KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

KİŞİSEL VERİLERİN **SİLİNMESİ, YOK EDİLMESİ** veya **ANONİM HALE GETİRİLMESİ** REHBERİ

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

KİŞİSEL VERİLERİN **SİLİNMESİ, YOK EDİLMESİ** veya **ANONİM HALE GETİRİLMESİ** REHBERİ

KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ veya ANONİM HALE GETİRİLMESİ REHBERİ

KVKK Yayınları

ISBN : 978-975-19-6807-4
Ocak 2018, Ankara

Fotoğraflar **:** www.shutterstock.com

Kişisel Verileri Koruma Kurumu

Adres **:** Nasuh Akar Mahallesi Ziyabey Caddesi 1407. Sokak No:6 Balgat /Çankaya / ANKARA / TÜRKİYE
Telefon : +90 312 216 50 50
Web **:** www.kvkk.gov.tr

“Bu kitapta yer alan yazı, fotoğraf ve sair içeriklerin, bireysel kullanım dışında izin alınmadan kısmen ya da tamamen kopyalanması, çoğaltılması, kullanılması, yayınlanması ve dağıtılması kesinlikle yasaktır. Bu yasağa uymayanlar hakkında 5846 sayılı Fikir ve Sanat Eserleri Kanunu uyarınca yasal işlem yapılacaktır. Ürünün tüm hakları saklıdır.”

KİŞİSEL VERİLER
SİLME
VERİ TABANI
ANONİMLİĞİN BOZULMASI
6698
ÇEŞİTLİLİK
YÖNETMELİK
MASKELEME
ANONİM HALE GETİRME
YOK ETME
KANUN
MEVZUAT
KARARTMA

ÖZET

Bu Rehber; 6698 sayılı Kişisel Verilerin Korunması Kanununa (“Kanun”) ve ilgili diğer mevzuat hükümlerine uygun olarak işlenmiş kişisel verilerin, işlenmesini gerektiren sebeplerin ortadan kalkması halinde silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin başlıca yöntemleri açıklamaktadır.

Rehberde silme ve yok etme yöntemleri kişisel verilerin işlendiği ve bulunduğu ortam dikkate alınarak ayrı ayrı açıklanmış, anonim hale getirme yöntemleri ve anonimliğin bozulması ise uygulama örnekleri ile birlikte detaylı olarak açıklanmıştır.

ABSTRACT

This Guide explains the major methods for the erasure, destruction or anonymization of personal data processed in accordance with the provisions of the Law on the Protection of Personal Data (Law No. 6698) and other relevant legislation, providing that no reason for processing that data is left.

In the Guide, the erasure and destruction methods, considering the environment in which the personal data is processed and stored are explained separately. Besides, anonymization methods and de-anonymization are covered in detail along with the examples of implementation.

ANAHTAR KELİMELER:

Kişisel veriler, silme, yok etme, anonim hale getirme, anonimliğin bozulması.

KEY WORDS:

Personal data, erasure, destruction, anonymization, de-anonymization.

İÇİNDEKİLER

ŞEKİL, RESİM ve TABLOLAR

Şekiller Listesi

Resimler Listesi

Tablolar Listesi

I.GİRİŞ

1.1. Amaç ve Dayanak

Kanunun 7 nci maddesinin üçüncü fıkrasında "Kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir" hükmü yer almaktadır.

Bu hüküm ve Kanunun 22 nci maddesinin birinci fıkrasının (e) bendine istinaden Kişisel Verileri Koruma Kurulu ("Kurul") tarafından Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") hazırlanmış olup 28 Ekim 2017 tarihli ve 30224 sayılı Resmi Gazete'de yayımlanmıştır.

Bu Yönetmeliğe dayanarak söz konusu işlemlerin nasıl yapılacağı hakkında uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması bakımından çeşitli konu başlıklarına dikkat çekmek amacıyla Kurul tarafından Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi ("Rehber") hazırlanmış ve kamuoyuna sunulmuştur.

1.2. Kapsam

Rehberin;

Birinci bölümü giriş bölümü olup; bu bölümde rehberin hazırlanmasının amacına, dayanağına, rehberin kapsamına ve tanımlara yer verilmiştir.

İkinci bölümünde kişisel verilerin silinmesi, silme işlemi yöntemleri ve süreci ile kişisel verilerin yok edilmesi ve buna ilişkin yöntemler açıklanmıştır.

Üçüncü bölümünde, kişisel verilerin anonim hale getirilmesi ile buna ilişkin yöntemler ve söz konusu yöntemlerin nasıl seçileceği, anonimliğin güvencesi ve anonimliğin bozulmasına dair riskler açıklanmıştır.

Dördüncü bölümünde, rehber hazırlanırken faydalanılan kaynaklara ve incelenmesinin uygun olacağı değerlendirilen dokümanlara yer verilmiştir.

1.3. Tanımlar

Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,

Doğrudan tanımlayıcılar: Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları,

Dolaylı tanımlayıcılar: Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları,

İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

İlgili kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen gerçek veya tüzel kişileri,

İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

Kanun: 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu,

Karartma: Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması gibi işlemleri,

Kayıt ortamı: Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı,

Kişisel veri saklama ve imha politikası: Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı,

Maskeleme: Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemleri,

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini, ifade eder.

Bu Rehberde yer almayan tanımlar için Kanun ve Yönetmelikteki tanımlara başvurulabilir.

II. KİŞİSEL VERİLERİN **SİLİNMESİ** ve **YOK EDİLMESİ**

Kişisel verilerin silinmesi ve yok edilmesi, kişisel veri saklama ve imha politikasında belirtilen esaslara uygun olarak aşağıda açıklanacak yöntemlerle gerçekleştirilebilir.

2.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

2.1.1. Kişisel Verilerin Silinmesi Süreci

Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi.
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi.
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi.
- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

Şekil 2.1. Kişisel Verilerin Silinmesi Süreci

2.1.2. Kişisel Verilerin Silinmesi Yöntemleri

Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir. Buna ilişkin örnekler aşağıda yer almaktadır:

