmak

[240] Gündüz, M.Ş. (2022). T.C. Batman Üniversitesi Lisansüstü Eğitim Enstitüsü Siyaset Bilimi Ve Uluslararası İlişkiler Anabilim Dalı, Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği Yüksek Lisans Tezi, s.85.

zorundadır. Oysa uygulamada bilhassa devlet otorite ve kurumlarının kişisel verilerin korunması hukukuna karşı bir direnç halinde olduğu görülmektedir. Bu halde diğer kişi gruplarında, henüz devlet kurumları bunları uygulamazken kendilerinin uygulamasının da makul olmadığı gibi bir algı oluşmaktadır. Devlet otorite ve kurumları, kişisel verilerin korunması hukukunun getirdiği yükümlülükleri uygulamamakla birlikte, kişisel verilerin korunması hukukuna aykırı emir ve talimatlarla diğer kişi gruplarının bu konudaki uygulamalardan çekinmesi de sebebiyet vermektedir. Örneğin bazı kurumlar, diğer kişi gruplarından, saklama süresi dolmuş olan kişisel verilerin yer aldığı belge ve bilgileri talep etmekte ve bu durum da kurumsal direnç başlığı altında incelediğimiz "imha korkusu"nu haklı hale getirmektedir. Bu gibi durumların önüne geçilebilmesi için öncelikle yapılması gereken devlet otoritesi ve devlet kurumlarının kişisel verilerin korunması hukukuna ve bu hukukun getirdiği yükümlülüklere uygun davranmasını ve eğitilmesini sağlamaktır. Bunun sağlanabilmesi için birincil çözüm, devlet kurumlarında veri koruma görevlilerinin bulunması; ikincil çözüm ise Kurum tarafından devlet kurumlarının süratle denetlenerek uyumluluklarının sağlanması için gerekli çalışmayı yapmaya zorlanmasıdır.

4.1.2. Yerel Otoritelerin Hatalı Uygulamaları

Kişisel verilerin korunması hukukunda ülkemizde, yerel otorite olarak Kişisel Verileri Koruma Kurumu ihdas edilmiştir. Kurum, gerek uygulamaya yönelik hazırladığı rehberler ile yol gösterici olma, gerekse yükümlülükler nezdinde yükümlü kişi gruplarını denetleme hak ve yetkisine sahiptir. Bu hak ve yetkiler minvalinde Kurum tarafından hazırlanan rehberler ve Kurul tarafından verilen kararlar kişisel verilerin korunması hukukunun uygulanmasında ciddi önem arz etmektedir. Bu sebeple Kurum'un yayınlamış olduğu rehberler, Kurul'un almış olduğu kararlar ve Kurum'un genel itibariyle bu alandaki tutumu, yükümlü kişi gruplarının uygulamalarında ve kişisel verilerin korunması hukukunun gelişiminde temel yapı taşlarıdır. Kurum tarafından bu süreçlerde yorum hataları yapılması, uygulamadan uzak değerlendirmeler yapılması, belli yükümlülüklere yoğunlaşıp diğer yükümlülüklerin öğrenilmesinin ve önem gösterilmesinin gölgelemesi, sistemli bir denetim mekanizması kurulmaması gibi durumlar Türk Veri Koruma Otoritesi olan Kurum'un başlıca hatalı uygulamalarıdır.

Kişisel verilerin korunması hukuku, getirdiği tüm yükümlülükler ile bir bütündür. Bu yükümlülüklerin bazılarının ön plana çıkarılması, diğer yükümlülükleri gölgesine almakta ve önemini azaltmaktadır. Ülkemizdeki uygulamada Veri Sorumluları Sicili (VERBİS)[241] adında bir sicil ihdas olunmuş ve bazı şartları sağlayan veri sorumlusu ve veri işleyenler bu sicile kayıttan muaf tutularak diğer veri sorumlularının sicile kaydı ve birtakım bildirimler yapması zorunlu tutulmuştur. Sicile kayıt için son tarih Kurul kararı ile belirlenmiş ve fakat bu tarih yine Kurul tarafından birçok kez ertelenmiştir. Bu nedenle uygulamada yükümlü kişi gruplarınca, kişisel verilerin korunması hukuku VERBİS kayıt ve bildirim yükümlülüğünden ibaret sanılmıştır. Bunun sonucu olarak da VERBİS'ten istisna tutulan kişi grupları kendisini tüm kişisel verilerin korunması mevzuatından muaf zannetmiş, VERBİS kayıt ve bildirim yükümlüsü kişi grupları ise yalnızca VERBİS kayıt ve bildirim yapılmasının yeterli olacağını ve VERBİS kayıt ve bildirim sürelerinin sona ermesine kadar vakitlerinin olduğu gibi yanlış yorumlar meydana gelmiştir. Buna karşılık Kurum ise somut, anlaşılır ve herkesçe ulaşılabilir bir açıklama ile; bu alanın VERBİS'ten ibaret olmadığı, VERBİS dışında da yükümlülüklerin bulunduğu yönünde bariz bir açıklamada bulunmamıştır. Sonuç olarak halen uygulamadaki yükümlü kişi gruplarının ve hatta kişisel verilerin korunması hukukunda yükümlü kişi gruplarına danışmanlık yapan kişi veya kuruluşların bu bilgi eksikliği devam etmiş ve bu durum hatalı uygulamalara yol açmıştır. Bu hatalı uygulamanın giderilebilmesi için Kurum'un, yükümlü kişi gruplarına yönelik; kısa, somut ve anlaşılabilir ifadelerle her türlü vasıta ile bu durumu izah eden faaliyetlerde bulunması, eğitimleri arttırarak bilhassa yükümlü kişi gruplarını bu eğitimlerde hedef alması, denetim sistemini ivedi olarak oturtması ve sistemli denetimlere başlaması gerekmektedir[242].

Kurum tarafından yapılan hatalı yorumların da kişisel verileri koruma hukukunun gelişimini olumsuz etkilediği ifade edilmelidir. Fakat kişisel verilerin korunması hukukunun bir hukuk alanı olduğu düşünüldüğünde, alanın gelişmesi için farklı yorumlara ihtiyaç duyulduğu ve her farklı yorumun bir hata olarak değerlendirilmesinin doğru olmadığı da kabul edilmelidir. Dolayısıyla çalışmamızda Kurum'un tüm farklı yorumlarının bir eleştirisi yapılmayacak olup yalnızca

[241] Detaylı bilgi için: 30.12.2017 tarihli ve 30286 numaralı Resmi Gazete. "Veri Sorumluları Sicili Hakkında Yönetmelik", https://www.resmigazete.gov.tr/eskiler/2017/12/20171230-7.htm.
[242] Özdemir, s. 126; Akgül, s. 193; Gündüz, s. 32.

uygulamada ciddi sorunlara yol açan bazı yorumlarına kısaca değinilecektir. Bu hatalı yorumların en başta geleni; bilişim ortamındaki kişisel verilerin, yer sağlayıcılar marifetiyle muhafazasında, yer sağlayıcıların sunucu panellerinin bulunduğu ülkeye kişisel veri aktarımının gerçekleşmiş sayılacağı şeklindeki yorumdur. Bu yorum sebebiyle uygulamada, dünya çapında kullanılan en büyük yer sağlayıcılardan ülkemizde yer alan yükümlü kişi grupları faydalanamamakta veya faydalanması halinde ciddi bir risk ya da yük altına girmek zorunda kalmaktadır[243]. Kurum'un bu yorumu yapmasında; verinin somut bir olgu olmadığını, yurt dışındaki sunucuda muhafaza edilmesinin de veriyi ülke dışındaki kimselerin kullanımına sunmayacağını gözetmemesinin sebep olduğu kanaati ile Kurum'un derhal bu görüşünden dönmesi gerektiği kanaatindeyiz.

Kurum'un hatalı uygulamalarından biri ve kanaatimizce en önemlisi de bir denetim sistemi kurarak sistemli bir denetim çalışmasına henüz başlamamış olmasıdır. Kurum halihazırda yaptığı denetimleri çok yüksek oranda şikayet üzerine yapmakta onun dışında ise toplumda tepki çeken olaylar üzerine bazı denetimler başlatmaktadır. Hal böyle olunca yükümlü kişi gruplarında, "bizi kim, neden şikayet etsin?", "şikayet edilmedikçe bir sorun yok." minvalinde düşünceler yerleşmektedir. Kurum'un geçen yıllara rağmen sistemli bir denetim çalışması başlatmamış olması, VERBİS kayıt ve bildirim tarihlerinin defalarca ertelenmesi gibi durumlar da bu düşünceleri perçinlemektedir. Bu düşünceler ise kişisel verilerin korunması hukukunun herkesçe uygulanmasını engellemekte, bu vesile ile gelişimi açısından da tehdit unsuru teşkil etmektedir. Oysa Kurum'un resen denetleme yetkisinin bulunduğu hususu KVKK m.15'te düzenlenmiştir. Ülkemizde uygulanmaya çalışan mevzuatların, denetim sonucunda cezai yaptırımlar uygulanıp bu durum kulaktan kulağa yayılmadıkça uygulanmadığı acı bir gerçektir. Bu sebeple Kurum'un sistemli bir denetim faaliyetine girişmesi gerektiği kabul edilmelidir[244]. Sistemli bir denetim faaliyeti için Kurum'un başta büyükşehirler olmak üzere farklı şehir ve bölgelerde birimler ihdas etmesi, bu birimler marifetiyle sistemli ve ciddi denetimler yürüterek gerek kişisel verilerin korunması hukukunun gerekse Kurum olarak bizzat kendisinin varlığını ve

[243] KVKK. Kurul Kararları. 31.05.2019 Tarihli ve 2019/157 Sayılı Karar Özeti, https://www.kvkk.gov.tr/Icerik/5493/2019-157, Erişim: 12.02.2023.
[244] Korkmaz, (Kişisel Verilerin Korunması) s. 85; Küzeci, s. 2020; Kuşkonmaz, s. 101; Develioğlu, s. 50.

gerekliliğini ispat etmesi gerektiği kanaatindeyiz. Bu kanaatin yanı sıra, günümüz ekonomik şartları da gözetilerek, yükümlü kişi gruplarına, doğrudan yaptırım uygulamak yerine, aykırılıklarının tespit edilerek giderilmesi için süre verilmesinin çok daha doğru olacağı ifade edilmelidir. Bu denetimlerin yaratacağı yankı ile yükümlü kişi gruplarının kişisel verilerin korunması hukukundan ve gereklerinden haberdar olacağına, bu doğrultuda gerekeni yapacaklarına, bu vesile ile de kişisel verilerin korunması hukukunun uygulanmasının ve gelişiminin sağlanacağına inanıyoruz.

4.2. Mikroçiplerin Kullanımında Kişisel Verilerin Korunması Açısından Yaşanabilecek Sorunlar

4.2.1. Güvenlik Sorunu

Teknolojinin bize sunduğu olanakların popülaritesini artıran unsurlar hayatı kolaylaştırma düzeyi ya da insanlara keyif verme düzeyidir. Bireyler hayatları kolaylaştıkça veya keyif aldıkça daha rahat hissedecek ve kullandığı teknolojiye güveni artacaktır. Örneğin sosyal medya hesaplarında bireyler kendileriyle ilgili birçok bilgiyi çekinmeden paylaşabilmektedirler[245]. Benzer şekilde, bir alışveriş sitesinden alışveriş yaparken buna alışmış bir kişi ad-soyad, adres, iletişim ve ödeme bilgilerini paylaşmaktan çekinmemektedir. Bireyler kimi zaman çekilişe katılmak veya promosyon ürün kazanmak gibi sebeplerle de kişisel verilerini paylaşabilmektedirler. Paylaşılan bu kişisel verileri ile bireyler bir nevi tercihlerini, zevklerini, ekonomik durumunu, ilgi alanlarını ve daha birçok verisini karşı tarafa aktarmaktadırlar.

Nöro pazarlama, insan beynindeki satın alma algısını baştan sona inceleyerek ortaya çıkan sonuçlardan bir pazarlama stratejisi geliştirme tekniğine denir. Kişisel verileri toplanan bireyler için bu veriler yine kendilerine yönelik reklam ve pazarlama aracı olarak kullanılmaktadır. Dolayısıyla kişisel verilerin alınması, toplanması nöro pazarlamaya hizmet etmektedir. Kişisel verilerden yola çıkarak kişiye sunulan ürünler, alışveriş piyasasında bir yerde kişinin kimliğini oluşturmaktadır. Bireyler istedikleri

[245] Güneş Peschke/ Peschke. (2013). "Protection Of The Mediatized Privacy In The Social Media: Aspects Of The Legal Situation In Turkey And Germany", Gazi Üniversitesi Hukuk Fakültesi Dergisi, C.XVII, Y.2013, Sa. 1-2, s. 867, https://dergipark.org.tr/tr/download/article-file/789306, Erişim: 27.01.2023.

ürünleri almak ya da kendilerine menfaat sağlamak amaçlı olarak düşünmeden ve çok incelemeden kişisel verilerini çevrimiçi ortamda paylaşabilmektedirler[246]. Hatta bireyler bu paylaştıkları kişisel verilerin kimlere hangi amaçlarla aktarıldığını dahi takip etmemek ve umursamamaktadırlar.

Bireyler kişisel verilerini dikkatsiz bir şekilde paylaşırken bir yandan kişilik haklarının zarar görmesi de olasıdır. Kişisel verilerin dikkatsizce paylaşılması kişiye sıkı sıkıya bağlı olan kişinin maddi, manevi ve iktisadi varlığı üzerinde olan haklarının paylaşılan kişinin önüne serilmesidir. Kişisel verilerinin rızası hilafına paylaşılmasından kaynaklı zarar gören bir kişi, kişisel verileri aynı zamanda kişi hakları kapsamında korunduğu için bir nevi kişilik haklarını korumaya yönelik tazminat davası açabilecektir[247]. Bu husus KVKK m.14/(3)'de "kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır" şeklinde ifade edilmektedir. Kişisel Verileri Koruma Kurulu bir kararında boşanma davasında eşinin eczanede kayıtlı ilaç bilgilerinin mahkemeye sunulması hususunda sunan tarafa idari para cezası verilmesine karar vermiştir[248]. Boşanma davası kapsamında zarar gören taraf bu zarara dayanarak karşı tarafa tazminat davası da açabilecektir.

Tarih boyunca insanların tercihleri, seçimleri, kimlerle yakın oldukları, nerelere gittikleri gerek istihbarat[249] sebebiyle devlet gerekse ticari menfaat sağlamayı düşünenler için merak konusu olmuştur. Teknolojinin gelişmesiyle birlikte de insanların gözetlenmesi her alanda kolaylaşmıştır. Günlük yaşantıda dışarıda ya mobese kamerası ya da evlerin, işyerlerinin kameraları bireylerin görüntü verisini her gün işlemektedir. Herhangi bir kameranın görmediği bir alanda durmak bugün neredeyse imkansızdır. Sadece fiziki olarak bedenlerimizin değil düşünce olarak karakterimizin de takip edildiği internet tabanlı sosyal mecralarda ise devletin yanı sıra bildiğimiz ya da bilmediğimiz birçok özel şirket de bizi gözetlemektedir. Bu gözetlenme ve takip edilme durumu kimi insanlar için sorun oluşturmamakta iken kimi

[246] Küzeci, s. 11; Oğuz, S. (2018)."Kişisel Verilerin Korunması Hukukunun Genel İlkeleri", Bilgi Yönetimi ve Ekonomi Dergisi, C.13, S.2, 121-138, s. 136.
[247] Keskin, s. 268.
[248] İlgili kişiye ait "Medula Eczane çıktılarının eczacının eşi tarafından kullanılması" hakkında Kişisel Verileri Koruma Kurulunun 07/05/2020 Tarihli ve 2020/355 Sayılı Karar . https://www.kvkk.gov.tr/Icerik/6767/2020-355, Erişim: 05.01.2023.
[249] Üstün Türkoğlu K. (2021). "Güvenlik Soruşturmalarında Kişisel Verilerin Korunması", Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi C. XXV, Y.2021, Sa. 2, s. 807, https://dergipark.org.tr/tr/download/article-file/1754338, Erişim: 06.06.2022.

insanlar bu durumdan hoşlanmamaktadır, kimi insan ise bu denli gözetlendiğinin farkında bile değildir. Sosyal mecralarda birçok verisini düşünmeden paylaşanların yanı sıra sosyal medya hesabı kullanmayan veya üyelik abonelik gerektiren platformlara hiç katılmayanlar mevcuttur. Bireylerin teknolojinin bizleri gözetlemesine ve takip etmesine karşılık bireylerdeki bu farklı bakış açıları gelecek zamanda mikroçip enjeksiyonuna olan tutumlarını da etkileyecektir[250].

