

İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

BAĞLANABİLİR ARAÇLARDA VERİ İŞLENMESİ

Yağmur Ekin KOÇ ÇAYLI

119691012

Dr. Öğr. Üyesi Tayfun ACARER

İSTANBUL

2024

Bağlanabilir Araçlarda Veri İşlenmesi

Data Processing in Connected Vehicles

Yağmur Ekin KOÇ ÇAYLI

119691012

Tez Danışmanı : Dr. Öğr. Üyesi Tayfun ACARER

Piri Reis Üniversitesi

Jüri Üyeleri : Prof. Dr. Leyla KESER BERBER

İstanbul Bilgi Üniversitesi

Doç. Dr. Mehmet Bedii KAYA

İstanbul Bilgi Üniversitesi

Tezin Onaylandığı Tarih : 10.09.2024

Toplam Sayfa Sayısı : 170

Anahtar Kelimeler (Türkçe)

- 1) Kişisel Veriler
- 2) Bağlanabilir Araç
- 3) Veri Güvenliği
- 4) Veri Aktarımı
- 5) Kişisel Verilerin İşlenmesi

Anahtar Kelimeler (İngilizce)

- 1) Personal Data
- 2) Connected Vehicle
- 3) Data Security
- 4) Data Transfer
- 5) Processing of Personal Data

İÇİNDEKİLER

İÇİNDEKİLER	iii
KISALTMALAR	vi
ŞEKİL LİSTESİ.....	ix
ÖZET.....	x
ABSTRACT	xi
GİRİŞ	1
BİRİNCİ BÖLÜM: YASAL GELİŞMELER.....	3
1.1 KİŞİSEL VERİLERİN KORUNMASI ALANINDA AVRUPA'DAKİ GELİŞMELER.....	4
1.2. ÜLKEMİZDE KİŞİSEL VERİLERİN KORUNMASI ALANINDAKİ GÜNCEL GELİŞMELER.....	7
1.3. AB VERİ YASASI	12
1.4. AB YAPAY ZEKA YASASI.....	23
1.5. NIS2 DİREKTİFİ	30
1.6. AB SİBER DAYANIKLILIK YASASI.....	35
1.7. YASAL GELİŞMELERİN BAĞLANABİLİR ARAÇLARDA VERİ İŞLENMESİ KAPSAMINDA İNCELENMESİ.....	37
İKİNCİ BÖLÜM: VERİ İŞLEME VE BAĞLANABİLİR ARAÇLAR	49
2.1. BAĞLANABİLİR ARAÇLAR: TANIM VE ÖZELLİKLER.....	49
2.2. BAĞLANABİLİR ARAÇ TEKNOLOJİSİNDEKİ GÜNCEL GELİŞMELER.....	52
2.3. BAĞLANABİLİR ARAÇLARIN KULLANIMI İLE İŞLENEN KİŞİSEL VERİLER.....	54
2.3.1. Konum Verisi.....	59
2.3.2. Biyometrik Veri.....	61
2.3.3. Cezai Suçları veya Diğer İhlalleri Ortaya Çıkaran Veriler	63
2.4. BAĞLANABİLİR ARAÇLARIN KULLANIMI İLE İŞLENEN KİŞİSEL VERİLERİN İŞLEME AMAÇLARI.....	65

2.5. BAĞLANABİLİR ARAÇLARIN KULLANIMI İLE KİŞİSEL VERİLERİN TOPLANMA YÖNTEMLERİ VE VERİ İŞLEMENİN HUKUKİ SEBEPLERİ	70
2.5.1. Veri İşlemenin Açık Rızaya Dayanması.....	73
2.5.2. Veri İşlemenin Sözleşmenin İfası İçin Gerekli Olması	80
2.6. İLGİLİ KİŞİ HAKLARI.....	89
2.7. KİŞİSEL VERİ AKTARIMI	94
2.7.1. Üçüncü Taraflara Veri Aktarımı Yapılması	95
2.7.2. Yurt Dışına Veri Aktarımı Yapılması	98
ÜÇÜNCÜ BÖLÜM: BAĞLANABİLİR ARAÇLARDA KİŞİSEL VERİ GÜVENLİĞİ	101
3.1. BAĞLANABİLİR ARAÇ TEKNOLOJİLERİNİN KULLANILMASINDAKİ RİSKLER.....	101
3.1.1. IoT Sistemlerinin Uygun Kullanılmaması	102
3.1.2. Konum Verisinin Mevzuat Düzenlemelerine Uygun İşlenmemesi	103
3.1.3. İlgili Kişinin Uygun ve Eksiksiz Şekilde Aydınlatılmaması	105
3.2. KİŞİSEL VERİ GÜVENLİĞİ TEMEL İLKELERİ	110
3.2.1. Veri Minimizasyonu.....	110
3.2.2. Tasarımla Veri Koruma ve Varsayılan Ayarlarla Veri Koruma	113
3.2.3. Anonimleştirme ve Takma Adlı Hale Getirme.....	116
3.2.4. Lokal Veri İşleme	120
3.2.5. Veri Koruma Etki Analizi	121
3.3. BAĞLANABİLİR ARAÇLARDA KİŞİSEL VERİ GÜVENLİĞİ SORUNLARI.....	124
3.4. VERİ GÜVENLİĞİ RİSKLERİ VE TEDBİRLER.....	126
3.5. VERİ GÜVENLİĞİ ÖRNEK SENARYOLARI	133
3.5.1. Veri Güvenliği Tehditleri ve Yaşanmış Saldırıları	133
3.5.2. Kazalara Yönelik Raporlama Çalışması.....	136
3.5.3. Araç Hırsızlığı ile Mücadele	138
3.5.4. E-Call Sistemi	139