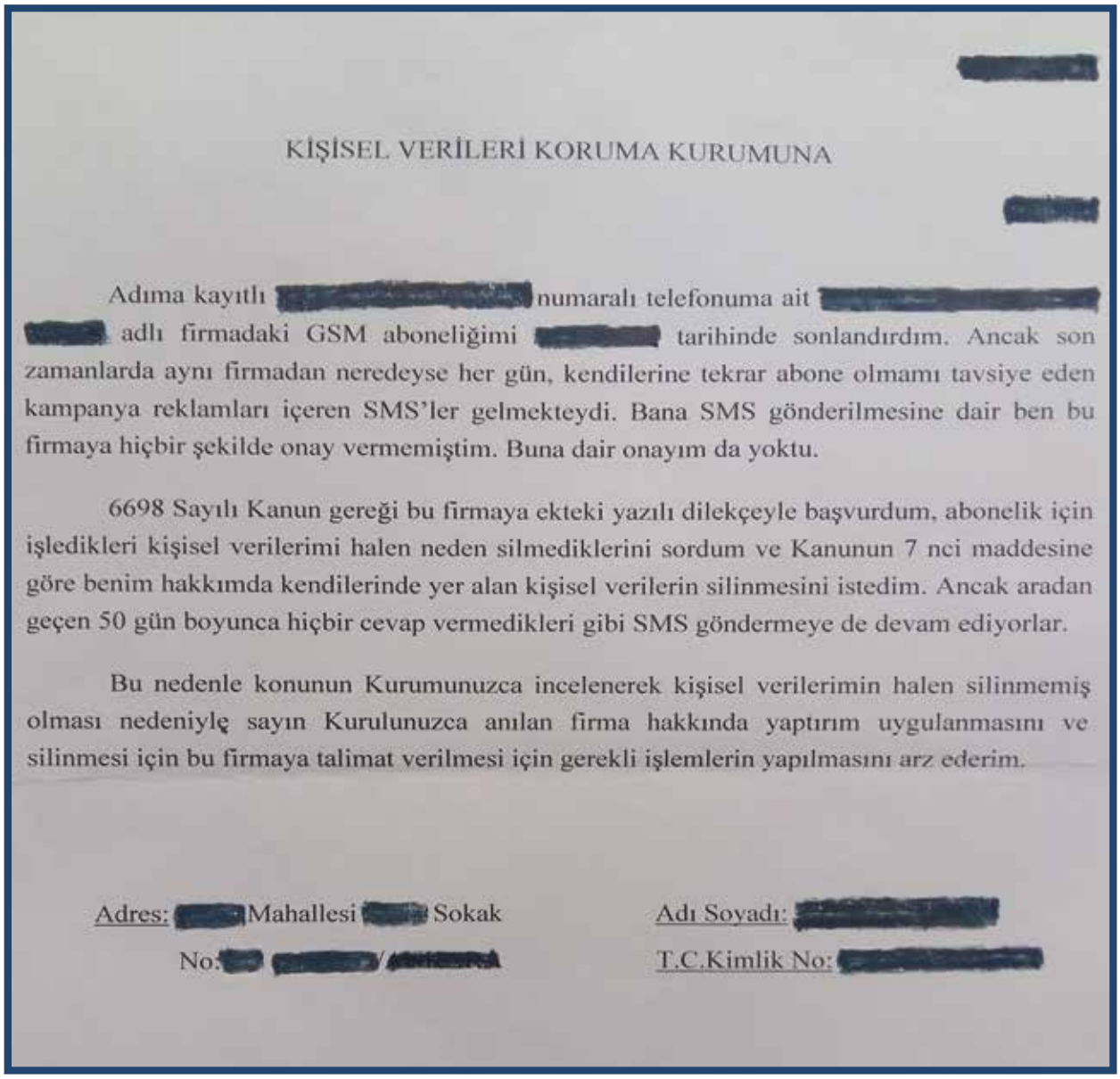
a) Hizmet Olarak Uygulama Türü Bulut Çözümleri (Office 365, Salesforce, Dropbox gibi)

Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

b) Kağıt Ortamında Bulunan Kişisel Veriler

Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmelidir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

Örneğin aşağıda Resim 2.1'de yer alan dilekçeden görüleceği üzere, kişisel verilerinin silinmesi talebiyle veri sorumlusuna başvurduğu halde sonuç alamayan bir kişinin Kurumumuza vermiş olduğu dilekçenin bir örneği paylaşılmak istendiğinde; anılan dilekçedeki kişisel verilerin korunması için bu kişisel verilerin üzeri okunamayacak şekilde çizilerek / boyanarak / silinerek bir tür karartma işlemi uygulanmıştır.



[redacted]

KİŞİSEL VERİLERİ KORUMA KURUMUNA

[redacted]

Adıma kayıtlı [redacted] numaralı telefonuma ait [redacted] adlı firmadaki GSM aboneliğimi [redacted] tarihinde sonlandırdım. Ancak son zamanlarda aynı firmadan neredeyse her gün, kendilerine tekrar abone olmamı tavsiye eden kampanya reklamları içeren SMS'ler gelmekteydi. Bana SMS gönderilmesine dair ben bu firmaya hiçbir şekilde onay vermemiştim. Buna dair onayım da yoktu.

6698 Sayılı Kanun gereği bu firmaya ekteki yazılı dilekçeyle başvurdum, abonelik için işledikleri kişisel verilerimi halen neden silmediklerini sordum ve Kanunun 7 nci maddesine göre benim hakkımda kendilerinde yer alan kişisel verilerin silinmesini istedim. Ancak aradan geçen 50 gün boyunca hiçbir cevap vermedikleri gibi SMS göndermeye de devam ediyorlar.

Bu nedenle konunun Kurumunuzca incelenerek kişisel verilerimin halen silinmemiş olması nedeniyle sayın Kurulunuzca anılan firma hakkında yaptırım uygulanmasını ve silinmesi için bu firmaya talimat verilmesi için gerekli işlemlerin yapılmasını arz ederim.

Adres: [redacted] Mahallesi [redacted] Sokak
No: [redacted]

Adı Soyadı: [redacted]
T.C.Kimlik No: [redacted]

Resim 2.1. Kişisel Verilerin Karartılması Örneği

c) Merkezi Sunucuda Yer Alan Ofis Dosyaları

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmelidir.

ç) Taşınabilir Medyada Bulunan Kişisel Veriler

Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

d) Veri Tabanları

Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.

2.2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

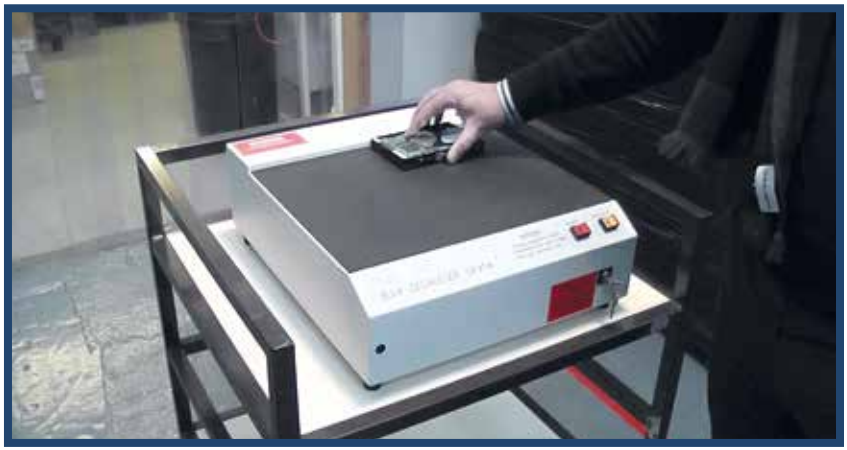
2.2.1. Kişisel Verilerin Yok Edilmesi Yöntemleri

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi gereklidir:

a) Yerel Sistemler

Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir.

i) De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.



Resim 2.2. Degausser Cihazı

ii) Fiziksel Yok Etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.

Resim 2.3. Fiziksel Yok Etme

iii) Üzerine Yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

Resim 2.4. Üzerine Yazma

b) Çevresel Sistemler

Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır:

i) Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

ii) Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

iii) Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

iv) Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

v) Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir**.**

vi) Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

vii) Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

viii) Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

c) Kağıt ve Mikrofiş Ortamları

Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

ç) Bulut Ortamı

Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

Yukarıdaki ortamlara ek olarak; arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

i) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,

ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,

iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması,

gerekir.

III. KİŞİSEL VERİLERİN **ANONİM HALE GETİRİLMESİ**

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya alıcı grupları tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

Veri sorumlusu, kişisel verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür. Kişisel verilerin anonim hale getirilmesi, kişisel veri saklama ve imha politikasında belirtilen esaslara uygun olarak aşağıdaki yöntemlerle gerçekleştirilir.

3.1. Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup/kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir.

Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır.

Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılmasıdır. Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir. Bu yöntemlerin uygulanması sonucunda elde edilen verilerin belirli bir kişiyi tanımlayamaz olması gerekmektedir. Örnek alınabilecek anonim hale getirme yöntemleri aşağıdaki tabloda gösterilmektedir:

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri	• Değişkenleri Çıkartma • Kayıtları Çıkartma • Bölgesel Gizleme • Genelleştirme • Alt ve Üst Sınır Kodlama • Global Kodlama • Örnekleme
Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	• Mikro Birleştirme • Veri Değiş Tokuşu • Gürültü Ekleme
Anonim Hale Getirmeyi Kuvvetlendirici İstatistiksel Yöntemler	• K-Anonimlik • L-Çeşitlilik • T-Yakınlık

Tablo 3.1. Anonim Hale Getirme Yöntemleri

3.1.1. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlamayan yöntemlerde kümedeki verilerin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satır veya sütunların bütününde değişiklikler yapılır. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini korurlar. Değer düzensizliği sağlamayan anonim hale getirme yöntemlerinden bazıları aşağıda örneklerle açıklanmıştır:

a) Değişkenleri Çıkartma

Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. Böyle bir durumda tablodaki bütün sütun tamamıyla kaldırılacaktır. Bu yöntem, değişkenin yüksek dereceli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması, değişkenin kamuya ifşa edilemeyecek kadar hassas bir veri olması veya analitik amaçlara hizmet etmiyor olması gibi sebeplerle kullanılabilir.

Yaş	Cinsiyet	Posta Kodu	Gelir	Din
20	K	SO17	20,000	Budist
38	E	SO18	22,000	Müslüman
29	E	SO16	32,000	Hristiyan
31	K	SO17	31,000	Müslüman
44	K	SO15	68,000	Yahudi
78	E	SO14	28,000	Yahudi

Tablo 3.2. Değişkenleri Çıkartma Örneği

b) Kayıtları Çıkartma

Bu yöntemde veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür. Genellikle çıkartılan kayıtlar diğer kayıtlarla ortak bir değer taşımayan ve veri kümesine dair fikri olan kişilerin kolayca tahmin yürütebileceği kayıtlardır.

Örneğin anket sonuçlarının yer aldığı bir veri kümesinde, herhangi bir sektörden yalnızca tek bir kişi ankete dahil edilmiş olsun. Böyle bir durumda tüm anket sonuçlarından "sektör" değişkenini çıkartmaktansa sadece bu kişiye ait kaydı çıkartmak tercih edilebilir.

Yaş	Cinsiyet	Doğum Y.	Sektör	Derece
31	K	İstanbul	Mimarlık	3.22
31	E	İstanbul	Mimarlık	3.04
31	E	Ankara	Sanayi	3.22
43	K	Ankara	Sanayi	2.86
51	E	Eskişehir	Sanat	2.93
27	K	İstanbul	Ticaret	2.97
27	K	Ankara	Ticaret	2.98

Tablo 3.3. Kayıtları Çıkartma Örneği

c) Bölgesel Gizleme

Bölgesel gizleme yönteminde amaç veri kümesini daha güvenli hale getirmek ve tahmin edilebilirlik riskini azaltmaktır. Belli bir kayda ait değerlerin yarattığı kombinasyon çok az görülebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine yüksek olasılıkla sebep olabilecekse istisnai durumu yaratan değer "bilinmiyor" olarak değiştirilir.

Örneğin Tablo 3.4'te yaş, cinsiyet ve meslek ayrımına göre HIV durumu görülmektedir. Bu tabloda Yaş=3 olan kayıt bir çocuğa ait olduğundan istisnai bir durum yaratmakta ve tahmin edilebilirlik ve çocuğun ailesine dair varsayımlar yapılması riskini arttırmaktadır.

Yaş	Cinsiyet	Meslek	HIV Durumu
17	K	Öğretmen	Pozitif
28	E	Mimar	Negatif
16	E	Öğretmen	Pozitif
3	K	-	Pozitif
64	K	Mühendis	Pozitif
52	K	Mühendis	Pozitif

Tablo 3.4. Bölgesel Gizleme Orijinal Veri Kümesi

Bu sebeple; bölgesel gizleme yöntemi ile bahsedilen kaydın yaş hanesi "bilinmiyor" olarak değiştirilirse ve Tablo 3.5'teki yeni durum elde edilirse, veri kümesine dair tahmin edilebilirlik riskinde azalma sağlanacaktır.

Yaş	Cinsiyet	Meslek	HIV Durumu
17	K	Öğretmen	Pozitif
28	E	Mimar	Negatif
16	E	Öğretmen	Pozitif
Bilinmiyor	K	-	Pozitif
64	K	Mühendis	Pozitif
52	K	Mühendis	Pozitif

Tablo 3.5. Bölgesel Gizleme Sonrası Dağılım

ç) Genelleştirme

İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Kümülatif raporlar üretirken ve toplam rakamlar üzerinden yürütülen operasyonlarda en çok kullanılan yöntemdir. Sonuç olarak elde edilen yeni değerler gerçek bir kişiye erişmeyi imkansız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir.

Örneğin TC Kimlik No 12345678901 olan bir kişi e-ticaret platformundan çocuk bezi aldıktan sonra aynı zamanda ıslak mendil de almış olsun. Yapılacak anonim hale getirme işleminde genelleştirme yöntemi kullanılarak e-ticaret platformundan çocuk bezi alan kişilerin %xx'i aynı zamanda ıslak mendil de satın alıyor şeklinde bir sonuca ulaşılabilir.

d) Alt ve Üst Sınır Kodlama

Alt ve üst sınır kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir. Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak ilerlenir.

Aşağıdaki örnekte Tablo 3.6 orijinal veri kümesini, Tablo 3.7 ise seçilen değişkenlerin alt ve üst sınır kodlaması yapılarak yeniden tasarlanmış ve anonim hale getirilmiş şeklini göstermektedir.

Yaş	Cinsiyet	Meslek	Gelir (Yıllık)	Test Sonucu	Harcamalar (Aylık)
3*	K	Mühendis	92.000	Negatif	8.000
4*	E	Mimar	110.000	Negatif	9.600
4*	E	Doktor	149.000	Negatif	10.000
5*	K	Doktor	123.000	Pozitif	10.800
5*	E	Doktor	125.000	Negatif	11.100
2*	E	Eczacı	85.000	Pozitif	16.300

Tablo 3.6. Alt ve Üst Sınır Kodlama Orijinal Veri Kümesi

Tablodaki Gelir ve Harcamalar değişkenlerine ait değerler alt ve üst sınır kodlama yöntemi ile aşağıdaki şekilde değiştirilir;

Gelir (Yıllık): Düşük = 100.000'den küçük ve eşit değerler;
Orta = 100.000 ve 120.000 arası değerler;
Yüksek = 120.000'den büyük ve eşit değerler,

Harcamalar (Aylık): Düşük = 10.000'den küçük ve eşit değerler;
Orta = 10.000 ve 11.000 arası değerler;
Yüksek = 11.000'den yüksek ve eşit değerler,

Bu kodlamaya göre anonim hale getirilmiş tablo aşağıdaki şekli alacaktır.

Yaş	Cinsiyet	Meslek	Gelir (Yıllık)	Test Sonucu	Harcamalar (Aylık)
3*	K	Mühendis	Düşük	Negatif	Düşük
4*	E	Mimar	Orta	Negatif	Düşük
4*	E	Doktor	Yüksek	Negatif	Orta
5*	K	Doktor	Yüksek	Pozitif	Orta
5*	E	Doktor	Yüksek	Negatif	Yüksek
2*	E	Eczacı	Düşük	Pozitif	Yüksek

Tablo 3.7. Alt ve Üst Sınır Kodlama Sonrası Anonim Hale Getirilmiş Veri Kümesi

e) Global Kodlama

Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya numerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir. Genelde belli değerlerin öbeklenerek tahmin ve varsayımlar yürütmeyi kolaylaştırdığı hallerde kullanılır. Seçilen değerler için ortak ve yeni bir grup oluşturularak veri kümesindeki tüm kayıtlar bu yeni tanım ile değiştirilir.