Mikroçiplerle veri işleme faaliyetinde mikroçipteki kişisel verilerin işlenme yöntemi için iki türlü ihtimal olduğuna daha önce değinmiştik. Kişisel verilerin mikroçiple işlenmesindeki ihtimal yöntemlerden birincisi halihazırda tüm verilerimizin bulunduğu devlet altyapısı iken ikincisi daha sonradan kişisel verilerimizi paylaşmamız gereken aracı nitelikte özel şirketlerdir. Mikroçiplerle veri işlenirken devlet altyapısının kullanıldığı durumda kanaatimizce bireyler kişisel verilerinin mikroçipe işlenmesi konusunda bir güven sorunu yaşamayacaktır. Ancak aracı nitelikte özel şirketler aracılığıyla bu faaliyet gerçekleştirilirse bireyler için bu durum şüphe yaratabilir. Devletin öncelikli amacı vatandaşına hizmet sağlamaktır oysa özel şirketlerin amacı kendi çıkarlarını korumak, gelir ve menfaat elde etmektir. Bu sebeple aracı nitelikte özel şirketler aracılığıyla veri işleme faaliyeti yürütülecekse dahi devletin bu alanda ciddi düzenlemeler yapması, katı kurallar koyması ve denetlemesi şart olacaktır. Mikroçiplerle kişisel veri işleme faaliyeti aracı nitelikte özel şirketler aracılığıyla yapılsa da devletin düzenlemelerine uygun ve devletin denetlemesi altında yürütülürse bireylerin güvenini kazanmak bir nebze daha kolay olacaktır.

Mikroçip kullanımının yaygınlaştığı durumlarda, kullanımın zorunlu olmayacağı yönünde düşünürsek güvenli olduğunu düşünenler kullanacak, güvenli olmadığını düşünenler ise kullanmayacaktır. Covid-19 aşıları için bile çip taşıdığına yönelik çıkan iddialarda bireylerin bu tip bir takip sistemine nasıl karşılık verdiği

[250] Santa Clara Üniversitesi Markkula Uygulamalı Etik Merkezi'nde teknoloji etiği direktörü Brian Green, mikroçip implantlarının etiği konusunda: "*Mikroçipler evcil hayvanlar için yeni bir teknoloji olmasa da, perakendecilerin, kredi kartı şirketlerinin ve işverenlerin zorunlu implantlara ihtiyaç duyduğu bir dünyada ülkenin bir "gözetim devleti" haline gelebileceği"* yönünde endişelerini belirtmiştir. Green ayrıca, gözetleme devleti modeli gerçekleşirse, mikroçip implantlarını kabul etmeyen bireylerin marjinalleştirilme ve modern kolaylıklardan dışlanma riskiyle karşı karşıya kalacağını ve bireylerin her zaman ayrımcılığa ve zulme maruz kalmadan implantlardan vazgeçme hakkına sahip olması gerektiğini düşünmektedir. Thomas Net. (2019). "The Future of Microchip Implants in Humans", https://www.thomasnet.com/insights/the-future-of-microchip-implants-in-humans/, Erişim: 12.12.2021.

görülmüştür. Sosyal medya hesapları, alışveriş geçmişleri, mobese kameraları ile her gün takip edilen bireylerin bu durumun çiple yapılması senaryosunda buna tepki göstermeleri de kanaatimizce anlaşılabilir değildir.

Mikroçiple veri işleme faaliyetinin güvenilirliğinde hukuka uygun olup olmadığı da tartışılırsa bu konuda mahremiyet etki değerlendirmesi uygulanmalı ve veri işleme faaliyetinin hukuka uygunluğuna bu çerçevede karar verilmelidir. Mikroçiplerle kişisel veri işleme faaliyetinde daha sonraki yapılacak geliştirici teknolojilerde de mevzuata uygunluk sağlanmalı ve bireylerin tekrar tekrar güvenilirliğinde şüphe duyması ortadan kaldırılmalıdır. Kanaatimizce veri işleme faaliyetlerinin çeşitlerine ilişkin güven ancak bireylerin kişisel verilerinin korunmasına ve korunmasının gerekliliğine ilişkin yeterli bilince sahip olmasıyla gerçekleşecektir.

Özel nitelikli kişisel veriler hassas veriler olarak da bilinmekte ve tabiri caizse özel korumaya tabi tutulmaları gerekmektedir. Bireyler adı-soyadı, adresi, iletişim bilgileri gibi bilgilerinden önce sağlık, cinsel hayat ve parmak izi verileri gibi verilerinin bilinmesini istemeyecektir. Bu nedenle mikroçiplerle bu verilerin saklanması durumunda da idari ve teknik tedbirler sıkı bir şekilde uygulanmalıdır. Kullanıcıların görüşleri alınmaksızın otomatik işlemeye dayalı bir karara maruz kalmamalarını temin edecek tipte veri işlemesi yapılmamalıdır[251].

Mikroçiple veri işleme yapılırken kullanıcılara seçim yapma özgürlüğü tanınmalıdır. Bireylerden bazıları her işlemi için mikroçip kullanmayı tercih ederken diğerleri sadece sağlık bilgilerinin bulunduğu ve acil durumlarda kullanılabilecek mikroçip kullanımını tercih etmek isteyebilir. Bu duruma uygun bir şekilde ürün tesisi yapılmalıdır.

Mikroçiplerle veri işlemede güvenin artırılması için çeşitli düzenlemeler yapılabilir. Örneğin kişinin mikroçipin veri işlemesini internet veri tabanı üzerinden ya da mobil uygulamadan açıp kapatabileceği bir sistem getirilebilir. Bu sayede kişi verilerini paylaşmanın riskli olduğu ya da veri sızıntısı olabileceğini düşündüğünü algıladığı durumda mikroçipin veri paylaşımını kapatabilecektir. Bir diğer düzenleme ise veri paylaşımında şifre isteme yöntemi olabilir. Kredi kartlarında kullanım öncesi

[251] Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. "Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler", https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf, Erişim: 03.01.2022.

şifre isteme yöntemi gibi mikroçiplerle de ödeme bilgileri paylaşılırken şifre isteme düzenlemesi getirilebilir.

Bireylerde mikroçiplere ilişkin genel korku diğer elektronik cihaz türleri gibi hackerlar tarafından ele geçirilme, virüs bulaştırma ya da gizli fotoğraf, video veya belgelere ulaşma olasılığıdır[252]. Çiplerin güvenliğinde oluşabilecek zafiyet çipin çalınması ya da kopyalanması olacaktır. Bu olasılığın önüne geçilebilmesi için teknik tedbirler alınmalıdır. Kişilerin vücutlarında bulunan mikroçipler pasif tipte çip olup okuyucuya yaklaştırıldığında aktif olmakta ve veriyi aktarabilmektedir. Bir kişinin kimlik hırsızlığı yapabilmesi için aktif bir çip geliştirip onu bataryalı ya da sarj edilebilir yapması gerekmektedir. Çünkü pasif çipler güce ihtiyaç duymazken aktif çipler için enerji gerekecektir. Henüz mikroçiplerde böyle bir teknoloji olmadığı için örneğin çipler, kişinin konum bilgisini de aktaramazlar. Ancak şunu da belirtmek de fayda var ki çiplerin klonlanması çok da zor değildir.

Cambridge, Mass'ta bağımsız bir güvenlik araştırmacısı olan Jonathan Westhues, yerleştirilebilir mikroçipi elektronik olarak klonlayan, elde taşınan bir cihaz olan bir "emülatör" icat etmiş ve bilgisayar güvenliği uzmanlarından oluşan bir ekiple, bir çipten veri koparmanın ne kadar kolay olduğunu televizyonda göstermiştir[253]. Bir başka çalışmada ise Hacker Seth Wahle, bir okuyucudaki güvenlik açığına yönelik bir saldırı gerçekleştirerek kötü niyetli bir link içeren e-postayı okuyucuya gönderebilmiştir[254]. Yani okuyucuları ele geçirmek ve kötü amaçlar için kullanabilmenin mümkün olduğunu göstermiştir. Johns Hopkins Üniversitesi araştırmacısı Adam Stubblefield: "Mikroçipli bir kişinin bir adım yakınından geçerken, çipin kodunu kopyalayarak, ardından bir düğmeye basarak aynı kimlik numarasını esasen kişinin kimliğini herhangi bir okuyucuya tekrarlarsınız" şeklinde ifadelerde bulunarak çiplerde kopyalamanın kolay olduğunu öne sürmüştür. VeriChip şirketinin CEO'su Scott Silverman da aynı şekilde: "Bir tarama cihazıyla radyo frekansı ürünlerinden bilgi almak zor değil" demiştir. Ancak, "çipin kendisi yalnızca

[252] Esmer, Ö. (2011). "RFID Teknolojisinde Veri Güvenliğinin Sağlanması İçin Melez Şifreleme Algoritmasının Uygulanması", Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara, s. 33.
[253] Youtube. "HOPE Number Six (2006): How To Steal Someone's Implanted RFID - And Why You'd Want To", https://www.youtube.com/watch?v=jzzg3-L-QDI, Erişim: 01.12.2022.
[254]Grauer Y.(2018). "A practical guide to microchip implants", Arstechnica, https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/, Erişim: 15.10.2021.

benzersiz, 16 haneli bir kimlik numarası içerir. İlgili bilgiler bir veri tabanında saklanır" şeklinde ifade etmiştir.

Mikroçiplerden veri kopyalanması ne kadar mümkün olmasa da uygulama da bunun işlevselliğinin pek olmadığından söz etmek gerekmektedir. Bir kişinin kişisel verilerini almanın mikroçipini kopyalamaktan daha kolay yolları vardır. Kişisel verilerinin korunması gerektiğinin bilincinde olmayanlar bu verilerini zaten paylaşmaktadırlar. Covid döneminin de etkisiyle iyice artan online alışverişte alışveriş yapılan siteler ile paylaşılan kişisel verilerimiz bu internet sitelerinin veri tabanında saklanmaktadır. Tek seferde siteyi eklemek ile binlerce onbinlerce kişinin verisine erişilebilecektir. Kişisel verileri ele geçirmek için tek tek mikroçip kopyalamaktan daha kolay olan bu yöntemin denenmesi daha sık rastlanılacak bir durumdur. Üstelik kopyalamak, çalmak gibi eylemlere de gerek kalmaksızın deepweb dediğimiz internetin gizli katmanlarında bedel karşılığı olarak kitlelerin kişisel verileri satılmaktadır[255].

Güvenlik zafiyetinin bir başka boyutu da araba ev gibi alanlara girişte mikroçip kullanımında mikroçipin ele geçirilerek-hacklenerek- eve girilmesi ya da arabaya binilmesidir. Gerçekten de böyle bir ihtimal bulunmaktadır. Evlere girişte ve arabalara binişte mikroçip kullanımının olması durumunda mikroçipin kopyalanarak eve giriş ve arabaya binmek mümkün olacaktır. Ancak şu an günümüzde de evin anahtarını ya da arabanın anahtarını çalan birisi de eve girebilecek ya da arabaya binebilecektir. Bu durumda mikroçipler için kopyalanma tehdidi anahtarın çalınması ile aynı düzeydedir. Yine kilitli kasalar gibi güvenli olması beklenen alanlar için de aynısı durum geçerlidir[256].

Güvenlik sorununun beraberinde getireceği sorunlar ile kişilerin kişilik hakları, mülkiyet hakları, fikri hakları gibi birtakım hakları zarar görebilecektir. Bu hususta güvenlik sorununun aşılması için yukarıda sayılanlar gibi mutlak veya nispi hakların korunmasının artırılması hususunda çalışmalar yapılmalı ve farklı koruyucu veya

[255] Hürriyet. (2020). "Bilgilerinizin Dark Web üzerinden satışa çıkarıldığını nasıl anlarsınız?", https://www.hurriyet.com.tr/teknoloji/bilgilerinizin-dark-web-uzerinden-satisa-cikarildigini-nasil-anlarsiniz-41625223, Erişim: 29.05.2023.
[256] Esmer, s.19; WhitePaper. (2007). "Radyo Frekanslı Tanımlama", KoçSistem , 3-6, https://silo.tips/download/rfid-teknolojsnde-ver-gvenlnn-salanmasi-n-melez-freleme-algortmasinin-uygulanmas, Erişim: 12.08.2022.

caydırıcı hukuki düzenlemeler getirilmelidir. Örneğin bir kişinin diğerinin mikroçipindeki bilgileri hacklemesi sonucunda hacklenen kişinin isim-soyisim bilgileriyle iş ve işlemler yapması, o kişinin taşınır veya taşınmazları aleyhine işlemler yapması gibi durumların ortaya çıkması durumunda kişilik hakları, mülkiyet hakları zarar gören kişinin bu hususları önleyici ve zararını giderici davalar açması gerekecektir.

Mikroçiplere olan güvenin artırılması için bireyler mikroçiplerde hangi verilerinin bulunduğu, mikroçiplerin çalışma mekanizması ve mikroçiplerdeki verilerini nasıl koruyabileceklerine ilişkin bilinçlendirilmelidir. Bunun yanı sıra mikroçipteki kişisel verileri barındıran veri tabanının veri sorumlusu KVKK'da öngörülen tüm idari ve teknik tedbirleri almalıdır. Mikroçipi taşıyan veri sahibi ilgili kişi kadar veri tabanında veri barındıran veri sorumluları da kişisel verilerin güvenliğini sağlamalıdır.

4.2.2. Aktarım Sorunu

Veri aktarımından söz edebilmek için bir veri sorumlusundan başka bir veri sorumlusuna ya da veri işleyene yönelik paylaşım gerekmektedir. Deri altı mikroçip kullanımı şüphesiz bireylerin hayatını kolaylaştıracak bir faaliyet olacaktır. İlk çıktığı günden bugüne tepki ile direnç karşılaşılmış olsa da kanaatimizce zamanla yaygınlaşırsa normalleşecektir. Mikroçipleri kullanırken de diğer kişisel veri aktarım cihazlarında olduğu gibi güvenliğe dikkat etmek gerekecektir. Bugün bireyler; telefon numarasını, T.C. kimlik numarasını, adresini alelade paylaşmıyorsa mikroçip ID numarasını da paylaşmamalı ve alelade her yerde kullanıma sunmamalıdır[257].

Internet of Things (IoT) olarak da bilinen nesnelerin interneti insan müdahalesi olmadan internete bağlı cihazların veri aktarımı yapabilmesi olarak tanımlanmaktadır[258]. Biz farkında olmadan elektronik cihazlarla her gün veri işlemesi yapılmaktadır. İnternete yüklenilen belge, fotoğraf gibi dokümanlar sadece

[257] Esmer, s. 14; Ari, J. (2005). "RFID Security and Privacy: A Research Survey", RSA Laboratories, 5- 11, https://www.researchgate.net/publication/3236246_RFID_security_and_privacy_A_research_survey, Erişim: 06.05.2022.

[258] European Union Agency for Network and Information Security. (2016). Cyber Security and Resilience of Intelligent Public Transport, "Good Practices and Recommendations", s. 50, https://www. enisa .europa.eu/ publications/good-practices-recommendations, Erişin:04.01.2022.

yüklediğimiz yerle kalmayıp farklı yerlere de iletilmektedir[259]. Mikroçiplerle veri aktarımında da nesnelerin interneti söz konusu olacak ve okuyucu tarafından okunulan çipteki veriler farklı yerlere aktarılabilecektir. Mikroçiplere yüklenilen verilere ilişkin aktarımın üzerinde durulması gerekmektedir.

Mikroçiplere yüklenen veriler bu verilere özel veri tabanında saklanırken başka yerlere aktarılıp aktarılmadığına ya da ne tip bir veri tabanında saklandığına bakılması gerekmektedir. Mikroçiplerdeki kişisel verilerin aktarılmasına ilişkin dikkat edilmesi gerekenler: Aktarımın veri sahibi ilgili kişinin rızasını gerektirip gerektirmediği, bu aktarıma ilişkin veri sahibi ilgili kişinin aydınlatılıp aydınlatılmadığı ve aktarımın yurtdışına olup olmadığıdır[260].

Kişisel verilerin işlenmesine ve aktarılmasına ilişkin şartlar KVKK'nın 5, 8, ve 9. maddelerinde açıklanmıştır. Kural olarak veri sahibi ilgili kişinin rızası olmadan işlenemeyen kişisel veriler, kanun maddelerinde sayılan istisnalara binaen işlenebilecektir[261]. Kanunda kişisel verilerin aktarılmasına ilişkin rıza istisnalarında kişisel verilerin işlenmesindeki maddeye atıf yapılmış ve istisnaları benzer olarak düzenlenmiştir. Mikroçiple veri işlemede kişinin kimlik, iletişim bilgilerinin yanı sıra özel nitelikli kişisel verileri olan sağlık verileri de işlenebilecektir. Bu durumda özel nitelikli kişisel verilerin mikroçiplerle işlenmesi ve aktarılması için açık rıza unsurunu ayrıca değerlendirmek gerekir; çünkü kanun özel nitelikli kişisel verilerin işlenmesini ve aktarılmasını farklı kurallara tabi tutmuştur.

Mikroçiple kişisel veriler işlenmeye başlanırken kişilerden veri işlenmesi ve aktarımına ilişkin rıza alınmasının mikroçipin enjekte edildiği aşamada gerçekleştirilmesi daha doğru olacaktır. Uygulamada kişinin mikroçipinin aktif olması için imzalanması gereken evraklar olduğu belirtilerek de kişiden rızası alınabilir. Kişi

[259] Bozkurt Yüksel E. (2015). "Nesnelerin İnternetinin Hukuki Yönden İncelenmesi", D.E.U. Hukuk Fakültesi Dergisi, Cilt: 17, Sayı: 2, s.115, https://www.academia.edu/32452815/Nesnelerin_%C4%B0nternetinin_Hukuki_Y%C3%B6nden_%C4%B0ncelenmesi_Looking_at_IoT_from_Legal_Perspective?email_work_card=view-paper, Erişim: 03.01.2022; Peppet S. (2015). "Regulating the Internet of things: First Steps Toward Managing Discrimination, Privacy, Security and Consent", Texas Law Review, s. 89, https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf, Erişim: 03.01.2022.
[260] Esmer, s. 36.
[261] Bkz. 4.1.2. numaralı başlık.

mikroçiple hangi verilerinin işleneceğine ve verilerinin nereye aktarılacağına ilişkin aydınlatılmalı ve kişiden açık rızası alınmalıdır[262].

Kişinin açık rızası olmaksızın verilerinin işlenebildiği ve aktarılabildiği haller: Kanunlarda açıkça veri işlemenin öngörülmesi, rızasını açıklayamayacak durumda bulunanlar veya rızasının hukuki geçerliliği olmayan kişinin kendisinin ya da bir başkasının hayatı ve beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifası için veri işlemenin gerekli olması, veri sorumlusunun hukuki yükümlülükleri için veri işlemenin zorunlu olması, veri sahibinin verisini alenileştirmiş olması, bir hakkın tesisi, kullanılması veya korunması için ve veri sahibinin temel hak ve özgürlükleri korunacak şekilde veri sorumlusunun meşru menfaatleri için veri işlemesinin gerektiği hallerdir.

Mikroçiplerle veri aktarımının bu istisnaların içerisinde olup olmayacağına ilişkin değerlendirmede bu çalışmada daha önce belirtilen iki ihtimal çerçevesinde düşünmemiz gerekmektedir. Yurtdışına veri aktarımı ise ayrıca değerlendirilecektir. Bunun yanı sıra çip kullanımının yaygınlaşması durumunda çiplerle ilgili yapılacak yasal düzenlemelere bakmak gerekecektir. Henüz bu yasal düzenlemeler mevcut olmadığı için ihtimaller dahilinde değerlendirme yapılarak görüş ve önerilere yer verilecektir.

Mikroçiplerin içerisindeki kişisel verilerin yer aldığı internet veri tabanının devletin himayesinde tutulduğu ihtimalinde devlet, kanundaki veri aktarımına ilişkin şartlardan istisnalar içinde yer alacak ve dolayısıyla bu durumda veri aktarımına ilişkin rıza alınması gerekmeyecektir. Aracı nitelikte özel şirketler için ise yapılan yasal düzenlemelere bakılması gerekecektir. Yasal düzenlemelerde şirketlerin veri aktarımına yetkili kişi olarak belirtilmesi durumunda bu şirketler de veri aktarımında açık rıza alma gerekliliğinin istisnaları arasında olacaktır. Kanun'un 8. maddesinde de belirtildiği gibi kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan diğer hükümler saklı kalacaktır.

Özel nitelikli kişisel verilerin işlenmesi ve aktarılması Kanun'un 6. maddesinde belirtilen şartlara göre yapılmalıdır. Kural olarak özel nitelikli kişisel veriler de veri

[262] Bu hususla ilgili olarak kişisel verileri mikroçip yoluyla işleyen veri sorumlusu aydınlatma metinlerini buna göre düzenleyecek veya güncelleyecektir.

sahibi ilgili kişinin açık rızası olmadan işlenemez ve aktarılamazlar. Kanundaki işleme ve aktarım istisnaları özel nitelikli kişisel veriler için de geçerlidir. Ancak Kanun iki tip özel nitelikli kişisel veriyi diğerlerinden ayrı tutmuş ve işleme aktarıma ilişkin yetkiyi sınırlamıştır. Kanun'a göre: "sağlık ve cinsel hayata ilişkin kişisel veriler ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi 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". Mikroçiplerle veri işleme ve aktarmada bu iki özel nitelikli kişisel veri için Kanun'da sayılan yetkili kişilerin tespitinde çipin okuyucusuna bakılması gerekmektedir. Çipin okuyucusunu barındıran veri sorumlusu bu sayılan kişilerden olmalıdır. Örneğin sağlık verilerinin okunduğu okuyucu hastanede, diş kliniğinde ya da özel muayene hizmeti veren kuruluşlarda olmalıdır.

Yurt dışına kişisel veri aktarımı kural olarak veri sahibi ilgili kişinin açık rızası olmaksızın yapılamaz. Yurt dışı veri aktarımı hem devlet hem de aracı nitelikte özel şirketler tarafından olabilecektir. Örneğin kişi yurtdışına gittiğinde ve mikroçipini orada bulunan bir okuyucuya okuttuğunda kişisel verileri okuyucunun bulunduğu ülkenin veri tabanlarından birine aktarılacaktır. Kanunda yurtdışına veri aktarımı konusu oldukça sıkı şartlara bağlanmıştır. Kanun'un 9. maddesi bu konuya ilişkin düzenlemeyi içermektedir. Yurtdışına kişisel veri aktarımda açık rıza olmaksızın aktarım yapılabilmesi için aktarım yapılacak ülkenin kişisel veriler konusunda "yeterli korumasının bulunması ve Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması" gerekmektedir[263].

Yurtdışı aktarım farklı şekillerde gerçekleşebilmektedir. Avrupa veri koruma otoriteleri veri sorumlusunun hakimiyetinde olan verilerin fiziki olarak yurtdışına çıkmasını yurtdışına aktarım olarak saymamakta iken Türk Hukukunda verinin fiziksel olarak yurtdışına çıkması yurtdışına aktarım olarak kabul edilmektedir. Yurtdışına aktarım bulut sistemine aktarım olarak da ortaya çıkabilir. Bulut sistemleri genelde

[263] KVKK. Yurtdışına Aktarım. https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim, Erişim: 12.04.2023.

sunucuları yurtdışında bulunan sistemlerdir. Bu nedenle yurtdışına aktarımı olan bulut sistemleri işin veri aktarımına ilişkin kurallara uyulmalıdır[264].

4.2.3. Sorumluluk

Teknolojik olarak sürekli gelişen ve internete bağımlı yaşanılan bir çağda çip kullanımı ile insanların da "online" bir varlık haline gelmesi söz konusu olacaktır. Vücuda yerleştirilen deri altı mikroçipi pasif konumda olduğu için teknik olarak sürekli internete bağlı ve veri akışı yapan türde bir cihaz değildir. Sadece okuyucu tarafından okunulduğu zaman veri paylaşımı yapabilecektir. Dolayısıyla bluetooth gibi uzaktan erişimle ulaşılamayacaktır ancak teknolojinin gelişmesiyle buna evrilebilecektir. Hatta mikroçip içerisine yüklü verilerin bir bulut altyapısı içerisinde yedeklenip bilgisayar, telefon gibi cihazlardan yüklü kişisel verilere erişim söz konusu olabilir. Yine telefonlara yüklenen bir mobil uygulama ile mikroçipin içerisine hangi verilerin yüklenebileceği serbestleştirilebilir[265]. Teknolojik olarak çiplerin kullanımı geliştikçe barındırdığı verinin çeşidi ve aktarım şekli değişebilecek, bu da beraberinde sorumluluğu getirecektir.

İş hayatında mikroçip kullanımı işverenlerce daha çok tercih edilen bir yöntem olacaktır. İşçilerin mikroçip kullanımı işverenlerin menfaatine olacak ve insan kaynakları, muhasebe gibi departmanlardaki iş akışını kolaylaştıracaktır. Hatta işverenler tarafından işe alımda mikroçip taşıyan işçilerin daha çok tercih edileceği söylenebilir. Bu hususta dezavantaj ise mikroçip kullanımının işçilere karşı bir mobbing unsuru olarak kullanılıp kullanılamayacağıdır. İşverenlerin mikroçip kullanımını artırmak amaçlı mikroçip sahibi işçilere birtakım ayrıcalıklar tanıması da muhtemeldir. Böyle bir durumda işveren tarafından eşit işlem ilkesine aykırılık oluşacaktır. Bu ihtimaller ancak uygulamada görülecektir; ancak kanaatimizce mikroçip kullanımının yaygınlaşması durumunda yapılacak olan yasal düzenlemelerde işçi-işveren ilişkisinde mikroçip kullanımı başlıklı düzenlemelere yer verilmelidir.

---

[264] Kara, 53.

[265] Aydoğdu Y. (2022). "Mobil Uygulamalarda Kişisel Verilerin İşlenmesi ve Yasal Olarak Dikkat Edilmesi Gereken Hususlar", Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, C. XXVI, Y.2022, Sa. 1, s. 401, https://dergipark.org.tr/tr/download/article-file/2222163, Erişim: 12.09.2022.

İşçilerin mikroçip kullanması durumunda işçilerin kişisel verileri veri sorumlusu olan işverenin sorumluluğunda olacaktır. İşveren mikroçip okuyucularının güvenliğini sağlamalı ve işçilerin kişisel verilerinin güvenliği için idari ve teknik tedbirler almalıdır[266]. Okuyucuların güvenliğinin sorumluluğu veri sorumlusunda olacaktır. Buna benzer şekilde örneğin alışveriş merkezine girerken kişilerin mikroçipini okuttuğu okuyucuların sorumluluğu alışveriş merkezi bünyesinde olacaktır. Mikroçiplerde sorumluluk ve verilerin güvenliği şu iki veri sorumlusu tarafından korunmalıdır: Birisi himayesinde çip okuyucuyu barındıran veri sorumlusu diğeri de mikroçipin içindeki verilerin tutulduğu veri tabanının sağlayıcısı olan veri sorumlusudur. Her iki veri sorumlusu da çipin barındırdığı kişisel verilerden sorumludur ve verilerin korunmasını sağlamalıdır.

Uygulamada veri sorumlularının bilgi teknolojilerini karşılamak için ya da harici birtakım hizmetler almak için bünyesinde bulundurduğu kişisel verileri aktardığı veri işleyenler de veri güvenliğinden veri sorumlularıyla müştereken sorumlu olacak ve veri güvenliği için tedbirler almaları gerekecektir[267]. Veri işleyenler, veri sorumlusunun talimatı doğrultusunda ve veri sorumlusunun kişisel verilerin saklanması ve imhası politikasına uygun hareket etmesi gerekmektedir. Veri işleyenler kendilerine aktarılan kişisel veriler hususunda sır saklama yükümlülüğüne tabi tutulmalıdır. Veri işleyenin sisteminde bir veri sızıntısı olması durumunda veri işleyen bu durumu derhal veri sorumlusuna bildirmelidir. Mikroçiple işlenen kişisel verilerde veri işleyenler teknik alt yapı için devlete ya da aracı nitelikteki özel şirketlere hizmet sağlayıcısı olarak görev yapan kuruluşlar olacaktır.

Kişisel veriler bulut depolama hizmeti alınarak saklanıyorsa burada bulut depolama hizmetini sağlayanlar ya da kişisel verilerin bulunduğu veri tabanının yer sağlayıcı firması veri işleyen olacaktır[268]. Veri işleyen bulut sağlayıcısı bulutta depolanan kişisel verilerin içeriğini bilmeli ve yedeklenmesini takip etmelidir. Mikroçiplerdeki kişisel verilerin bir bulut altyapısında saklandığı düşünülürse uzaktan

[266] Özer Deniz, M. (2020). "İşçilerin Özel Nitelikli Kişisel Verilerinin Korunması Ve Bundan Doğan Sorumluluk", Türkiye Adalet Akademisi Dergisi, Yıl:12, S. 45, 355-378, s. 361; Manav, s. 136.
[267] Yücedağ, s. 53.
[268] Kuntoğlu, s. 188; Paşaoğlu, C. (2019). "Kişisel Verilerin Korunması Kanunu Kişilerin Temel Hak ve Özgürlüklerini Korumak Amacındadır," Video, 6:02, 1.e-Safe Boğaziçi Kişisel Verileri Korumada Yerli Çözümler Zirvesi, yükleyen: e-Safe, https://www.youtube.com/watch?v=e-M392izsks&ab_channel=e-Safe. Erişim: 03.04.2023.

erişim için çift kademeli kimlik doğrulama kontrolü sağlanmalıdır. Bu kontrol tipi Kurum'un da bulut sistemi kullanımı için önerdiği bir güvenlik çeşididir. Kanaatimizce mikroçiplerdeki verilere bulut sisteminden erişimde mutlaka çift kademeli kimlik doğrulama kontrolü olmalıdır. Bunun yanı sıra kişisel verilerin depolanırken kriptografik yöntemlerle şifrelenmesi ve bulut sistemine öyle atılması, faklı bulut sistemleri için ayrı ayrı şifreleme kullanılması gerekmektedir[269]. Örneğin kişisel veriler ile özel nitelikli kişisel veriler farklı bulutlarda saklanacaksa şifrelemeleri ayrı ayrı yapılmalıdır aynı şifre seçilmemelidir. Bulut depolama hizmeti kullanılması bırakılırsa kişisel verilere erişim sağlayabilecek tüm şifreleme anahtarlarının ve kopyalarının yok edilmesi gerekecektir.