Aşağıdaki örnekte Tablo 3.8 orijinal veri kümesini, Tablo 3.9 ise global kodlama uygulamasından sonraki anonim hale getirilmiş veri kümesini göstermektedir.

Cinsiyet	Meslek	İlçe	Medeni Durum
K	Mimar	Çankaya	Evli
K	Mühendis	Çankaya	Bekar
K	Mimar	Çankaya	Boşanmış
K	Mimar	Çankaya	Bekar
K	Mühendis	Çankaya	Bekar
K	Mühendis	Çankaya	Boşanmış
K	Mühendis	Çankaya	Evli

Tablo 3.8. Global Kodlama Orijinal Veri Kümesi

Bu veri kümesinde tek bir ilçedeki kadınların nüfusuna ait verinin meslek değişkeninde iki kategoride yığılma görüldüğünden söz konusu iki kategorinin birleşiminden tek bir kategori elde edilebilir ve bu durumda veri daha güvenli hale getirilmiş olur.

Cinsiyet	Meslek	İlçe	Medeni Durum
K	Mimar veya Mühendis	Çankaya	Evli
K	Mimar veya Mühendis	Çankaya	Bekar
K	Mimar veya Mühendis	Çankaya	Boşanmış
K	Mimar veya Mühendis	Çankaya	Bekar
K	Mimar veya Mühendis	Çankaya	Bekar
K	Mimar veya Mühendis	Çankaya	Boşanmış
K	Mimar veya Mühendis	Çankaya	Evli

Tablo 3.9. Global Kodlama Sonrası Anonim Hale Getirilmiş Veri Kümesi

f) Örnekleme

Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin üretme riski düşürülmüş olur. Örnekleme yapılacak alt kümenin belirlenmesinde basit istatistik metotları kullanılır.

Örneğin; İstanbul ilinde yaşayan kadınların demografik bilgileri, meslekleri ve sağlık durumlarına dair bir veri kümesinin anonim hale getirilerek açıklanması ya da paylaşılması halinde İstanbul'da yaşadığı bilinen bir kadına dair ilgili veri kümesinde taramalar yapmak ve tahmin yürütmek anlamlı olabilir.

Ancak ilgili veri kümesinde yalnızca nüfusa kayıtlı olduğu il İstanbul olan kadınların kayıtları bırakılır, nüfus kaydı diğer illerde olanlar veri kümesinden çıkartılarak anonimleştirme uygulanır ve veri açıklanır ya da paylaşılırsa, veriye erişen kişi, İstanbul'da yaşadığını bildiği bir kadının nüfus kaydının İstanbul'da olup olmadığını tahmin edemeyeceğinden tanıdığı bu kişiye ait bilgilerin elindeki verinin içerisinde yer alıp almadığına dair güvenilir bir tahmin yürütemeyecektir.

3.1.2. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlayan yöntemlerle yukarıda bahsedilen yöntemlerden farklı olarak; mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılır. Bu durumda kayıtların taşıdığı değerler değişmekte olduğundan veri kümesinden elde edilmesi planlanan faydanın doğru hesaplanması gerekmektedir. Veri kümesindeki değerler değişiyor olsa bile toplam istatistiklerin bozulmaması sağlanarak hala veriden fayda sağlanmaya devam edilebilir.

Değer düzensizliği sağlayan anonim hale getirme yöntemlerinden bazıları aşağıda örneklerle açıklanmıştır:

a) Mikro Birleştirme

Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.

Aşağıdaki Tablo 3.10'daki kayıtlar "Gelir" sütunundaki değişkenler, değerlerine göre birbirine yakın olan üçerli gruplara ayrılmış ve gruplar renk kodlarıyla işaretlenmiştir. Her grup içindeki değerlerin aritmetik ortalaması alınmış ve gruptaki tüm kayıtlara, bulunan yeni değerler atanarak orijinal değeri tespit edebilmek engellenmiştir.

Yaş	Cinsiyet	Posta Kodu	Gelir
23	K	1556	25.000
37	K	1559	28.000
41	E	1559	37.000
25	K	1557	49.000
34	E	1558	56.000
48	E	1556	60.000

Tablo 3.10. Mikro Birleştirme Orijinal Veri Kümesi

Grup 1 için mikro birleştirme sonucunda yeni değer : (25.000 + 28.000 + 37.000) / 3 = 30.000

Grup 2 için mikro birleştirme sonucunda yeni değer : (49.000 + 56.000 + 60.000) / 3 = 55.000

Yaş	Cinsiyet	Posta Kodu	Gelir
23	K	1556	30.000
37	K	1559	30.000
41	E	1559	30.000
25	K	1557	55.000
34	E	1558	55.000
48	E	1556	55.000

Tablo 3.11. Mikro Birleştirme Sonucu Elde Edilen Yeni Veri Kümesi

b) Veri Değiş Tokuşu

Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesidir.

Yaş	Cinsiyet	İl	Gelir
21	K	İstanbul	20.000
24	K	Ankara	30.000
35	E	İzmir	30.000
36	K	İstanbul	25.000
45	E	İzmir	55.000
50	E	İzmir	15.000

Tablo. 3.12. Veri Değiş Tokuşu Orijinal Veri Kümesi

Tablo 3.12 orijinal değerleri içeren kayıtlara sahiptir. Tablo 3.13'te veri değiş tokuşu işlemi sonucunda elde edilen yeni veri kümesini içermektedir. Söz konusu tablodan görüleceği üzere Yaş = "24", Cinsiyet = "K", İl = "Ankara" olan kayda ait gelir bilgisi ile Yaş = "45", Cinsiyet = "E", İl = "İzmir" olan kaydın gelir bilgisi birbirleriyle değiştirilmiştir. Aynı şekilde Yaş = "35", Cinsiyet = "E", İl = "İzmir" olan kayda ait gelir bilgisi ile Yaş = "50", Cinsiyet = "E", İl = "İzmir" olan kayıtların gelir bilgisi birbirleriyle değiştirilmiş ve yeni veri kümesi oluşturulmuştur.

Yaş	Cinsiyet	İl	Gelir
21	K	İstanbul	25.000
24	K	Ankara	55.000
35	E	İzmir	15.000
36	K	İstanbul	20.000
45	E	İzmir	30.000
50	E	İzmir	30.000

Tablo 3.13. Veri Değiş Tokuşu Sonucu Elde Edilen Yeni Veri Kümesi

c) Gürültü Ekleme

Bu yöntem ile, seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkartmalar yapılır. Bu yöntem çoğunlukla sayısal değer içeren veri kümelerinde uygulanır. Bozulma her değerde eşit ölçüde uygulanır.

Yaş	Cinsiyet	İl	Gelir
21	K	İzmir	45.000
24	K	Ankara	20.000
35	E	Ankara	123.000
36	K	Ankara	18.000
45	E	İstanbul	75.000
50	E	İstanbul	7.000

Tablo 3.14. Gürültü Ekleme Orijinal Veri Kümesi

Tablo 3.14'teki gelir değişkenleri için her bir kaydın değerlerine +80.000 işlemi uygulanmış ve Tablo 3.15'teki yeni değişkenler oluşmuştur.

Yaş	Cinsiyet	İl	Gelir
21	K	İzmir	125.000
24	K	Ankara	100.000
35	E	Ankara	203.000
36	K	Ankara	98.000
45	E	İstanbul	155.000
50	E	İstanbul	87.000

Tablo 3.15. Gürültü Ekleme Sonucu Elde Edilen Veri Kümesi

3.1.3. Anonim Hale Getirmeyi Kuvvetlendirici İstatistiksel Yöntemler

Anonim hale getirilmiş veri kümelerinde kayıtlardaki bazı değerlerin tekil senaryolarla bir araya gelmesi sonucunda, kayıtlardaki kişilerin kimliklerinin tespit edilmesi veya kişisel verilerine dair varsayımların türetilebilmesi ihtimali ortaya çıkabilmektedir.

Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir. Bu yöntemlerdeki temel amaç, anonimliğin bozulması riskini en aza indirirken, veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

a) K-Anonimlik

Anonim hale getirilmiş veri kümelerinde, dolaylı tanımlayıcıların doğru kombinasyonlarla bir araya gelmesi halinde kayıtlardaki kişilerin kimliklerinin saptanabilir olması veya belirli bir kişiye dair bilgilerin rahatlıkla tahmin edilebilir duruma gelmesi anonim hale getirme süreçlerine dair olan güveni sarsmıştır. Buna istinaden çeşitli istatistiksel yöntemlerle anonim hale getirilmiş veri kümelerinin daha güvenilir duruma getirilmesi gerekmiştir.

K-anonimlik, bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilmesiyle oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır. Örneğin; Tablo 3.16'da ad-soyad, doğum tarihi, cinsiyet, hastalık ve posta kodu gibi değişkenler vardır.

Ad Soyad	Doğum Tarihi	Cinsiyet	Posta Kodu	Hastalık Adı
*	1983	E	3440*	Soğuk Algınlığı
*	1980	K	3440*	Hepatit-B
*	1983	E	3440*	Astım
*	1982	E	3440*	Baş Ağrısı
*	1982	E	3440*	Beyin Tümörü
*	1983	E	3440*	Yüksek Tansiyon
*	1983	E	3440*	Baş Ağrısı
*	1980	K	3440*	Grip
*	1983	E	3440*	Akciğer Kanseri

Tablo 3.16. K-Anonimlik Orijinal Veri Kümesi

Tabloda ad-soyad ve posta kodu değişkenlerine dair değerlerde maskeleme uygulanarak veri anonim hale getirilmiş olmakla birlikte böyle bir anonimleştirme yapılırken aynı değerleri içeren sadece bir kayıt varsa bu kayıtla doğru kişiyi tespit mümkün olacaktır. Ancak kayıtların çoklanması halinde, tekillik yaratabilecek değişkenlere dair belli bir çeşitlilik sağlanmış olacaktır. Örneğin; Tablo 3.16'da 1983 yılında doğmuş, cinsiyeti erkek ve posta kodu 3440 ile başlayan 5 adet kayıt için "Hastalık Adı" alanında beş ayrı hastalık çeşitliliği sağlanmış olduğundan 1983 yılında doğmuş cinsiyeti erkek olan ve posta kodu 3440 ile başlayan bir kişinin bu 5 hastalıktan hangisine sahip olduğuna dair tahmin yürütmek mümkün değildir. Bu nedenle, Tablo 3.17'de olduğu gibi çerçeve içerisinde yer alan doğum tarihi, cinsiyet ve posta kodu verileri aynı değerleri içeren kayıtların açıklanması ya da paylaşılması halinde 1983 yılında doğmuş cinsiyeti erkek olan ve posta kodu 3440 ile başlayan bir kişinin bu 5 hastalıktan hangisine sahip olduğuna dair tahmin yürütmek mümkün değildir.

Ad Soyad	Doğum Tarihi	Cinsiyet	Posta Kodu	Hastalık Adı
*	1980	K	3440*	Grip
*	1980	K	3440*	Hepatit-B
*	1982	E	3440*	Baş Ağrısı
*	1982	E	3440*	Beyin Tümörü
*	1983	E	3440*	Soğuk Algınlığı
*	1983	E	3440*	Yüksek Tansiyon
*	1983	E	3440*	Baş Ağrısı
*	1983	E	3440*	Astım
*	1983	E	3440*	Akciğer Kanseri

Tablo 3.17. K=4 Anonimlik Uygulanmış Veri Kümesi

b) L-Çeşitlilik

K=4 anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşan L-çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır. Tablo 3.18'de, bir hastanede yatmakta olan kişilere ait hastalık bilgisi verilirken bu kişilerin ad soyad veya kimlik numarası verilmeyerek K-anonimlik uygulanmış olmakla birlikte posta kodu, yaş ve etnik köken bilgisi paylaşılmış olduğundan tespit edilebilme ihtimali bulunmaktadır.

Posta Kodu	Yaş	Uyruk	Hastalık
13053	28	Rus	Kalp
13068	29	Amerikalı	Kalp
13068	21	Çinli	Viral Enfeksiyon
13053	23	Amerikalı	Viral Enfeksiyon
14853	50	İngiliz	Kanser
14853	55	Rus	Kalp
14850	47	Amerikalı	Viral Enfeksiyon
14850	49	Amerikalı	Viral Enfeksiyon
13053	31	Amerikalı	Kanser
13053	37	İngiliz	Kanser
13068	36	Japon	Kanser
13068	35	Amerikalı	Kanser

Tablo 3.18. L-Çeşitlilik Orijinal Veri Kümesi

Posta Kodu	Yaş	Uyruk	Hastalık
130**	< 30	*	Kalp
130**	< 30	*	Kalp
130**	< 30	*	Viral Enfeksiyon
130**	< 30	*	Viral Enfeksiyon
1485*	≥ 40	*	Kanser
1485*	≥ 40	*	Kalp
1485*	≥ 40	*	Viral Enfeksiyon
1485*	≥ 40	*	Viral Enfeksiyon
130**	3*	*	Kanser
130**	3*	*	Kanser
130**	3*	*	Kanser
130**	3*	*	Kanser

Tablo 3.19. K=4 Anonimleştirme Uygulanmış Veri Kümesi

Tablo 3.19'dan görüleceği üzere, Tablo 3.18'de yer alan bilgiler maskeleme mantığı (posta kodu ve yaş bilgisinden maskelemeyle 4'erli gruplar yaratılmıştır) içerisinde gruplanarak öncelikle K=4 anonimlik yöntemiyle anonimliği kuvvetlendirilmiştir.

Ancak ilk işlem sonucunda tablo 3.19'da görüleceği gibi son 4 kayıttaki grupta tüm "Hastalık" değerleri "Kanser" olarak gruplanmıştır. Bu durum posta kodu 130 ile başlayan 30'lu yaşlardaki herkesin uyruğundan bağımsız olarak "Kanser" hastası olduğu bilgisini paylaşmaktadır.

Bu iki bilgiye sahip olan bir kullanıcı, tanıdığı bu özellikte bir kişinin kanser hastası olduğu sonucuna kolaylıkla varabilecektir. Bu nedenle her bir grubun içinde belli bir çeşitlilik yaratılmasına dikkat edilerek maskeleme yöntemi kullanılmalıdır.

Tablo 3.20'de, aşağıdaki şekilde gruplanarak anonimleştirilmiş bir veri kümesinde K=4 olacak şekilde gruplar oluşturulmuştur ve aynı zamanda her bir grubun içinde de L=3 olacak şekilde (yani en az 3 çeşit hastalık tutturularak) çeşitlilik elde edilmiştir.

Her grubun içinde 4 kayıt ve 3 farklı çeşit hastalık yer alması sağlanarak anonimleştirme yapılmıştır. Bu işlem anonimleştirme işlemini kuvvetlendirmiş, dış bilgiye sahip kullanıcının tahmin gücünü azaltmıştır.