Kişisel verileri barındıran cihazların arızalanması durumunda cihazların içeriğinde kişisel veriler bulunuyorsa burada cihazları tamir edecek tamirci, üretici, satıcı, servis gibi üçüncü kurumların himayesine gönderilen cihazlarda bu üçüncü kişilerin sorumluluğu doğacaktır. Böyle bir durumda cihazın arızasıyla ilgilenecek üçüncü kişiden sorumluluğuna binaen taahhüt alınmasında fayda vardır. Alternatif yol olarak cihazın kişisel verileri içeren parçası, örneğin bilgisayarlarda hard disk çıkartılarak cihaz teslim edilebilir. Cihazın veri sorumlusunun himayesinde arızası giderilecekse veri sorumlusu bu aşamada özenli olmalı ve sistemden veri sızıntısı olmasını önlemelidir.

Mikroçip kullanımında sadece veri sorumlusunun değil çipi taşıyan veri sahibi ilgili kişinin de sorumluluğu olacaktır. Bu sorumluluğun bilincinin kazanılması ve kişisel verilerin güvenliğinin sağlanması için birtakım düzenlemeler getirilebilir. Daha önceki başlıklarda yer verilen mikroçip kullanımının şifreli olması ya da özel nitelikli kişisel veri aktarımında şifre kullanılması gibi düzenlemeler getirilebilir. Şifre kullanımı birçok yönden çiplerdeki verilerin güvenliğini sağlayacak ve kişide de koruma içgüdüsü oluşturacaktır.

Mikroçip kullanımının aynı zamanda bir yaş şartına tabii tutulması söz konusu olabilir. Doğar doğmaz küçük bir bebeğe mikroçip enjekte edilmesinin gerekliliği tartışılabilir. Bebekler için doğdukları anda anne ve babasının rızasıyla mikroçip enjekte etmek mümkün olabilir. Mikroçip enjekte edilmiş bir bebekte, bebeğin kimliği

[269] Esmer, s. 41-42; Phil, Z.,(2005). "The Basics of Crytography ", An Introduction to Cryptography, 1-3.

hemen belirlenmiş olacaktır. Böylelikle az da olsa rastlanılan hastanede bebeklerin karışmasının önüne geçilebilecektir. Yine bebekteki mikroçip, bebeğin tüm tıbbi geçmişinin mikroçipe yüklenmesiyle hangi aşılarını olup olmadığını, ya da daha gelişkin bir mikroçip olduğu düşünülürse vücudunda hangi besin değerlerinin eksik olduğunu gösterebilecektir. Bu tip faaliyetler için oldukça faydalı bir kullanım olsa da mikroçip kullanımının bireyin kendi tasarrufuna bağlı olmasının gerektiğini ve belli bir yaşa geldiğinde kişinin kendi kararıyla enjeksiyon yapılmasını daha doğru bulanlar olacaktır. Eğer mikroçip kullanımı için eğitim ve ehliyet şartı aranacaksa bebekler için bu bahsedilenler söz konusu olmayacaktır.

Yaş şartının yanı sıra sorumluluğun belirlenmesi için belli ehliyete sahip bireylerin mikroçip kullanımına izin verilmesi söz konusu olabilir. Bu durumda hukukumuzda geçerli olan ehliyet şartlarına göre mikroçip kullanımı söz konusu olacaktır. Ancak farklı düzenlemeler de yapılabilir. Kanaatimizce ehliyet şartı, veri güvenliği açısından uygun olacaktır. Kişilere mikroçip kullanımına ilişkin mikroçipin özel kimlik numarasını da içeren bir kullanım kartı da ehliyet olarak verilebilir.

Mikroçip kullanımının yaygınlaşması ile bireylerin bu yönde eğitim alması gerektiği göz ardı edilmemelidir. Bugün hukukumuzda evlenmek, çocuk sahibi olmak gibi önemli faaliyetler için kişinin herhangi bir eğitim alması ya da sertifika, ruhsat gibi belge geçerliliği aranmamaktadır. Ancak kanaatimizce mikroçip kullanımı gibi önemli bir hususta bu durumun kişilere eğitim verilerek sertifika almaları sağlanarak yapılması daha sağlıklı olacaktır. Aksi takdirde doğar doğmaz herkese mikroçip takmanın başka amaçlara da hizmet ettiği düşünülebilir. Bu durum kişileri etiketlemek olarak düşünülebilecektir.

Veri sorumlusu mikroçiplerdeki kişisel verilerin güncelliğinden sorumlu olacaktır[270]. Mikroçiplerdeki verilerin bu nedenle belli periyotlarla (2 yıl-5yıl) veri tabanının sahibi olan veri sorumlusu tarafından güncellemesinin yapılması gerekecektir. Güncellemenin takibini hem veri sorumlusu hem de veri sahibi ilgili kişi yapacaktır. Mikroçip kullanımında ehliyet şartının olduğu durumda bu ehliyetler için de belli aralıklarla güncelleme getirilmesi düşünülebilir. Ehliyetin güncellenmesi aşamalarında mikroçipi kullanan kişinin ehliyet şartlarını taşıyıp taşımadığı tekrardan

[270] Manav, s. 50.

gözden geçirilebilir ve ehliyeti yenilenerek geri verilir ya da iptal edilir. Ehliyet hususuna ilişkin yasal düzenleme devlet eliyle yapılacağı için devlet burada bireyin kişisel verilerinin ihlale uğramasını kişinin kendinden dahi koruyacaktır.

Mikroçiplerdeki kişisel verilerin aracı nitelikte özel şirketler tarafından işleneceği düşünülürse bu şirketler, günümüzdeki operatör şirketlerine benzetilebilir. Birden fazla aracı nitelikte özel şirket olması birden fazla veri tabanı olması anlamına gelecek ve her bir veri tabanı himayesinde bulunduğu veri sorumlusu tarafından korunacaktır. Şirketlerin kişisel verilerin korunmasına ilişkin aldığı önlemler farklılaşacak ve kanuna uygun olup olmadığının ayrı ayrı denetlenmesi gerekecektir. Örneğin aracı nitelikteki bir şirket sadece mikroçiplerdeki bir özel nitelikli kişisel veri türü olan sağlık verilerine ilişkin işleme faaliyeti yapacaksa bu şirketin alması gereken idari ve teknik tedbirler daha fazla, veri güvenliğine ilişkin risk seviyesi ve sorumluluğu daha yüksek olacaktır[271]. Her bir şirket kendi veri koruma politikasını oluşturacak ve mikroçiplerdeki verilerin korunmasından tüzel kişilik olarak tek başına sorumlu olacaktır. Şirketlerde herhangi bir veri sızıntısı olması durumunda kendi tüzel kişilikleri ile kuruma bildirim yapacak, şikayet üzerine veya resen soruşturma yürütülmesi sonucunda verilen yaptırım kararına kendi başına katlanacaktır[272].

Devletin veri tabanı üzerinden mikroçiplerde kişisel veri işleme faaliyetin veri sızıntısına ilişkin sorumluluk devlete ait olacaktır. Bu veri tabanının yürütülmesine ilişkin sorumlu teşkilat veri sızıntısı durumunda idari yaptırım ile karşı karşıya kalacaktır[273].

4.2.4. Yükümlülük

Kişisel verilerin işlenmesinde verileri himayesinde barındıran veri sorumlusunun birtakım yükümlülükleri vardır. Bu yükümlülükler başlıca şunlardır: Kişisel verilerin hukuka uygun olarak işlenmesi, aydınlatma yükümlülüğü, veri güvenliği, kişisel verilerin imhası, sicil kayıt yükümlülükleri ve başvurulara cevap

[271] Özdemir/Yılmaz/Kaya, s. 89.
[272] Korkmaz, (Kişisel Verilerin Korunması) s. 138.
[273] İnan, S. (2021). "Kişisel Verilerin Korunması Kapsamındaki Yaptırımlara Karşı Yargısal Başvuru Yolları: Karşılaştırmalı Bir İnceleme", Kişisel Verileri Koruma Dergisi, C.3, S.2, https://dergipark.org.tr/en/download/article-file/2131340, s. 54.

verme. Veri sorumlusu kişisel veri işleme süreçlerini bu yükümlülüklerine uyarak yürütmelidir[274].

4.2.4.1. Kişisel verilerin hukuka uygun olarak işlenmesi yükümlülüğü ve aydınlatma yükümlülüğü

Kişisel verilerin hukuka uygun olarak işlenmesi için ölçülülüğe uygun ve amaçla sınırlı olması, gerekli rızaların alınması gibi Kanun'da öngörülen şartların yerine getirilmesi gerekmektedir. Bu yükümlülük veri sorumluları ve veri işleyenler için görevleri sona erdikten sonra da devam edecektir[275]. Bunun yanı sıra KVKK harici kanunlarda belirtilen özel hususlar varsa bunlara da uyulmalıdır. Veri sorumlusu verisini işlediği veri sahibi ilgili kişiyi; kimliği, verilerini hangi amaçla işlediği, verilerinin kimlere hangi amaçla aktarılabileceği, kişisel verilerinin toplanma yöntemi ve hukuki sebebi ve hakları konusunda aydınlatmalıdır. Aydınlatma yükümlülüğü en önemli yükümlülüklerden biridir. Aydınlatma yükümlülüğüne uymamanın yaptırımı mevzuatta ayrı olarak düzenlenmiştir[276].

Aydınlatma yükümlülüğünün yerine getirilmesi her ne kadar bir sorumluluk türü olmasa da bir yönden sözleşme öncesi sorumluluk hükümlerine (culpa in contrahendo) benzemektedir. Culpa in contrahendo sözleşme öncesi kusurlu davranıştan bir diğer deyişle sözleşme görüşmelerinden doğan bir sorumluluk türüdür[277]. Bunun gibi aydınlatma yükümlülüğünün de veri işleme faaliyeti öncesinde veya veri işleme anında yerine getirilmesi gerekmektedir. Culpa in contrahendo sorumluluğunda sözleşme görüşmelerinde karşı taraf aydınlatılmalı ve özenli davranılmalıdır[278]. Veri işleme faaliyeti de taraflar arasında bir anlaşma, bir sözleşme olarak kabul edilirse bu durumda veri işleme faaliyetine dair sözleşme açısından culpa in contrahendo hükümleri aydınlatma yükümlülüğü kapsamında değerlendirilecektir. Bir sözleşme ilişkisinde ve sözleşme öncesinde tarafların sözleşme konusuna dair paylaşmış oldukları bilgilerin doğruluğu culpa in contrahendo kapsamında değerlendiriliyor ise veri işleme faaliyetinde de veri işleme amacı, hukuki sebebi, veri aktarımına dair

[274] Mikroçip kullanan ilgili kişiler açısından sicil kayıt yükümlülüğü ve başvurulara cevap verme yükümlülüğü doğmayacağından bu başlık altında yer verilmemiştir.
[275] Korkmaz, (Kişisel Verilerin Korunması) s. 134.
[276] Bkz. Kişisel verileri Koruma Kanunu m.18.
[277] Eren, s. 396.
[278] Oğuzman, K. /Öz, T.(2006). *Borçlar Hukuku Genel Hükümler,* İstanbul, s.321;

yapılan belirlemelerin doğruluğu aydınlatma yükümlülüğü kapsamında değerlendirilecektir. Bu kapsamda karşımıza çıkacak olan "yanıltıcı bilgi"den kaynaklı culpa in contrahendo sorumluluğu aydınlatma yükümlülüğünde eksik yahut hatalı bilgi verilmesi suretiyle veri işleme faaliyetinde de karşılık bulacaktır. Sözleşme öncesi sorumluluktan kaynaklı olarak zarara uğrayan kişinin bu zararı tazmin etme hakkı olabileceği gibi kişisel verilerin işlenmesine ilişkin aydınlatma yükümlülüğünün yerine getirilmemesinden yahut eksik ya da hatalı yerine getirilmesinden kaynaklı zarara uğrayan kişi de bu hakkını tazmin edebilecektir[279].

Aydınlatma yükümlülüğü ahde vefa ilkesine de benzetilebilir. Ahde vefa ilkesi (pacta sund servanda) gereğince sözleşmenin tarafları borçlarına sadık olmalı ve sözlerine bağlı olmalıdır[280]. Aydınlatma yükümlülüğünü yerine getiren veri sorumlusu da aydınlatma yükümlülüğünde beyan ettiği hukuki sebep, amaç ve aktarıma ilişkin hususlarla veri sahibi kişiye karşı bağlı olacaktır. Kişisel verilerin işlenmesinde temel ilkelerden biri olan "işleme amacıyla bağlantılı, sınırlı ve ölçülü olma" ilkesinin temel sonuçlarının biri, veri sorumlusunun işlemiş olduğu kişisel veriyi işlerken var olan veri işleme amacıyla bağlı olduğu ve bu amaç dışında kişisel veriyi kullanamayacağıdır. Aydınlatma yükümlülüğü kapsamında ilgili kişiye bildirilmiş olan veri işleme amacı, veri sorumlusu için veri işleme faaliyeti kapsamında verilen bir söz ve taahhüt hükmündedir. Veri sorumlusu bağlı olduğu bu söz ve taahhüdün dışına çıkamayacak yani veriyi aydınlatma yükümlülüğü kapsamında ilgili kişiye bildirmiş olduğu işleme amacı dışında kullanamayacaktır. Bu durum ahde vefa ilkesi ile aydınlatma yükümlülüğünün ilişkili olduğu anlamını taşımaktadır.

Kişisel veri işleme faaliyetinden sonraki süreçte ise veri sorumlusunun veri sahibine karşı yükümlülüğü "ileriye etkili sadakat yükümlülükleri" ile benzemektedir. İleriye etkili sadakat yükümlülükleri edimin ifasından sonra da borçlunun bazı durumlarda alacaklıya karşı sağlamak zorunda olduğu koruma yükümlülükleridir[281]. Kişisel verilerin işlenmesinde de veri sorumlusu olan kişi gruplarının veri sahibi olan ilgili kişilerin kişisel verileri üzerinde koruma yükümlülüğü bulunmaktadır. Kişisel verilerin güvenliğinin sağlanmasına ilişkin yükümlülükler ileriye etkili sadakat

[279] Arıkan, M. (2009). "Culpa In Contrahendo Sorumluluğu", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 17, S. 1, https://dergipark.org.tr/tr/download/article-file/262715, Erişim: 25.05.2023
[280] Eren, s. 1281.
[281] Eren, s. 1047.

yükümlülükleri kapsamında değerlendirilebilecektir. Veri sahibi kişinin kişisel verilerinin işlenmesi tamamlansa bile veri sorumlusu bu kişisel verileri koruma, saklama ve süresi dolunca imha etmekle yükümlü olmaya devam edecektir.

Mikroçiplerle hukuka uygun veri işleme ve aydınlatma yükümlülüğünün yerine getirilmesi hususunda meydana çıkabilecek sorunların yorumlanmasında Türk Borçlar Hukuku kapsamında yukarıda yapılan benzetme ve ilişkilendirmeler etkili olacaktır.

Mikroçiplerle hukuka uygun veri işleme ve aydınlatma yükümlülüğü mikroçipin enjekte edilmesinden önce yapılmalıdır. Kişi mikroçipi takmadan bu mikroçipteki verilerin hangi veri tabanında tutulacağı, bu veri tabanının detaylı bilgileri, hangi verilerinin işleneceği ve hangi amaçlarla işleneceği, bu verilerinin nerelere aktarılabileceği ve verileriyle ilgili hangi haklara sahip olduğu konusunda aydınlatılmalıdır. Bu bilgilerin bilincinde olarak mikroçip kullanımını kabul etmelidir. Reşit olmayanların mikroçip kullanımı söz konusu olacak ise velileri, kısıtların mikroçip kullanımı söz konusu olacak ise de vasileri bu uygulamaları kabul etmelidir[282].

4.2.4.2. Veri güvenliği yükümlülüğü

Kanunun veri güvenliğine ilişkin 12. maddesine göre veri sorumlusu; "kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak" ile yükümlüdür. Veri sorumlusu veri güvenliğini sağlarken Kişisel Verileri Koruma Kurumu'nun öngördüğü idari ve teknik tedbirlere uymalıdır. Veri sorumluları Kişisel Verileri Koruma Kurulu'nun düzenlemelerinin yanı sıra sektörel bazda ilave tedbirler alabilecektir.

Veri sorumlusunun sadece veri güvenliğine ilişkin tedbirler alması yeterli olmayıp aynı zamanda bu tedbirlerin uygulanması aşamasını denetlemesi veya bir üçüncü kişi aracılığıyla denetimi sağlaması gerekmektedir[283].

Veri güvenliğine ilişkin yapılması gerekenler şirketin barındırdığı kişisel verilerin niteliği, şirketin büyüklüğü gibi faktörler eşliğinde farklılaşabilecektir. Veri

[282] Triplem. (2018). "Would You Microchip Your Kids To Keep Them Safe?", https://www.triplem.com.au/story/would-you-microchip-your-kids-to-keep-them-safe-87113, Erişim: 25.05.2023.
[283] Korkmaz, (Kişisel Verilerin Korunması) s. 134.

sorumluları himayesinde bulundurduğu kişisel veriler için tabi olduğu riskleri değerlendirmeli ve ona göre tedbirler almalıdır.

Kişisel Verileri Koruma Kurulu veri güvenliği kapsamında açıklayıcı olması için Kişisel Veri Güvenliği Rehberi hazırlamıştır[284]. Kurul bu rehberde kişisel verilerin korunması açısından alınması gereken idari ve teknik tedbirleri örnekleyici bir dille anlatmıştır. Veri sorumlusu veri güvenliğinin sağlanması için; kişisel verilerin niteliğine, kişisel verilerin özel nitelikli olup olmadığına, kişisel verilerin bulunması gereken gizlilik seviyesine, güvenlik ihlali olması durumunda ortaya çıkabilecek zararın niteliğini ve niceliğine dikkat etmelidir. Veri sorumlusu bu faktörleri belirleyip sağlamak için plan hazırlığına girişmeli, çözüm alternatifleri üretmeli, maliyet uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirmelidir.

Kişisel verilerin deri altı mikroçiplerle işlenmesinde veri tabanının sahibi olan veri sorumlusu bu sayılan hususları yerine getirmelidir. Veri sorumlusu mikroçip enjekte aşamasında rol alan ve veri tabanı üzerinde tasarruf yetkisi sahibi olan tüm personeline kişisel verilerin korunmasına ilişkin eğitim vermeli ve bu hususta personelde bilinç oluşturmalıdır. Kişisel verilerin hukuka aykırı olarak açıklanması ya da paylaşılması veri güvenliği ihlalini oluşturacağı için veri sorumlusu personelinin bu hususta dikkatli olması önemlidir. Mikroçiplerle kişisel veri işleme faaliyeti devletin veri tabanı kullanılarak gerçekleştirilecekse kamu personellerine, aracı nitelikte özel şirketler tarafından gerçekleştirilecekse şirketin personeline eğitim verilmelidir. Kamu personeli aracılığıyla yürütülecek veri işleme faaliyetinde kişisel veri ile teması olacak personellere uzmanlık şartı koşulabilecektir. Hali hazırda Kurum bünyesinde çalışacak personel için uzmanlık şartı aranmakta, alınacak personel sınava tabi tutulmakta ve uzman yardımcısı olarak göreve başlatılmaktadır. Mikroçiplerle kişisel veri işlenmesinde devlet alt yapısının kullanıldığı ve buna ilişkin ayrı bir idari teşkilat kurulduğunda bu teşkilata personel alımı da bu şekilde gerçekleştirilebilecektir.

Veri sorumlusu, kişisel verilere erişim konusunda personelleri arasındaki yetki ayrımını sağlamalı ve personellerin bu yetki ayrımına riayet etmesini kontrol etmelidir. Veri sorumlusu, kişisel verilerin korunmasındaki idari tedbir olarak personeli ile

[284] Kişisel Verileri Koruma Kurumu. (2018). "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", s. 17, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf, Erişim: 05.01.2022.

"kişisel verilerin korunmasında görev ve gizlilik sözleşmesi" adı altında bir sözleşme imzalayabilir. Personelin kişisel verilerin korunmasına ilişkin kurallara uyması konusunda caydırıcı olacak nitelikte bir disiplin yönetmeliği düzenlenmeli ve personele disiplin yaptırımlarıyla ilgili bilgi verilmelidir. Personele yönelik yapılacak bu düzenlemelerde herhangi bir değişiklik yapılması durumunda bu durum personele bildirilmeli ve alınan idari tedbirlerin güncelliği sağlanmalıdır[285].

Veri sorumlusu kişisel verilerin korunmasına yönelik hazırladığı politikaları iş süreciyle uyumlu bir şekilde hazırlamalı, mevcut risklere ilişkin gerekli önlemleri almalı, yaptığı denetimleri belgeleyerek kişisel verilerin korunmasında sürekli bir gelişim içerisinde olmalıdır. Veri sorumlusu olası veri güvenliği risklerine karşı nasıl hareket edileceğini, hangi personelin risk yönetimi konusunda yetkili olacağını belirlemelidir[286].

Veri sorumlusu aracı nitelikte özel şirketler veya devlet mikroçiplerde yer alan kişisel verilerin korunması için bu sayılan idari tedbirlerin yanı sıra teknik tedbirler de almalıdır. Teknolojinin gelişmesiyle teknolojiyi kötü emelleri için kullananların sayısı artmış ve bu durum siber güvenliğin önemini ortaya koymuştur. Son dönemde birçok şirketin yaşadığı sıkıntı, veri tabanına sızılarak insan kaynakları, muhasebe ve finans gibi departmanların verilerinin bloke edilmesiyle birtakım siber saldırılara maruz kalınması ve bu saldırılar karşılığında ele geçirilen veriler için veri sorumlusu şirketten fidye talep edilmesidir. Bu saldırılar farklı çeşitlerde gerçekleşebilmektedir[287]. Şirketlerin bu tip faaliyetlerle karşılaşması siber güvenlik zafiyetleri bulunması kaynaklıdır.

Mikroçiplerdeki kişisel verileri himayesinde bulunduran şirketlerin böyle bir tehdit altında olması durumunda çok sayıda kişinin kişisel verilerinin ele geçirilmesi ve kötü amaçlar için kullanılması söz konusu olacaktır. Bu nedenle bu şirketlerin teknik alt yapısını güçlendirmesi ve olası tehditlere karşı sürekli tedbir almaları gerekmektedir. Mikroçiplerdeki kişisel veriler devletin tayin ettiği bir idari teşkilat

[285] Kişisel Verileri Koruma Kurumu. (2018). "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", s. 9.
[286] Yücedağ, s. 61.
[287] Gürses B. (2013). "Sosyal Paylaşım Ağlarında Kişisel Verilerin Güvenliği; Sorunlar ve Çözüm Önerileri", BTK İdari Uzmanlık Tezi, s. 34-41.

tarafından barındırıldığı takdirde de gerekli bütün teknik tedbirler idari teşkilat bünyesinde alınmalıdır[288].

İyi bir teknik altyapıda ilk bulunması gerekenler güvenlik duvarı ve ağ geçididir[289]. İnternet üzerinden gelen siber saldırılara ilişkin ilk koruma bu sistemlerden gelecektir. Saldırı kullanılmakta olan internet ağında ilerlemeden güçlü bir şekilde yapılandırılmış bir güvenlik duvarı tarafından engellenebilir. İnternet ağ geçidi ise internet ağı kullanıcılarının sistem için tehdit oluşturan internet sitelerine, uygulamalara ve çevrimiçi servislere erişimini engelleyecektir. Kişisel verilerin güvenliği için hem içeriden oluşabilecek yanlış erişimlere hem de dışarıdan gelebilecek saldırılara ilişkin bu şekilde koruma sağlanabilecektir. Örneğin mikroçipler için veri tabanı hizmeti sunan bir şirkete karşı yapılacak internet ağı saldırısında güvenlik duvarı bu saldırıya karşı korurken internet ağ geçidi ise şirketin çalışanlarından birinin yanlış bir siteye girmesiyle siteden herhangi bir erişimin olmasının önüne geçecektir. Bilhassa sağlık verileri gibi özel nitelikli kişisel verilerin barınabileceği mikroçipler için ciddi siber güvenlik önlemlerinin alınması gerekmektedir[290].

Mikroçip sahibi kişinin internet ağı üzerinden çipteki verilere ulaşabildiği bir uygulama veya internet sitesi tayin edilmesi durumunda bu internet sitesi için de tüm bu bahsedilen teknik tedbirlerin alınması gerekmektedir[291]. İnternet sitesindeki kullanıcı hesabına girişte müşterilerin büyük, küçük harf, rakam ve sembollerden oluşan şifre kullanması konusunda yönlendirici uyarılar bulunmalıdır. Şifrelerin karmaşık olması kaba kuvvet yöntemi ile yani bütün şifre ihtimalleri denenerek çözülmesini zorlaştıracaktır[292]. Kullanıcı hesabına girişte şifre deneme sayısı olmalı örneğin üçten fazla girişte hesap bloke olmalı ve kişinin kimliğini teyit etmesi gerekliliği istenmelidir[293]. Ölüm, ehliyet kaybı, isteğe bağlı veya sair nedenlerle

[288] Küzeci, s. 244; Korkmaz, (Kişisel Verilerin Korunması) s. 136.
[289] Kişisel Verileri Koruma Kurumu. (2018). "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", s.16.
[290] Işık, s. 348.
[291] Aydoğdu, 399.
[292] Gürses, s. 88.
[293] Kişisel Verileri Koruma Kurumu. (2018). "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", s.17.

mikroçip kullanımı sona eren kullanıcıların hesapları sistemden bir an önce silinmelidir.

Teknik altyapının güçlenmesi için kullanılmayan yazılım, uygulama ve servislerin silinmesi gerekmektedir. Güncellenmemiş ve eski sürüm olarak kalmış yazılımlar teknik altyapı için tehdit oluşturmaktadır. Çipteki kişisel verilerin bulunduğu veri tabanı sahibi şirketin çalışanları kişisel verilere erişim de yetki sınırlamasına tabi tutulmalı ve örneğin şirketin çip enjeksiyonu bölümündeki çalışanların müşterilerin kişisel verilerine erişimi bulunmamalıdır[294]. Dışarıdan gelecek tehditlerden korunmak için sistemi sürekli olarak tarayan ve tehlike unsurlarını belirleyebilen antivirüs, antispam ürünleri kullanılmalıdır. Bu uygulamalar kurulumlarının yanı sıra güncel tutulmalıdırlar.

Şirket veri tabanının korunması için getirilebilecek bir diğer koruma ise log kaydı almak olacaktır[295]. Log kaydı çalışanların veri tabanı üzerinde yaptığı değişiklikleri kaydeden bir kayıt türüdür[296]. Bu kayıt türü ile hangi çalışanın sistemde ne değişiklik yaptığı görülebilmektedir. Böylelikle çalışanlar daha dikkatli davranmaktadır. Çalışanların yaptıkları hatalara ilişkin tespit kolaylığı olduğu için sorumlulukları da bellidir. Çalışanların sorumluluklarını belirlemek için bir diğer yöntem ise her bir çalışanın sisteme erişimde kullanıcı adı ve parola kullanması olup departman ayrımının sağlanmasıdır[297]. Örneğin sistem içerisinde insan kaynakları verilerine erişim ile finans verilerine erişim farklı yerden olmalıdır. Bu sayede finans personeli insan kaynakları departmanında bulunan verilere bilhassa kişisel verilere erişemeyecektir. Her bir personel kendi departmanının verilerine sadece kendisine ait olan kullanıcı adı ve parolayı kullanarak girecek ve böylelikle personeller arasında yetki ve erişim kısıtlaması sağlanmış olacaktır[298]. Bu kısıtlama personelin erişiminin gerekmediği kişisel verileri görmesinin önüne geçecek ve böylelikle veri güvenliği temin edilmiş olacaktır[299].

---

[294] Kişisel Verileri Koruma Kurumu. (2018). "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", s.17.
[295] Kişisel Verileri Koruma Kurumu. (2018). "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", s. 18.
[296] Kaya, s.238.
[297] Gündüz, s. 30; Küzeci, s. 244.
[298] Kişisel Verileri Koruma Kurumu. (2018). "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", s. 17.
[299] Gündüz, s. 29; Şimşek s. 96.

Veri sorumlusu kişisel veri içeren ortamların güvenliğini sağlamalıdır. Gerek fiziksel gerek dijital veriler için koruma sağlanmalıdır[300]. Kişisel veriler dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunmalı ve verilerin bulunduğu alana giriş/çıkışlar kontrol altına alınmalıdır. Arşiv odası, sistem odası, kamera kayıt odası gibi yoğun kişisel veri içeren alanların korunması gerekmektedir. Arşiv odası, sistem odası ve kamera kayıt odasındaki kişisel verilerin harici bir mekana veya cihaza yedeklenmesi durumunda bu mekanın ve cihazın ya da cihazların fiziksel güvenliği, kişisel verilerin güvenliği için sağlanmalıdır[301]. Veri sorumlusu kişisel verilerin zarar görmesi, çalınması, silinmesi gibi durumlarda yedeklenen verileri kullanarak işleyişe devam etmelidir[302].

4.2.4.3. Kişisel verilerin imhası yükümlülüğü

Mikroçiplerin veri tabanına sahip olan veri sorumluları kişisel veri işleme süreçlerinde olabildiğince az kişisel veri almaya dikkat etmelidir[303]. Mikroçiplerin kullanılması günlük hayat için kolaylaştırıcı nitelikte olacağı için sadece bu kolaylaşmanın sağlanması için gerekli olan kişisel veriler işlenmelidir. Bunun sağlanması için veri tabanını haiz veri sorumlusu ya da birden fazla olacaksa veri sorumluları için kişisel verilerin korunması alanında gerekli bilgiye sahip olunması gerekecektir. Veri sorumlusu tüm bu süreçlerin uygulanmasını kendisi takip edebileceği gibi kişisel verilerin korunmasında uzman danışmanlık hizmeti verenlerle de çalışabilecektir[304].