Posta Kodu	Yaş	Uyruk	Hastalık
1305*	≤ 40	*	Kalp
1305*	≤ 40	*	Viral Enfeksiyon
1305*	≤ 40	*	Kanser
1305*	≤ 40	*	Kanser
1485*	> 40	*	Kanser
1485*	> 40	*	Kalp
1485*	> 40	*	Viral Enfeksiyon
1485*	> 40	*	Viral Enfeksiyon
1306*	≤ 40	*	Kalp
1306*	≤ 40	*	Viral Enfeksiyon
1306*	≤ 40	*	Kanser
1306*	≤ 40	*	Kanser

Tablo 3.20. K=4 Anonimlik ve L=3 Çeşitlilik Uygulanması Sonucu Elde Edilen Yeni Veri Kümesi

c) T-Yakınlık

L-çeşitlilik yöntemi kişisel verilerde çeşitlilik sağlıyor olmasına rağmen, söz konusu yöntem kişisel verilerin içeriğiyle ve hassasiyet derecesiyle ilgilenmediği için yeterli korumayı sağlayamadığı durumlar oluşmaktadır.

Bu haliyle kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denilmektedir.

Tablo 3.21'de; doğum tarihi, cinsiyet ve posta kodu alanlarına göre K=3 olacak şekilde K-anonimlik ve L=3 olacak şekilde L-çeşitlilik sağlanmasına rağmen 1970 yılında doğmuş, 3440* adresinde oturan ve cinsiyeti erkek olan bir kişinin hastalıkları kanser, beyin tümörü ve hepatit b gibi ciddi hastalıklar olduğu için, bu grupta söz konusu kişinin hastalığının ciddi olduğu tespit edilebilir.

Doğum Tarihi	Cinsiyet	Posta Kodu	Hastalık Adı	Hasta Sayısı
198*	E	3440*	Grip	80
198*	E	3440*	Tansiyon	20
198*	E	3440*	Baş Ağrısı	70
197*	E	3440*	Kanser	10
197*	E	3440*	Beyin Tümörü	10
197*	E	3440*	Hepatit-B	10

Tablo 3.21. K=3 Anonimlik ve L=3 Çeşitlilik Uygulanmış Veri Kümesi

Bu tahmin gücünü azaltabilmek için de anonimleştirme içindeki gruplamalarda Tablo 3.22'de görülebileceği üzere öyle bir düzenleme yapılmıştır ki üçerli kayıtlardan oluşan gruplarda (K=3) en az 3 farklı (L=3) hastalık tipi olacak şekilde ayarlanmış ancak bir araya gelen bu 3 farklı hastalığın da hepsinin ciddi olmaması sağlanarak (beyin tümörü ve Hepatit-B ciddi hastalıklar iken baş ağrısı ciddi sayılmayacak bir hastalıktır) o gruptaki hastalara dair tahminler azaltılmıştır.

Doğum Tarihi	Cinsiyet	Posta Kodu	Hastalık Adı	Hasta Sayısı
≥ 1970	E	3440*	Grip	80
≥ 1970	E	3440*	Kanser	10
≥ 1970	E	3440*	Tansiyon	70
1975 ≤ x ≤1985	E	3440*	Baş Ağrısı	20
1975 ≤ x ≤1985	E	3440*	Beyin Tümörü	10
1975 ≤ x ≤1985	E	3440*	Hepatit-B	10

Tablo 3.22. T-Yakınlık Sonucu Elde Edilen Veri Kümesi

3.2. Anonim Hale Getirme Yönteminin Seçilmesi

Veri sorumluları yukarıdaki yöntemlerden hangilerinin uygulanacağına ellerindeki verilere bakarak karar verirler. Anonim hale getirme yöntemleri uygulanırken sahip olunan veri kümesine dair aşağıdaki özelliklerin de veri sorumluları tarafından dikkate alınması tavsiye edilir:

- Verinin niteliği,
- Verinin büyüklüğü,
- Verinin fiziki ortamlarda bulunma yapısı,
- Verinin çeşitliliği,
- Veriden sağlanmak istenen fayda / işleme amacı,
- Verinin işlenme sıklığı,
- Verinin aktarılacağı tarafın güvenilirliği,
- Verinin anonim hale getirilmesi için harcanacak çabanın anlamlı olması,
- Verinin anonimliğinin bozulması halinde ortaya çıkabilecek zararın büyüklüğü, etki alanı,
- Verinin dağıtıklık/merkezilik oranı,
- Kullanıcıların ilgili veriye erişim yetki kontrolü,
- Anonimliği bozacak bir saldırı kurgulanması ve hayata geçirilmesi için harcayacağı çabanın anlamlı olması ihtimali.

Bir veriyi anonim hale getirdiğini düşünen veri sorumlusu, kişisel veriyi aktardığı diğer kurum ve kuruluşların bünyesinde olduğu bilinen ya da kamuya açık bilgilerin kullanılması ile söz konusu verinin yeniden bir kişiyi tanımlar nitelikte olup olmadığını, yapacağı sözleşmelerle ve risk analizleriyle kontrol etmek sorumluluğundadır.

3.3. Anonimlik Güvencesi

Bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilebilmesi için aşağıdaki şartların yerine getirilmesi gereklidir. Bu şartların yerine getirilmiş olmasını veri sorumluları sağlamalıdır:

- Anonim hale getirilmiş veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin bozulamaması,
- Bir ya da birden fazla değerin bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturamaması,
- Anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi.

Bu riskler sebebiyle veri sorumlularının, anonim hale getirdikleri veri kümeleri üzerinde bu maddede sıralanan özellikler değiştikçe kontroller yapmaları ve anonimliğin korunduğundan emin olmaları gerekmektedir.

3.4. Anonim Hale Getirilmiş Verilerin Tersine İşlem İle Anonimleştirmenin Bozulmasına Dair Riskler

Anonim hale getirme işlemi, kişisel verilere uygulanan ve veri kümesinin ayırt edici ve kimliği belirleyici özelliklerini yok etme işlemi olduğundan bu işlemlerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski bulunmaktadır. Bu durum anonimliğin bozulması olarak ifade edilir.

Anonim hale getirme işlemleri yalnızca manuel işlemlerle veya otomatik geliştirilmiş işlemlerle ya da her iki işlem tipinin birleşiminden oluşan melez işlemlerle sağlanabilir. Ancak önemli olan anonim hale getirilmiş verilerin paylaşıldıktan veya açıklandıktan sonra veriye erişebilen veya sahip olan yeni kullanıcılar tarafından anonimliğin bozulmasını engelleyecek önlemlerin alınmış olmasıdır.

Anonimliğin bozulmasına dair bilinçli olarak yürütülen işlemlere “anonimliğin bozulmasına yönelik saldırılar” denilmektedir. Bu saldırılar farklı profildeki kullanıcılar tarafından farklı motivasyonlarla gerçekleşebilmektedir.

Saldırıların motivasyonlarını aşağıdaki başlıklarda toplayabiliriz:

- Anonimliğin derecesini ve güvenilirliğini test etmek amacıyla yapılan saldırılar,
- Kurumları, şirketleri, organizasyonları, belirli bir kişiyi veya topluluğu zor durumda bırakmaya ve itibar riski yaratmaya yönelik saldırılar,
- Anonimliğin bozulması sonucu ortaya çıkacak kişisel verilerden ve elde edilebilecek değerlerden maddi veya manevi fayda sağlama amacıyla yapılan saldırılar.

Yukarıda sıralanan senaryoların farklılığına bağlı olarak saldırıları yürüten kullanıcıların profilleri ve erişim yetkileri de değişkenlik göstermektedir. Bu kişiler aşağıda listelenen örneklerdeki profillere sahip olabilirler:

- Kamuya açılmış veriye erişimi olan genel bir kullanıcı,
- Yazılım, istatistik, veri madenciliği konularında uzmanlaşmış bir profesyonel, akademisyen veya araştırmacı,
- Kuruluş, şirket, organizasyon içinde çalışan veya sistemlere erişim hakkı olan bir kullanıcı,
- Anonim hale getirilmiş veriyi kullanarak çalışan ancak diğer bazı verilere veya sistemlere erişimi olan kullanıcı,
- Açıklanmış /paylaşılmış veri kümesinde yer aldığını bildiği bir kişinin yakını, aile üyesi veya arkadaşı.