Bir senaryoda mikroçip kullanımının her an sonlandırılabilecek bir kullanım türü olması, mikroçipi kullanan veri sahibi ilgili kişinin vefat etmesi, veri sahibi ilgili kişinin mikroçipini kullanamaz hale gelmesi ya da mikroçip kullanma ehliyetini kaybetmesi durumlarında mikroçipteki kişisel veriler aracı nitelikteki şirketlerin himayesinde ise şirket tarafından arşivlenmeli ve güvenli bir ortamda muhafaza

[300] Gündüz, s. 179; Dülger, Kişisel Verilerin Korunması Hukuku, s. 393-394,
[301] Şimşek, s. 96; Kuşkonmaz, s. 116; Küzeci, s. 245; Korkmaz, (Kişisel Verilerin Korunması) s. 136.
[302] Kişisel Verileri Koruma Kurumu. (2018). "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", s. 24.
[303] Kişisel Verileri Koruma Kurumu. "İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık)", https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik-, Erişim: 17.01.2023.
[304] Bizzat bizim uzman danışmanlık verdiğimiz şirketle ilgili detaylı bilgi için: www.odakveri.com adresini ziyaret edebilir ve bizlere ulaşabilirsiniz.

edilmelidir[305]. Bu kullanılmayan verilerin sorumluluğu da veri sorumlusu olan aracı nitelikteki şirkette olacaktır. Şirket bu kişisel verilere ihtiyaç duyulmayacağı yönünde karar verirse şirketin kişisel verileri saklama ve imha politikası uyarınca verileri; Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Yönetmeliğine[306] uygun bir şekilde imha etmesi gerekecektir. Bu yönetmeliğin m.7/3 hükmüne göre İmha işlemlerine ilişkin yapılan tüm faaliyetlerin kayıtları en az üç yıl süreyle saklanmalıdır. Aracı nitelikteki şirketler himayesinde bulundurduğu tüm kişisel verileri analiz etmeli ve imha süreleri gelmiş olanları periyodik aralıklarla imha zamanlarında imha etmelidir. Periyodik imhanın zamanı şirketin kişisel verilerin saklanması ve imhası politikasında belirlenmiş olan zaman olacaktır. Periyodik olarak yapılacak imhaların zaman aralığı, Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Yönetmeliği m.11/2'e göre altı ayı geçemez.

[305] Kara, s. 56.

[306] 28.10.2017 tarihli ve 30224 sayılı Resmi Gazete. "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik", https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm, Erişim: 07.01.2022

5. SONUÇ

Kişinin ayırt edici özelliklerini ifade eden kişisel veri kavramı ve kişisel verilerin korunması maalesef günümüzde halen daha hak ettiği değeri görememiştir. Farkında olmadan paylaşılan kişisel verilerin aleyhe sonuçlar doğuracağı henüz veri sahibi ilgili kişiler tarafından anlaşılamamıştır. Tarih boyunca bu bilincin oluşması ve kişisel verilerin korunması için ülkelerde bu konuya ilişkin düzenlemeler ve denetimler yapan veri koruma otoriteleri kurulmuştur. Veri koruma otoriteleri kendi ülkelerindeki kişisel verilerin korunması, kişisel verilerin korunması süreçlerinin nasıl yürütüleceği, bireylerin ve kuruluşların nasıl hareket etmesi gerektiği, alınması gereken tedbirler ve ihlaller halindeki uygulanacak yaptırımlar gibi hususlarda yol gösterici olmuşlardır.

Yeni bir düzenleme olması nedeniyle halen uygulamada sorunlarla karşılaşılabilen kişisel verilerin korunmasına uyumluluğu artırabilmek için çalışmalara devam edilmesi gerekmektedir. Bireylerin kişisel verilerinin ele geçirilmesi nedeniyle uğradığı zararlar minimize edilmeli ve bu tip eylemlerin yaptırımlarının artırılması gerekmektedir. Kişinin kişilik hakları, mülkiyet hakkı, fikri haklar gibi mutlak hakları açısından doğrudan veya dolaylı olarak kişisel verilere veri sahibinin rızası hilafına ulaşılması durumunda hak kaybı yaşamaması için gerekli önlemler alınmalıdır.

Kişisel Verileri Koruma Kanununa uyum süreçlerinde kişinin verilerinin korunması bazı yönleriyle Türk Borçlar Hukuku çerçevesinde hakların korunmasına da benzemektedir. Örneğin sözleşme öncesi sorumluluk olarak da bildiğimiz culpa in contrahendo sorumluluğu Kişisel Verileri Koruma Kanununda yer alan aydınlatma yükümlülüğüne benzemektedir. Sözleşme öncesi tarafların birbirini aydınlattığı gibi veri işleme süreçlerinde de taraflar birbirini aydınlatmalıdır. Yine kişisel verisinin rızası dışında işlenmesi halinde ya da kişisel verileri ile ilgili veri sorumlusunun veri güvenliği sağlayamaması durumunda zarara uğrayan kişi Türk Borçlar Hukuku kapsamında haksız fiil hükümlerine dayanarak zararını talep edebilecektir.

Teknolojinin getirdiği yeniliklerle birlikte yeni yasal düzenlemelerin yapılması gereksinimi duyulmakta ya da mevcut yasal düzenlemelerde değişiklikler yapılmaktadır. Bu çalışmanın konusunu oluşturan mikroçip kullanımının yaygınlaşması da şüphesiz buna yol açacaktır. Bu çalışmada mikroçip kullanımının yaygınlaştığı durumda kişisel veri akışının nasıl olacağına, uyulması gereken kurallara

ve yasal düzenlemelere ilişkin neler yapılabileceğine yönelik önerilerde bulunulmuştur. Hem kamu hukuku hem de özel hukuk boyutunda değişiklikler yapılması gerekecektir. Mikroçiplerle hukuka uygun veri işleme ve aydınlatma yükümlülüğünün yerine getirilmesi hususunda meydana çıkabilecek sorunların yorumlanmasında Türk Borçlar Hukuku kapsamında yukarıda yapılan benzetme ve ilişkilendirmeler etkili olacaktır.

Kişilerin ve kuruluşların mikroçiple kişisel verilerin işlenmesinde yasal mevzuata ve düzenlemelere uyulması yönünde önerilerde bulunduğumuz bu çalışmada mikroçiplere ilişkin farklı senaryolar üzerinden değerlendirmeler yapılmıştır. Üzerinde durulması ve karar verilmesi gereken ilk süreç mikroçiplerdeki kişisel verilerin devlet veri tabanı ile mi yoksa aracı nitelikteki özel şirketlerin sunacağı veri tabanı hizmeti ile mi sağlanacağıdır. Çalışmada her iki senaryoya göre de çıkarımlarda bulunulmuş ve kişisel verilerin korunması için alınması gereken idari ve teknik tedbirlere yönelik bilgilendirme yapılmıştır.

Kanaatimizce mikroçiplerdeki kişisel verilerin devlet veri tabanı hizmeti ile işlenmesi gerekmektedir. Bu şekilde doğruluğu ve güncelliği gibi birçok açıdan hem mikroçiplerin kullanım alanlarında hem de mikroçipleri kullanan kişiler açısından güvenilirlik sağlanmış olacaktır. Ancak burada şunu belirtmekte fayda vardır. Günümüzde birçok hizmet artık özel şirketler aracılığıyla yürütülmektedir. Gerçekten de devletin bireyler üzerindeki otoritesi ve etkisi azalmıştır. İlk çıkışından bu yana mikroçipleri devletin bir izleme aracı olarak kullanması kaygısı önemini yitirmiştir. Çünkü cebimizdeki cep telefonları, bilgisayarlar ve internete bağlanan herhangi bir cihazdan yaptığımız faaliyetleri devletten çok özel şirketler menfaatleri için takip etmektedir. Bu denli izlendiğimiz bir teknolojide mikroçiplerle izleme fikri oldukça geri planda kalmaktadır. Bu sebeple kullandığımız internete bağlı herhangi bir cihaz bize ilişkin verilerin internet ortamına yayılmasına aracı olmaktadır.

İnternet ortamında yayılan kişisel verilere ilişkin kişilerin daha bilinçli olması, kişisel verilerin paylaşılması ile uğrayabileceği zararları bilmeleri ve kişisel verileri üzerindeki haklarını bilmeleri ile mümkün olabilecektir. Özellikle mikroçip teknolojisi ile veri paylaşımı başladığı takdirde kişilerin kimlik kartlarında yer alan çiple birçok verisini paylaşabileceği bir durumun söz konusu olması halinde devletin vatandaşlarının güvenliği için de vatandaşlarını bilinçlendirmesi gerekecektir. Bu

bilinçlendirme sürecinde Kişisel Verileri Koruma Kurumu'nun rolü büyük olacak ve hatta bu husus da özel danışmanlık şirketleriyle, danışmanlarla da anlaşılabilecektir.

Mikroçip kullanımında da dikkat edilmesi gereken bireylerin izlenmesi ya da takip edilmesi ihtimali değildir. Üstelik çalışmamızda da bahsettiğimiz gibi günümüzde kullanılan mikroçipler henüz böyle bir teknolojiye sahip değildir. Her alanda olduğu gibi öncelikle bireyin kişisel verinin ne olduğu, kişisel veri aktarımının ve paylaşımının ne şekilde olabileceği ve kişisel verilerin korunması alanında eğitilmesi şarttır. Kanaatimizce yeterli bilince sahip toplumlar için mikroçip kullanımı izlenme ya da takip edilme endişesini taşımaktan çok hayatı kolaylaştıracak bir unsur haline dönecektir.

Devletler tarafından kişisel verilerin korunması alanındaki yasal düzenlemelerin artırılması, bu alandaki denetimin sıklaştırılması ve yaptırımların uygulanması ile gerekli bilinç yerleştirilerek yaşanabilecek tüm zararların önüne geçilebilecek ve mikroçip kullanımı da yaygınlaşarak kişilerin bir kimlikle birçok işlemi yapabilmesinin önü açılacaktır.

KAYNAKLAR

Açıkgöz A.N. (2005). "Gerekçeli-Karşılaştırmalı Ve Açıklamalı Yeni Türk Ceza Kanunu", Van, http://www.ceza-bb.adalet.gov.tr/makale/187.doc, Erişim:08.08.2021.

Akgül A. (2014). *Danıştay ve İnsan Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta Yayıncılık*, İstanbul.

Aksoy H.C. (2010). *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, 1. Bası, Çakmak Yayınevi, Ankara.

Akkurt, S.S. (2020). "Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", Kişisel Verileri Koruma Dergisi, C. 2, S. 1.

Anı N. A. (2018). *Kişisel Verilerin İşlenmesi ve Açık Rıza*, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Arıkan, M. (2009). "Culpa In Contrahendo Sorumluluğu", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 17, S. 1, https://dergipark.org.tr/tr/download/article-file/262715, Erişim: 25.05.2023

Ari, J. (2005). "RFID Security and Privacy: A Research Survey", RSA Laboratories, 5-11, https://www.researchgate.net/publication/3236246_RFID_security_and_privacy_A_research_survey, Erişim: 06.05.2022.

Aşıkoğlu, İ.Ş. (2018). Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri. İstanbul Üniversitesi Hukuk Fakültesi Özel Hukuk Yüksek Lisans Tezleri Dizisi No:5, İstanbul, On İki Levha Yayıncılık.

Avcıoğlu N.H. (2018). *Türk Hukukunda Kişisel Verilerin Korunması Hakkı*, Yayımlanmamış Yüksek Lisans Tezi, Konya.

Avrupa Konseyi. "Convention108+:The Modernised Version Of A Landmark Instrument", https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108, Erişim:10.08.2021.

Aydın, U. (2002). İş Hukukunda İşçinin Kişilik Hakları, Eskişehir.

Aydoğdu Y. (2022). "Mobil Uygulamalarda Kişisel Verilerin İşlenmesi ve Yasal Olarak Dikkat Edilmesi Gereken Hususlar", Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, C. XXVI, Y.2022, Sa. 1, s. 399, https://dergipark.org.tr/tr/download/article-file/2222163, Erişim:12.09.2022.

Ayözger A.Ç. (2016). *Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması*, Yayımlanmamış Doktora tezi, İstanbul.

Badur E./ Kurt Konca N. (2022). "Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini Ve Görevli Mahkeme", İnönü Üniversitesi Hukuk Fakültesi Dergisi, C.13, S.2, 476-490, s. 482, https://dergipark.org.tr/en/download/article-file/2585121, Erişim:22.12.2022.

Başalp N. (2004). *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınları, Ankara.

Bayındır, H. (2019). *Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması,* Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Birleşmiş Milletler Genel Kurulu. (1990). "Guidelines fort he Regulation of Computarized Personal Data Files", http://www.refworld.org/pdfid/3ddcafaac.pdf, Erişim:10.08.2021.

Boz A. (2014). *Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri*, Yayımlanmamış Yüksek Lisans Tezi, Ankara.

Bozkurt Yüksel E. (2015). "Nesnelerin İnternetinin Hukuki Yönden İncelenmesi", D.E.U. Hukuk Fakültesi Dergisi, Cilt: 17, Sayı: 2, https://www.academia.edu/32452815/Nesnelerin_%C4%B0nternetinin_Hukuki_Y%C 3%B6nden_%C4%B0ncelenmesi_Looking_at_IoT_from_Legal_Perspective?email_work_card=view-paper, Erişim:03.01.2022.

By Michelson Found Animals Foundation. "5 Things You Didn't Know About Microchips", https://www.foundanimals.org/5-things-didnt-know-microchips/, Erişim: 05.12.2022.

Carey P. (2018). Data Protection Principles, "Data Protection: A Practical Guide to UK and EU Law", 5. Bası, Oxford, Oxford University Press.

Chadwick, L./ Wasserman, R. (2021). "Will microchip implants be the next big thing in Europe?", https://www.euronews.com/next/2020/05/12/will-microchip-implants-be- the-next-big-thing-in-europe, Erişim:12.12.2021.

Çekin, M. S. (2018). *6698 Sayılı Kişisel Verilerin Korunması Kanunu*, İstanbul: Oniki Levha Yayınevi.

Çelik, Y. (2017). "Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı", TAAD, Yıl. 8, Sayı.

Coldiron R. (2021). "Here's How to Update Your Pet's Microchip Information" , https://www.marthastewart.com/8136232/how-update-pet-microchip-information#:~:text=Visiting%20the%20Registry's%20Site,information%20or%20call%20the%20registry. Erişim: 02.02.2022.

Dede, R. (2022). Kişisel Verilerin Korunması Kanunu Bakımından Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati, Altınbaş Üniversitesi Lisansüstü Eğitim Enstitüsü Kamu Hukuku Yüksek Lisans Tezi.

Demirezen, M. (2020). *Kişisel Verilerin Korunması Hukuku ve Uyum Projelerinin Yürütülmesi*, Platon Yayıncılık, İstanbul.

Develioğlu, H.M. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü*, İstanbul: Oniki Levha Yayınevi.

Devlet Denetleme Kurulu (DDK). *"Kişisel Verilerin Korunmasına İlişkin Ulusal Ve Uluslararası Durum Değerlendirmesi İle Bilgi Güvenliği Ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları Denetleme Raporu"*, No:3, http://www.kisiselsaglkverileri.org/icerik/dosyalar/denetleme_rpr.pdf, Erişim:12.12.2021.

Dinkci, F. (2014). *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye Örneği,* Yayımlanmamış Yüksek Lisans Tezi, Samsun.

Dülger, M.V.(2020). *Kişisel Verilerin Korunması Hukuku* (*Kişisel Verilerin Korunması Hukuku)*, 3. Baskı, Hukuk Akademisi, İstanbul.

Dülger. M.V. (2016). "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, C.3, S.2, 101-167.

Eltorai, A./ Fox H./ McGurrin, E./ Guang, S. (2016). "Microchips in Medicine: Current and Future Applications", https://www.hindawi.com/journals/bmri/2016/1743472/, Erişim:08.10.2021.

Erarslan, S. (2020). *Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller*, 2. Baskı, Oniki Levha Yayıncılık A.Ş, İstanbul.

Erdinç, G.H. (2017). *Bilgi Güvenliği, Kişisel Verilerin Korunması Ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler.* Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Erdinç, G.H. (2020). "Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi", Kişisel Verileri Koruma Dergisi, Cilt: 2, Sayı:1.

Eren, F. (2015). *Borçlar Hukuku Genel Hükümler*, 19. Baskı, Yetkin Yayınları, Ankara.

Ersoy, U. (2009). *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tez, Ankara.

Esmer, Ö. (2011). "RFID Teknolojisinde Veri Güvenliğinin Sağlanması İçin Melez Şifreleme Algoritmasının Uygulanması", Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara.

European Commission. "What is Personal Data?", https://ec.europa.eu/info/law/law-topic/data- protection/reform/what-personal-data_en, Erişim: 05.05.2021.

European Union Agency for Network and Information Security. (2016). Cyber Security and Resilience of Intelligent Public Transport, *"Good Practices and Recommendations"*, s. 50, https://www. enisa .europa.eu/ publications/good-practices- recommendations, Erişin:04.01.2022.

European Union Agency for Fundamental Rights and Council of Europe. (2018). "Hanbook of European Data Protection Law", Luxembourg: Publications Office of the European Union. http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition, Erişim:22.12.2022

Farra, R./Sheppard, N./ Langer, R./MCcabe, L./ Neer, R./ Anderson, J./ Santini, J./Cima, M. (2012). "First-in-Human Testing of a Wirelessly Controlled Drug Delivery Microchip", Science Translational Medicine, https://www.science.org/doi/10.1126/scitranslmed.3003276, Erişim:07.10.2021.

Francis, L.P./Francis, J.G. (2017). *"Privacy What Everyone Needs To Know"*, New York, Oxford University Press.

Gündüz, M.Ş. (2022). T.C. Batman Üniversitesi Lisansüstü Eğitim Enstitüsü Siyaset Bilimi Ve Uluslararası İlişkiler Anabilim Dalı, Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği Yüksek Lisans Tezi.

Güneş Peschke/ Peschke. (2013). "Protection Of The Mediatized Privacy In The Social Media: Aspects Of The Legal Situation In Turkey And Germany", Gazi Üniversitesi Hukuk Fakültesi Dergisi, C.XVII, Y.2013, Sa. 1-2, s. 867, https://dergipark.org.tr/tr/download/article-file/789306, Erişim:27.01.2023.

Gür, İ. (2009). *Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları,* Yayımlanmamış Yüksek Lisans Tezi, Ankara.

Gürses, B. (2013). *Sosyal Paylaşım Ağlarında Kişisel Verilerin Güvenliği; Sorunlar ve Çözüm Önerileri,* BTK İdari Uzmanlık Tezi.

Güven, V. (2016). *Sağlık Hukukunda Tıbbi Kayıtların Tutulmasından ve Saklanmasından Doğan Sorumluluk*, Ankara, Adalet Yayınevi.

Göçmen Uyarer, S. (2019). *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması,* Seçkin Yayıncılık, Ankara.

Grauer, Y. (2018). "A practical guide to microchip implants", Arstechica, https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/, Erişim:15.10.2021.

Hakeri, H. (2019). *Sağlık Hukuku*, 2.Baskı, Seçkin Yayıncılık, Ankara.

Henkoğlu, T./Yılmaz, B. (2013). "Avrupa Birliği(AB) Bilgi Güvenliği Politikaları-European Union(EU) Information Security Policies", Türk Kütüphaneciliği Dergisi, C.XXVII, No:3, s.451-741, http://www.tk.org.tr/index.php/TK/article/view/384/377, Erişim: 17.10.2021.

Hilbert, M. (2013). "Big Data for Development: From İnformation to Knowledge Societes", United Nations ECLAC.

Işık, O. (2022). "Kişisel Verilerin Korunması Kanunu Kapsamında Veri Sorumlusu Olarak Sosyal Güvenlik Kurumu", Erciyes Üniversitesi Hukuk Fakültesi Dergisi , 17 (2) , 263-362, https://dergipark.org.tr/tr/pub/eruhfd/issue/73314/1195339.

İnan, S. (2021). "Kişisel Verilerin Korunması Kapsamındaki Yaptırımlara Karşı Yargısal Başvuru Yolları: Karşılaştırmalı Bir İnceleme", Kişisel Verileri Koruma Dergisi, C.3, S.2, https://dergipark.org.tr/en/download/article-file/2131340.

Jones C. (2023). "4 Thıngs That Wıll Defıne Government Data Storage In 2023 And Beyond", https://redriver.com/storage/government-data-storage, Erişim:02.02.2023.

Kara, İ. (2019). "Dijital Verilerin İmha Süreçlerinin Tanımlanması Ve Uygulama Yönünden Değerlendirilmesi", https://dergipark.org.tr/tr/download/article-file/901385, Erişim: 12.12.2022.

Kaya, M. (2015). Elektronik Ortamda (Elektronik Haberleşme-İnternet-Sosyal Medya) Kişilik Hakkının Korunması, Ankara, Seçkin Yayıncılık.

Kaya, C. (2011). "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas(Kişisel) Veriler ve İşlenmesi", İÜHFM, C.LXIX, No:1-2, http://dergipark.gov.tr/download/article- file/97634, Erişim:07.07.2021.

Kaya, M.B./Taştan F.G. (2018). *Kişisel Veri Koruma Hukuku*, 1.Baskı, Oniki Levha Yayıncılık A.Ş..

Kardo, K.İ./ Arnab, P./ Nicolai, O. (2019). "Adoption Of Human Microchip Implants For Business Organizations" Aalborg University, Doktora Tezi, https://projekter.aau.dk/projekter/en/studentthesis/adoption-of-human-microchip- implants-for-business-organizations(4ae5f3a0-db6c-476d-b904-d040559227d4).html, Erişim: 12.10.2021.

Kelner M. (2017). "Call for athletes to be fitted with microchips in fight against drug cheats" https://www.theguardian.com/sport/2017/oct/10/call-for-athletes-to-be-fitted-with-microchips-fight-against-drug-cheats, Erişim: 15.10.2021.

Keskin, D. (2022). Bizzat Karar Verme Hakkı, Adalet Yayınevi, Ankara.

Korkmaz, İ. (2016). (Kişisel Verilerin Korunması), "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", Türkiye Barolar Birliği Dergisi (124), http://tbbdergisi.barobirlik.org.tr/m2016-124-1571, Erişim: 12.05.2023.

Korkmaz, İ.(2019). *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, 2.Basım, Ankara.

Kuner, C. (2007). "Europen Data Protection Law: Corporate Compliance and Regulation, Second Edition", Oxford, Oxford University Press, kn.2.30.

Kuntoğlu, Ö.F. (2021). "Elektronik Ticarette Kişisel Verilerin Korunması". Bilişim Hukuku Dergisi 3, no: 1, 176-229.

Kuşkonmaz E. M. (2013). Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Yüksek Lisans Tezi, İstanbul.

Küzeci, E. (2019). *Kişisel Verilerin Korunması*, 3.Baskı, Turhan Kitabevi, Ankara.

Lambert, P.B. (2017). "The Data Protection Officer: Profession, Rules and Role", New York, CRC Press Taylor&Francis Group.

Latham, K. (2022). "The microchip implants that let you pay with your hand", https://www.bbc.com/news/business-61008730, Erişim: 04.11.2022.

Lily, M. (2018). "Sydney Bio-Hacker Who İmplanted Opal Card İnto Hand Fined For Not Using Valid Ticket" , https://www.abc.net.au/news/2018-03-16/opal-card-implant- man-pleads-guilty-transport-offences/9555608, Erişim:11.10.2021.

Lohrmann D. (2023). "From Progress to Bans: How Close Are Human Microchip Implants?", https://www.govtech.com/blogs/lohrmann-on-cybersecurity/from-progress-to-bans-how-close-are-human-microchip-implants, Erişim: 20.03.2023

Manav, Eda A. (2015). "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", Gazi Üniversitesi Hukuk Fakültesi Dergisi C.XIX, Y.2015, Sa. 2, s. 97. https://dergipark.org.tr/tr/download/article-file/789086, Erişim: 04.04.2022.

Molly, M. (2007). "Human-İmplantable RFID Chips: Some Ethical And Privacy Concerns", Healthcare IT News, https://www.healthcareitnews.com/news/human-implantable- rfid-chips-some-ethical-and-privacy-concerns, Erişim:11.10.2021.

Nadezhda, P. (2009). "Property Rights in Personal Data: Learning from the American Discourse", Computer Law & Security Review, Vol.25, No.6.

Oğuz, S. (2018)."Kişisel Verilerin Korunması Hukukunun Genel İlkeleri", Bilgi Yönetimi ve Ekonomi Dergisi, C.13, S.2, 121-138.

Oğuzman, K. /Öz, T.(2006). *Borçlar Hukuku Genel Hükümler,* İstanbul.

Oğuzman, M.K./Barlas, N. (2018). *Medeni Hukuk*, 24.Bası, Vedat Kitapçılık, İstanbul.

Oğuzman, M.K./Seliçi, Ö./Oktay-Özdemir, Ş. (2018). *Kişiler Hukuku (Gerçek ve Tüzel Kişiler)*, 17. Basım, Filiz Kitabevi, İstanbul.

Orak, B. (2019). *Kişisel Sağlık Verilerinin Korunması,* Yetkin Yayınları, Ankara.

Ömür, R. (2018). "Kişisel Sağlık Verilerinin Korunması ve Hastanelerin Sorumluluğu", YÜHFD, C.XV, No:1, s. 133-180, http://law.yeditepe.edu.tr/sites/default/files/yuhf_dergisi_v.14.pdf, Erişim:09.10.2021.

Özdemir, H.(2009). *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması,* Seçkin Yayıncılık.

Özdemir, M./Yılmaz, M./Kaya, H. (2022). "Kişisel Sağlık Verilerinin 6698 Sayılı Kanun Çerçevesinde Korunması", 19 Mayıs Sosyal Bilimler Dergisi, C.3, S.1, 85-96, dergipark.org.tr/tr/pub/19maysbd.

Özer Deniz, M. (2020). "İşçilerin Özel Nitelikli Kişisel Verilerinin Korunması Ve Bundan Doğan Sorumluluk", Türkiye Adalet Akademisi Dergisi, Yıl:12, S. 45, 355-378.

Privacy Internatiol. (2018). "The Keys to Data Protection:A Guide For Police Engament on Data Protection", United Kingdom, https://privacyinternational.org/sites/default/files/2018-03/Data%20Protection%20COMPLETE.pdf, Erişim: 15.10.2021.

Peppet, S. (2015). "Regulating the Internet of things: First Steps Toward Managing Discrimination, Privacy, Security and Consent", Texas Law Review, https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf, Erişim:03.01.2022.

Phil, Z.,(2005). "The Basics of Crytography ", An Introduction to Cryptography, 1-3.

Polater, S. (2019). "Kişisel Verilerin Reklam Amaçlı İşlenmesinde Hukuka Uygunluk Sebepleri", Kişisel Verileri Koruma Dergisi, Cilt:1, Sayı:1.
Pontius N. (2023). "What is RFID? Types of RFID Tracking Tags, Their Uses, Disadvantages and How They Compare to Barcode Labels", https://www.camcode.com/blog/what-is-rfid/, Erişim: 16.03.2023.
Prescott, J./Lipka, S./ Baldwin, S. (2006). "Chronic, Programmed Polypeptide Delivery From An İmplanted Multireservoir Microchip Device", Nature Biotechnolohy, https://www.nature.com/articles/nbt1199, Erişim: 08.10.2021.
Ryan, P. (2021). "Future of healthcare: microcihp implants and no trips to the doctor by 2050", https://www.thenationalnews.com/uae/health/future-of-healthcare-microchip- implants- and-no-trips-to-the-doctor-by-2050-1.1248262, Erişim: 17.10.2021.
Saka, R./Çağlayan, R./Koca, M. (2020). *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası,* Seçkin Yayıncılık, Ankara.
Samuelson, P. (1999). "Privacy as Intellectual Property", Stanford Law Review, Vol. 52, https://www.jstor.org/stable/1229511, Erişim: 08.08.2021.
Sarıusta, K. (2018). *Kişisel Verilerin Ceza Hukuku Yoluyla Korunması*, Yayımlanmamış Yüksek Lisans Tezi, Gaziantep.
Saygı, S. (2020). "6698 Sayılı Kanun'un Sistematiğinde Yargısal Başvuru Yolları", Kişisel Verileri Koruma Dergisi, C.2, S.2, https://dergipark.org.tr/tr/download/article-file/1106037, Erişim:25.04.2023
Schwartz, P.M. (2004). "Property, Privacy, And Personal Data", Harvard Law Review.
Schwartz, O. (2019). "The rise of microchipping: are we ready for technology to get under the skin?", https://www.theguardian.com/technology/2019/nov/08/the-rise-of-microchipping-are-we-ready-for-technology-to-get-under-the-skin, Erişim:11.10.2021.
Selvan, E. (2023). Veri Diplomasisi Ve Uluslararası Veri Güvenliği Politikaları, T.C. Milli Savunma Üniversitesi Atatürk Stratejik Araştırmalar Ve Lisansüstü Eğitim Enstitüsü Stratejik İletişim Anabilim Dalı Stratejik İletişim Programı Yüksek Lisans Tezi.
Serozan, R. (2018). Medeni Hukuk-Genel Bölüm: Kişiler Hukuku, 8. Basım, Vedat Yayıncılık, İstanbul.
Şeşen, Y./Kuzcuoğlu, A.H. (2021). Veri ve Bilgi Güvenliği Bağlamında İstihbarat Faaliyetleri, Lamre Journal, C.2, S.2.
Sevimli, A. (2006). *İşçinin Özel Yaşamına Müdahalenin Sınırları,* İstanbul.
Süzek, S. (2018). *İş Hukuku,* İstanbul.
Sharma, S./Nijdam, A./Sinha, P. (2006). "Controlled-release Microchips", https://www.tandfonline.com/doi/full/10.1517/17425247.3.3.379, Erişim:08.10.2021.
Şimşek, O.(2008). *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta Basım.
Singh, A. (2016). "Protecting Personal Data As A Property Right", ILI Law Review, Winter Issue.
Stephen, S./ Penny, T. (2018). "The technology getting under your skin: Swedish biohacker says bio-implants movement growing globally" News, https://www.abc.net.au/news/2018- 08-28/swedish-biohacker-says-bio-implants- movement-growing-globally/10170326, Erişim:10.10.2021.
Türkiye Büyük Millet Meclisi (TBMM). "Kişisel Verilerin Korunması Kanunu Tasarısı/1/541) ve Adalet Komisyonu Raporu",

https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf, Erişim:02.02.2022.
Todd, L. (2007). USAToday, "Microchips İn Humans Spark Privacy Debate", https://usatoday30.usatoday.com/tech/news/surveillance/2007-07-21-chips_N.htm, Erişim:11.10.2021.
Toğuz, Ö. (2010). *Data Protection and Intellectual Property in the EU and Turkey,* Middle East Univerty, Unpublished Gratuate Thesis, Ankara.
Tükel, R. "Kişisel Sağlık Verileri Korunmalıdır!", http://www.tipdunyasi.dr.tr/2017/06/kisisel-saglik-verileri-korunmalidir/, Erişim:02.02.2022.
Tüylek, Z. (2017). "İlaç Taşıyıcı Sistemler Ve Nanoteknolojik Etkileşim", İnönü Üniversitesi Elektronik ve Otomasyon Bölümü Biyomedikal Teknolojisi, Bozok Tıp Dergisi 7(3); 89-98, s. 90, http://tipdergisi.bozok.edu.tr/dosyalar/Eylul2017/95-104.pdf, Erişim:11.10.2021.
Uçak, M. (2021). "Kişisel Verilerin Ölümden Sonra Korunması", İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi, C. VI, S. 10.
Uncular, S. (2018). "Kişisel Verilerin Korunması Kanunu ve AB Genel Veri Koruma Tüzüğü Kapsamında İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", Seçkin Yayıncılık, Ankara.
Uygun, M. (2010). "Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Koruması", Yayımlanmamış Yüksek Lisans Tezi, Ankara.
Üstün Türkoğlu Kamile. (2021). "Güvenlik Soruşturmalarında Kişisel Verilerin Korunması", Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi C. XXV, Y.2021, Sa. 2, s. 807, https://dergipark.org.tr/tr/download/article-file/1754338, Erişim: 06.06.2022.
Voigt, P./ Bussche, A. (2017). "The EU General Data Protection Regulation (GDPR): A practical Guide", Switzerland, Springer.
Yürük, Z. (2023). Kişisel Verilerin İhlalinden Doğan Özel Hukuk Sorumluluğu, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı Tezli Yüksek Lisans.
Yücedağ N. (2019). "Kişisel verilerin korunması kanunu kapsamında genel ilkeler", Kişisel Verileri Koruma Dergisi, C.1, S.1, https://dergipark.org.tr/tr/download/article-file/737938, Erişim: 08.10.2021.
Wang, M./Jiang, Z. (2017). "The Defining Approaches and Practical Paradox of Sensitive Data:An İnvestigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World", İnternatiol Journal of Communication, No:11, Çin, http:// ijoc.org/index.php/ijco/article/viewFile/6892/2111, Erişim:07.07.2021.
Zaki, M./Patil, S./Baviskar, D./Jain, D. (2012). "Implantable Drug Delivery System: A Review", department of Pharmaceutics, Institute of Pharmaceutical Education, https://sphinxsai.com/2012/pharm/pharm/pt=40(280-292)jm12.pdf, Erişim:05.10.2021.
Zor S. (2014). "Bir Mikroçipim Olsa: RFID", Açık Bilim, http://www.acikbilim.com/2014/10/dosyalar/bir-mikrocipim-olsa-rfid.html, Erişim:11.10.2021.