Saldırıların sonucunda başarılı olunmuş ve anonimlik bozulmuşsa ortaya çıkan kişisel veriye dair üç farklı senaryo oluşmaktadır. Bu senaryolar;

- Gerçek kişinin kimliğinin tamamen ortaya çıkmış olması,
- Gerçek kişiye ait belli bir bilginin ortaya çıkmış olması,
- Bir kişiye dair varsayımsal bir bilginin ortaya çıkmış olması,

olarak sayılabilir.

Kişinin kimliğinin tamamen ortaya çıkmış olması durumu, çoğunlukla saldırganın elindeki anonim hale getirilmiş veriyi elde ettiği veya erişiminin olduğu bir başka veri kümesiyle birleştirmesinden veya doğrudan tanımlayıcılar yerine kullanılan kod veya takma isimlerin kodlamalarının bozulmasından kaynaklanabilir. Böyle bir durumda gerçek kişinin doğrudan tanımlayıcılarına ulaşılır ve kimlik tamamen saptanabilir hale gelir.

Bazı hallerde kimlik tamamen tespit edilebilir hale gelmese de bir kişinin ilgili anonim hale getirilmiş veri kümesi içinde yer aldığını bilen bir kullanıcı anonim hale getirilmiş veri kümesinin dar bir tanımlama yapıyor olmasından ötürü o kişiye ait bir özelliğini ortaya çıkartabilir. Örneğin, bir hastanenin 20 yaşındaki tüm kadın hastalarına dair tek bir teşhis ve tedavi bilgisi paylaşıyor olması halinde, tanıdığı 20 yaşındaki kadının o hastanede tedavi edildiğini bilen bir kişi, tanıdığı kişinin hastalığını öğrenmiş olmaktadır. Bu halleri engelleyebilmek için hastanenin sadece 20 yaşındaki kadın hastalar yerine yaş aralığını ve cinsiyeti genişleterek ve teşhis ve tedavi bilgilerinin çeşitlenmesini sağlayacak önlemler alması ve tekil olarak belli bir kişinin ayırt edilebilme ihtimalini düşürmesi gerekmektedir.

Buna benzer şekilde, özellikle belli bir sınıf, grup veya topluluğa dair çok kesin ve çeşitliliği az olan tekil bilgilerin açıklanıyor veya paylaşılıyor olması halinde o gruba, sınıfa veya topluluğa mensup olduğu bilinen kişilerle ilgili varsayımsal sonuçlar çıkartılmasına mahal verilecektir. Örneğin; belli bir coğrafi bölgede yaşayan bireyler için bir kamu organının tek bir hastalığa dair yüksek oranlar paylaşmış olması o coğrafyada seyahat etmiş tüm insanlara dair varsayımlar yürütülmesini sağlayacaktır.

Bu kapsamda, anonim hale getirilmiş kişisel verilerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski olup olmadığı araştırılarak ona göre işlem tesis edilmelidir.

IV. REHBER HAZIRLANIRKEN FAYDALANILAN **KAYNAKLAR** ve **İNCELENMESİNİN UYGUN OLACAĞI DEĞERLENDİRİLEN DOKÜMANLAR**

Article 29 29.Madde Veri Koruma Grubu, Opinion 4/2007 on the concept of personal data, 2007, bkz. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Article 29 29.Madde Veri Koruma Grubu, Opinion 5/2014 on Anonymisation Techniques, bkz. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_ en.pdf

Bacak A.Bacak, Gizliliği Koruyarak Veri Yayınlamak İçin K-Anonimity ve L-Diversity Metodları, 2013, bkz. https://www.bilgiguvenligi.gov.tr/siniflandiril mamis/gizliligi-koruyarak-veri-yayinlamak-icin-k-anonimity-ve-l-diversity-metodlari.htm

Barbaro/ Zeller M.Barbaro, T.Zeller, A Face is Exposed for AOL Searcher No. 4417749, New York Times, bkz. http://www.nytimes.com /2006/08/09/technology/09aol.html?pagewanted=all&_r=0

Barth-Jones D.C.Barth-Jones, The Re-Identification of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now (2012). Available at SSRN: http://ssrn.com/abstract=2076397 or http://dx.doi.org/10.2139/ssrn.2076397

Brown/Marsden I.Brown, C.T. Marsden, Regulating Code: Good Governance and Better Regulation in the Information Age, The MIT Press, 2013

Castells M.Castells, Ağ Toplumunun Yükselişi, Birinci Cilt, çev. E.Kılıç, İstanbul Bilgi Yayınları, 2005

Cavoukian/ El Emam A.Cavoukian, K.El Emam, De-identification Protocols:Essential for Protecting Privacy, Privacy by Design, June 25, 2014. https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-de-identifcation_essential.pdf

Cavoukian A.Cavoukian, Privacy By Design, Take the Challenge, Canada, 2009

Christen/ Alfano/ Bangerter/ Lapsley M.Christen, M.Alfano, E.Bangerter, D.Lapsley, Ethical Issues of Morality Mining: Moral Identity as a Focus of Data Mining, Ethical Data Mining Applications for Socio- Economic Development, IGI Global, 2013

Chunara/ Andrews/ Brownstein R.Chunara, J.R.Andrews, J.S. Brownstein, Social and News Media Enable Estimation of Epidemiological Patterns Early in the 2010 Haitian Cholera Outbreak, The American Society of Tropical Medicine and Hygiene,2010,bkz. http://healthmap.org/documents /Chunara_AJTMH_2012.pdf

Clifton/ Tassa C.Clifton, T.Tassa, On Syntactic Anonymity and Differential Privacy, 2013 Trans. Data Privacy 6, 2 (2013), 161-183.

Demirci İ.Demirci, T-Closeness Metodu Gizliliği Koruyarak Veri Yayınlamak İçin, 2014 bkz. http://www.phphocam.com/t-closeness- metodu-gizliligi-koruyarak-veri-yayinlamak- icin/#sthash.z70qZ2sb.dpuf

Digital Rights Ireland and Seitlinger Judgment in Joined Cases C-293/12 and C- 594/12,Digital Rights Ireland and Seitlinger and Others, Court of Justice of the European Union , Press Release No 54/14, Luxembourg, 8.4.2014

Directive 95/46/EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Oficial Journal of the European Communities of 23 November 1995, No L. 281, s. 31.

Directive 2002/58/EC Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and protection of privacy in the electronic communications sector OJ L201/37

Divanis / Loukides A.G.Divanis, D.G.Loukides, Medical Data Privacy Handbook, Springer 2015

Doyle/ Lane P. Doyle, J. Lane, Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies, North-Holland Publishing, Dec 31, 2001

El Emam K.El Emam, Guide to the de-identification of Personal Health Information, CRC Press, 2013

El Emam/ Arbuckle K.El Emam, L.Arbuckle, Anonymizing Health Data, O'Reilly, Cambridge, MA. 2013

European Statistical System Project (ESSNet) A.Hundepool, J.Domingo-Ferrer, L.Franconi, S.Giessing, E.S. Nordholt, K.Spicer, P.P. Wolf, Handbook on Statistical Disclosure Control Version 1.2, ESSNet, 2010

European Statistical System Project (ESSNet) A.Hundepool, A. De Wetering, R.Ramaswamy, L.Franconi, S.Polettini, A.Capobianchi, P.P.de Wolf, J.Domingo, V.Torra, R.Brand, S.Giessing, μ-ARGUS version 4.2 User's Manuel, ESSNet-Project, 2008

Fayyoumi/ Oommen E.Fayyoumi, B.J.Oommen, A survey on statistical disclosure control and micro-aggregation techniques for secure statistical databases. 2010, Software Practice and Experience. 40, (2010), 1161-1188. DOI=10.1002/spe.v40:12 http://dx.doi.org/10.1002/spe.v40:12

Fung/ Wang/ Chen/ Yu B.C.M.Fung, K.Wang, R.Chen, P.S.Yu, Privacy-Preserving Data Publishing: A Survey on Recent Developments, Computing Surveys, June 2010

Garfinkel S.L.Garfinkel NISTIR 8053 De-Identification of Personal Information, 2015 bkz. https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2015/10/NIST.IR_.8053.pdf

Gözüküçük M.Gözüküçük, Veri İşleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirmesi İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Yüksek Lisans Programı (Bilişim Hukuku), 2014

Gür İ.Gür, Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar, Turhan Kitabevi, 2010

Gürses/ Danezis S.Gürses, G.Danezis, A Critical Review of Ten Years of Privacy Technology, UK, 2012

Gürses/ Troncoso/ Diaz S.Gürses, C.Troncoso, C.Diaz, Engineering Privacy by Design, International Conference on Privacy and Data Protection (CPDP) Book,

Hilbert M.Hilbert, Big Data for Development: From Information- to Knowledge Societies, United Nations ECLAC, 2013

Honer J.Honer, U.S. government commits big R&D money to 'Big Data', bkz.http:// www.zdnet.com/blog/btl/u-s- government-commits-big-r-andd-money-to-big- data/72760

Hunter/Letterie J.Hunter, J.Letterie, IBM harnesses power of Big Data to improve Dutch flood control and water management systems, bkz. http://www- 03.ibm.com/ press/us/en/pressrelease/41385.wss

ICO Enformasyon Komiserliği Ofisi, Privacy by Design, 2008, bkz. http://ico.org. uk/for_organisations/data_protection/ topic_guides/~/ media/documents/ pdb_report_html/ PRIVACY_BY_DESIGN_REPORT_V2.ashx

ICO Enformasyon Komiserliği Ofisi, Anonymization: Managing Data Protection Risk Code of Practice, 2012.bkz. http://ico.org.uk/for_ organisations/data_ protection/topic_guides/anonymisation

ICO Enformasyon Komiserliği Ofisi, Anonymisation: Managing data protection risk, Code of Practice 2012, Information Commissioner's Office. https://ico. org.uk/media/for- organisations/documents/1061/ anonymisation-code. pdf.

Irzık G.Irzık, "Bilgi Toplumu mu, Enformasyon Toplumu mu? Analitik-Eleştirel Bir Yaklaşım", Bilgi Toplumuna Geçiş Sorunlar Görüşler Yorumlar Yorumlar

Koot M.R.Koot, Measuring and Predicting Anonymity, Gildeprint Drukkerijen, 2012

Korff D.Korff, Comperative Study on Different Approaches to New Privacy Challanges, In Particular in the Light of Technological Developments, Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in meeting the

challanges posed by global social and technical developments, London Metropolitan University, 2010,bkz. http://ec.europa.eu/ justice/policies/ privacy/ docs/studies/new_privacy_challenges/ final_report_working_ paper _2_en.pdf

Krishnan K.Krishnan, Data Warehousing in the Age of Big Data, Newnes, 2013

Küzeci E.Küzeci, Kişisel Verilerin Korunması, Turhan Kitabevi, 2010

Lagos / Polonetsky Y.Lagos, J.Polonetsky, Public vs. Nonpublic Data: The Benefits of Administrative Controls, Stanford Law Review Online, 66:103, Sept. 3, 2013

Laney D.Laney, 3D Data Management: Controlling Data Volume, Velocity and Variety, META Group, 2001. Bkz. http://blogs.gartner.com/doug- laney/ files/2012/01/ad949-3D-Data-Management- Controlling-Data-Volume-Velocity-and- Variety.pdf

Lessig L.Lessig, Code Version 2.0, Basic Books, 1996

Levine/Roos J.H. Levine, H.B. Roos, Introduction to Data Analysis:The Rules of Evidence, bkz. http://www.dartmouth.edu/~mss/docs/Volume s_1-2.pdf

Li/Li/ Venkatasubramanian N.Li, T.Li, S.Venkatasubramanian, t-Closeness: Privacy beyond k-Anonymity and l-Diversity, Data Enginering (ICDE) IEEE 23rd International Conference,

Machanavajjhala/ Gehrke/ Kifer A.Machanavajjhala, J.Gehrke, D.Kifer, l-Diversity: Privacy Beyond k-Anonymity, Cornell University, 2007

McCallister/ Grance/ Scarfone E.McCallister, T.Grance, K.Scarfone, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122, National Institute of Standards and Technology, U.S. Department of Commerce, 2010

Moore R.A. Moore Jr, Controlled Data-Swapping Techniques for Masking Public Use Microdata Sets, US Bureau of the Census Washington, 1996

Morozov E.Morozov, The Net Delusion: How not to Liberate World, Penguin Books, 2011

Narayanan/ Shmatikov A.Narayanan, V.Shmatikov, How to Break Anonymity of the Netflix Prize Dataset, The Universtiy of Texas, 2008

Ohm P.Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, Vol 57, 2010

Oram A.Oram, The Information Technology Fix For Health, OReilly, 2014

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

Özmen Ş.I.Özmen, Ağ Ekonomisinde Yeni Ticaret Yolu: E-Ticaret, İstanbul Bilgi Üniversitesi Yayınları, 2012

Pfitzmann/ Hansen A.Pfitzmann, M.Hansen, Anonymity, Unobservability, Pseudonymity, and Identity Management:A Proposal for Terminology, bkz. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.18.pdf

Schmarzo B.Schmarzo, Big Data:Understanding How Data Powers Big Business, Wiley, 2013

Simon P.Simon, Too Big To Ignore:The Business Case for Big Data, Wiley, 2013

Spiekerman/ Cranor S.Spiekerman, L.F.Cranor, Engineering Privacy, IEEE Transactions on Software Engineering, Vol. 35, Nr. 1, 2009

Stream Computing Bulletin of IEEE A.Biem, E.Bouillet, H.Feng, A.Ranganathan, A.Riabov, O. Verscheure, H.Koutsopoulos, M.Rahmani, B.Güç, Real-Time Traffic Information Management using Stream Computing, bkz. http://sites.computer.org/debull/A10june/Anan d.pDf

Sweeney L.Sweeney, k-Anonymity: A Model for Protecting Privacy, Carnegie Mellon University, 2002

Swire/ Ahmad P.P.Swire, K.Ahmad, Foundations of Information Privacy and Data Protection,IAPP , 2012

Şimşek O.Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta Basım, 2008

Vural Y.Vural, ρ-Kazanım: Mahremiyet Korumalı Fayda Temelli Veri Yayınlama Modeli Doktora Tezi, Hacettepe Üniversitesi Bilgisayar Mühendisliği. 2017

Yakowitz J.Yakowitz, Tragedy of Data Commons, Harvard Journal of Law and Technology, Vol.25, 2011

Warren/Brandeis S.D.Warren, L.D.Brandeis, The Right to Privacy, Harvard Law Review, 1890

Wolfe/ Gunasekara/ Bogue N.Wolfe, L.Gunasekara, Z.Bogue, Crunching Digital Data can help the World, 2011,http://edition.cnn.com/2011/OPINION/02/02/wolfe.gunasekara.bogue.data/index.html?_s=PM:O PINION

Wu F.T.Wu, Defining Privacy and Utility in Data Sets, University of Colorado Law Review 1117 (2013)