Yararlanılan İnternet Kaynakları

AVMA. "Microchipping FAQ", https://www.avma.org/resources-tools/pet-owners/petcare/microchips-reunite-pets-families/microchipping-faq, Erişim: 11.09.2020.

Berqnet. "NFC Nedir? Nasıl Çalışır? Kullanım Alanları Nelerdir?" https://berqnet.com/blog/nfc, Erişim: 10.10.2022

Bilim ve Gelecek. (2017). "Sürekli sağlık gözlemi yapan mikroçip", https://bilimvegelecek.com.tr/index.php/2017/07/01/surekli-saglik-gozlemi-yapan- mikrocip/, Erişim:05.06.2022.

Biohackinfo, "The world's first implantable vaccine passport is here and it can monitor pandemics in real time", https://biohackinfo.com/news-dsruptive-temperature-microchip-implant/, Erişim: 12.10.2021.

Cambrige Dictionary. "Orwellian", https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/orwellian, Erişim: 11.11.2021

CNN Edition. "Forget wearable tech, embeddable implants are already here", http://edition.cnn.com/2014/04/08/tech/forget-wearable-tech-embeddable-implants/index.html, Erişim: 12.10.2021.

Cumhuriyet Haber. "Elon Musk'ın 'Beyin Çipi' Projesi Bir Maymun Üzerinde Test Edildi", https://www.cumhuriyet.com.tr/haber/elon-muskin-beyin-cipi-projesi-bir-maymun- uzerinde-test-edildi-1827168, Erişim: 06.06.2021.

Dangerous Things. https://dangerousthings.com/, Erişim:10.10.2021; BraveNewCoin. "Biohacking: Implants That Can Store A Private Key", https://bravenewcoin.com/insights/biohacking-implants-that-can-store-a-private-key, Erişim: 10.10.2021.

Dangerous Things. "X-Series Implantable Transponder FAQ", https://forum.dangerousthings.com/t/x-series-implantable-transponder-faq/28#faq- checkpoints, Erişim: 10.10.2021.

Dsruptive Subdermals. "Biohackinfo News (English)", https://dsruptive.com/media/ , Erişim: 12.10.2021.

Dünya Haber. "3 Bin İsveçli Neden Çip Takıyor?", https://www.dunya.com/sektorler/teknoloji/3-bin-isvecli-neden-cip-takiyor-haberi- 425296, Erişim: 12.12.2021.

Euronews. "Robotlar insanları işsiz mi bırakacak yoksa yeni iş imkanları mı yaratacak?" https://tr.euronews.com/next/2022/06/22/robotlar-insanlari-issiz-mi-birakacak-yoksa-yeni-is-imkanlari-mi-yaratacak., Erişim: 10.10.2022.

Forbes. (2022). "Chip Shot", https://www.forbes.com/forbes/2002/1223/076.html?sh=3b52aa1d11ee, Erişim: 01.10.2021.

Fortune Business Insights. (2023). The global digital transformation market is projected to grow from $2.27 trillion in 2023 to $8.92 trillion by 2030, at a CAGR of 21.6% during the forecast period... Read More at:- https://www.fortunebusinessinsights.com/digital-transformation-market-104878, Erişim: 17.03.2023.

Hürriyet. (2019). "Tamamen silinmesi istenen verinin üzerine yeni veri yazılmalı", https://www.hurriyet.com.tr/teknoloji/tamamen-silinmesi-istenen-verinin-uzerine-yeni-veri-yazilmali-41108551, Erişim: 19.12.2022.

Hürriyet. (2020). “Bilgilerinizin Dark Web üzerinden satışa çıkarıldığını nasıl anlarsınız?”, https://www.hurriyet.com.tr/teknoloji/bilgilerinizin-dark-web-uzerinden-satisa-cikarildigini-nasil-anlarsiniz-41625223, Erişim: 29.05.2023.

Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler. “Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi”, s. 6, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134- f57bc727af7d.pdf, Erişim: 02.09.2021.

Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler.“100 Soruda Kişisel Verilerin Korunması Kanunu”, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e- 1d48322ca352.pdf, Erişim: 07.07.2021.

Kişisel Verileri Korunma Kurumu Resmi Web Sitesi. Rehberler. “Özel Nitelikli Kişisel Verilerin İşlenme Şartları”, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0ef45a05-ac30-4f35-bc4b- 3b2cbefc9864.pdf, Erişim: 08.07.2021.

Kişisel Verileri Koruma Kurumu Resmi Web Sitesi.” Kişisel Verilerin Korunması Kanunu Ve Uygulaması”,https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%0KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf, Erişim: 08.09.2021

Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler, “Kişisel Verilerin İşlenme Şartları”,https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/9feefe58-9b0f- 49c9- a0c7-2b2eb8c012bb.pdf, Erişim: 24.11.2021.

Kişisel Verileri Koruma Kurumu Resmi Web sitesi. Rehberler, “Açık Rıza”, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51- 71bcf07c09b5.pdf, Erişim: 11.11.2021.

Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. Rehberler, “Veri Sorumlusu Veri İşleyen”, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1- 1ca9bdb81ea5.pdf, Erişim: 06.01.2022.

Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. “Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler”, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf, Erişim: 03.01.2022.

Kişisel Verileri Koruma Kurumu Resmi Web Sitesi. (2018). “Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)”, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf, Erişim: 05.01.2022.

Kişisel Verileri Koruma Kurumu. “İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık)”, https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik-, Erişim: 19.12.2022.

Klinik İletişim. “Mikroçipler Aslında Küçük Birer Laboratuvar!”, https://www.klinikiletisim.com/mikrocipler-aslinda-kucuk-birer-laboratuvar/, Erişim: 08.08.2021.

Lawn&Landscape. “Ohio Employer Implants Employee Microchip” https://www.lawnandlandscape.com/news/ohio-employer-implants-employee-microchip/, Erişim: 01.10.2021

Notes From Poland. “World’s first payment chip that can be implanted under skin launched by Polish-British startup”, https://notesfrompoland.com/2021/04/14/worlds-first- payment-chip-implanted-under-skin-launched-by-polish-british-startup/, Erişim: 13.12.2021.

Paşaoğlu, C. (2019). “Kişisel Verilerin Korunması Kanunu Kişilerin Temel Hak ve Özgürlüklerini Korumak Amacındadır,” Video, 6:02, 1.e-Safe Boğaziçi Kişisel Verileri Korumada Yerli Çözümler Zirvesi, yükleyen: e-Safe, https://www.youtube.com/watch?v=e-M392izsks&ab_channel=e-Safe. Erişim: 03.04.2023.

Prof. Dr. İlhan Helvacı Dersleri. Türk Medeni Kanunu. http://www.ilhanhelvacidersleri.com/turk-medeni-kanunu/turk-medeni-kanunu- madde-2, Erişim: 05.06.2022.

Soteks. “RFID nedir?” , https://www.soteksetiket.com/rfid-nedir/, Erişim: 10.10.2021.

VivoKey. “Vivokey Ecosystem”, https://www.vivokey.com/ecosystem, Erişim: 10.10.2021.

Wikipedia. “Radio-frequency identification”, https://en.wikipedia.org/wiki/Radio-frequency_identification#Hospitals_and_healthcare, Erişim:10.10.2021.

OECD. “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personel Data”,http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtr ansbor derflowsofpersonaldata.htm, Erişim: 08.08.2021.

OpenMind BBVA. (2021). “Technology Under Your Skin: 3 Challenges of Microchip Implants”. https://www.bbvaopenmind.com/en/technology/innovation/technology-under-your-skin/, Erişim: 05.01.2022.

RFIDHY Technology. “RFID Hayvan Etiketi İle Geleneksel Hayvan Etiketi Arasındaki Fark Nedir?” https://www.rfidhy.com/tr/what-is-the-difference-between-rfid-animal-tag- and-traditional-animal-tag/, Erişim: 11.10.2021.

Teknopedia. “What Does Microchip Mean?”, https://www.techopedia.com/definition/8331/microchip, Erişim:10.09.2020.

Tekno Kampüs. “Mikroçip Nedir?”, https://teknokampus.net/mikrocip-nedir-ne-ise-yarar- nasil-uretilir/, Erişim: 08.08.2021.

Thomas Net. (2019). “The Future of Microchip Implants in Humans” https://www.thomasnet.com/insights/the-future-of-microchip-implants-in-humans/, Erişim: 15.10.2021.

Triplem. (2018). “Would You Microchip Your Kids To Keep Them Safe?”, https://www.triplem.com.au/story/would-you-microchip-your-kids-to-keep-them-safe-87113, Erişim: 25.05.2023.

Türkiye Cumhuriyeti İçişleri bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü. “Türkiye Cumhuriyeti Kimlik Kartı”, https://www.nvi.gov.tr/tc-kimlik-karti, Erişim: 07.11.2022.

Türk Dil Kurumu Güncel Türkçe Sözlüğü. https://sozluk.gov.tr/, Erişim: 15.09.2021.

28.10.2017 tarihli ve 30224 sayılı Resmi Gazete. “Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik”,

https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm, Erişim: 07.01.2022.
Türkiye Gazetesi, (2022). "İnternette karanlık ticaret! Türkiye'de her gün 50 milyon dolarlık işlem yapılıyor: Instagram hesabı çalma, kredi sicili düzeltme...", https://www.turkiyegazetesi.com.tr/ekonomi/internette-karanlik-ticaret-turkiyede-her-gun-50-milyon-dolarlik-islem-yapiliyor-instagram-hesabi-calma-kredi-sicili-duzeltme-907887, Erişim: 08.10.2021.
Uralstk. "İnsan vücudundaki bir çip nasıl belirlenir. İnsanlara kim cips koyar? Parçalamanın avantajları ve dezavantajları", https://uralstk.ru/tr/a-healthy-lifestyle/kak-opredelit-chip-v-tele-cheloveka-kto-stavit-lyudyam-chipy/, Erişim:19.12.2022.
VeriChip. "GlucoChip" , http://www.verichipcorp.com/products_glucochip.html, Erişim: 12.10.2021.
Vox. "How biohackers are trying to upgrade their brains, their bodies — and human nature", https://www.vox.com/future-perfect/2019/6/25/18682583/biohacking-transhumanism-human-augmentation-genetic-engineering-crispr, Erişim: 10.10.2021.
YouTube. "Derimin Altına Çip Taktım (RFID Implantı)" https://www.youtube.com/watch?v=qMODQYqF1wA, Erişim: 12.12.2021.
YouTube. "Biohacking - the forefront of a new kind of human evolution: Amal Graafstra at TEDxSFU" https://www.youtube.com/watch?v=7DxVWhFLI6E, Erişim: 10.10.2021.
YouTube. "Unboxing xSIID NFC chip implant with LED", https://www.youtube.com/watch?v=mm7jEMuNBxs, Erişim:10.10.2021.
YouTube. "comprar en maquina vending con implante chip sin llevar dinero bodyhacker" https://www.youtube.com/watch?v=tLWzTIvRIkk, Erişim: 10.10.2021.
YouTube. "MythBusters The RFID CHIP IMPLANT!", https://www.youtube.com/watch?v=IDq_LBH_ZYs, Erişim: 11.10.2021.
Youtube. "Implanted microchip may help trat osteoporosis", https://www.youtube.com/watch?v=Ap47khjw5n8&t=37s, Erişim: 07.10.2021.
Youtube. "HOPE Number Six (2006): How To Steal Someone's Implanted RFID - And Why You'd Want To", https://www.youtube.com/watch?v=jzzg3-L-QDI, Erişim: 01.12.2022.
WhitePaper. (2007). "Radyo Frekanslı Tanımlama", KoçSistem, 3-6. https://silo.tips/download/rfid-teknolojsnde-ver-gvenlnn-salanmasi-n-melez-freleme-algortmasinin-uygulanmas, Erişim: 12.08.2022.
WIDEX. *"How The Chıp Transformed The Industry",* https://www.widexpro.com/en-ca/blog/global/how-the-chip-transformed-the-industry/, Erişim: 08.08.2021.
Wikipedia. *"Entegre Devre",* https://tr.wikipedia.org/wiki/Entegre_devre, Erişim: 08.08.2021.
Wikipedia. "Mikrochip implant (human)" https://en.wikipedia.org/wiki/Microchip_implant_(human)#:~:text=A%20human%20microchip%20implant%20is,body%20of%20a%20human%20being., Erişim: 05.01.2022.
Wikipedia. "Dangerous Things" https://en.wikipedia.org/wiki/Dangerous_Things, Erişim: 10.10.2021.

Wikipedia, “Mikrochip implant (human)”, https://en.wikipedia.org/wiki/Microchip_implant_(human)#:~:text=A%20human%20microchip%20implant%20is,body%20of%20a%20human%20b eing., Erişim: 06.01.2022.
Wikipedia. “Veri Bankası”, https://en.wikipedia.org/wiki/Data_bank, Erişim: 02.01.2022.
Wikita. “Amal Graafstra”, https://wikitia.com/wiki/Amal_Graafstra, Erişim: 10.10.2021
Wipelot. https://wipelot.com/rfid-teknolojisi-nedir-ve-is-sagligi-ve-guvenligi-alanlarinda-nasil-kullanilir Erişim: 12.10.2022
Woshoe County. “What is a microchip and how do they work?”, https://www.washoecounty.gov/animal/faq/microchip_work.php, Erişim: 11.06.2021.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : Kazanbaş, Defne Nur

Uyruğu : Türkiye Cumhuriyeti

Eğitim

Lisans	KTO Karatay Üniversitesi	2019
Lise	Dolapoğlu Anadolu Lisesi	2013

İş Deneyimi

Yıl	**Yer**	**Görev**
2020-2023	Kazanbaş Hukuk Bürosu	Yönetici Avukat
2020-2023	Odak Veri Danışmanlık Ltd. Şti.	Uzman Danışman

Yabancı Dil

İngilizce

ankara HBM

ankara HBV

le.ahbv.edu.tr