3.5.5. Verilerin Araçta Otomatik Bir İşlem Tetiklemek İçin Uzaktan Hizmet Sağlayıcısına Aktarılması.....	140
SONUÇ.....	144
KAYNAKÇA	147



KISALTMALAR

AB	: Avrupa Birliđi
ABAD	: Avrupa Birliđi Adalet Divanı (<i>Court of Justice of the European Union</i>)
AEA	: Avrupa Ekonomik Alanı
AİHS	: İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme
bkz.	: Bakınız
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
CLEPA	: Avrupa Otomotiv Tedarikçileri Birliđi
CNIL	: Commission Nationale de l'Informatique et des Libertés (<i>Fransız Veri Koruma Otoritesi</i>)
CSIRT	: Computer Security Incident Response Team
EDPB	: European Data Protection Board (<i>Avrupa Veri Koruma Kurulu</i>)
EDPS	: European Data Protection Supervisor (<i>Avrupa Veri Koruma Denetçisi</i>)
ENISA	: European Union Agency for Network and Information Security (<i>Avrupa Birliđi Ağ ve Bilgi Güvenliđi Teşkilatı</i>)
e.t.	: Erişim Tarihi
EUROJUST	: European Union Agency for Criminal Justice Cooperation (<i>Avrupa Birliđi Adli İş Birliđi Teşkilatı</i>)
EUROPOL	: European Union Agency for Law Enforcement Cooperation (<i>Avrupa Birliđi Polis Teşkilatı</i>)
GDPR	: General Data Protection Regulation

*(2016/679 Sayılı Avrupa Birliđi Genel Veri Koruma
Tüzüğü)*

ISO	: International Organization for Standardization
Komisyon	: European Commission (Avrupa Komisyonu)
Kurul	: Kişisel Verileri Koruma Kurulu
Kurum	: Kişisel Verileri Koruma Kurumu
m.	: Madde
NIS Direktifi	: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
NIS2 Direktifi	: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148
OECD	: Organisation for Economic Co-operation and Development (İktisadi İş birliđi ve Kalkınma Teşkilatı)
PSAP	: Public Safety Answering Point
s.	: Sayfa
UAB	: Ulaştırma ve Altyapı Bakanlığı
UNECE	: United Nations Economic Commission for Europe (Birleşmiş Milletler Avrupa Ekonomik Komisyonu)
USOM	: Ulaştırma Siber Güvenlik Operasyon Merkezi
TCK	: 5237 Sayılı Türk Ceza Kanunu
vd.	: Ve Devamı, Ve Diğerleri
WP 29	: Working Party 29

(Madde 29 Çalışma Grubu)

108 nolu Sözleşme : 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Sözleşme no 108+ : Convention 108+

(Modernize Edilmiş 108 Sayılı Sözleşme)

KVKK : 6698 Sayılı Kişisel Verilerin Korunması Kanunu

95/46 sayılı Direktif : Data Protection Directive 95/46/EC

(95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktifi)

2002/58/EC sayılı Direktif : Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

ŞEKİL LİSTESİ

Şekil 2. 1. Bağlanabilir Araç Özellikleri Gelişimi.....	50
Şekil 2. 2. Bağlanabilir Araç Ekosistemi	51
Şekil 2. 3. Veri Sorumlusuna Başvuru Usulü	94
Şekil 2. 4. KVKK m.9 Yurt Dışına Veri Aktarım Yöntemleri	98
Şekil 3. 1. Bağlanabilir Araç Ekranlarında Sunulan Semboller	110



ÖZET

Dijital dönüşüm, otomotiv sektöründe bağlanabilir araçların kullanımını ve dijital dönüşüm etkisi, yeni iş modelleri ve işlenen kişisel veri hacimlerini artırmaktadır. Bağlanabilir araçlarda işlenen kişisel verilerdeki bu artış, kişisel verilerin korunmasının öneminin de gün geçtikçe artırmakta ve bu alanda yasal düzenleme ihtiyaçlarını doğurmaktadır.

“Bağlanabilir Araçlarda Veri İşlenmesi” başlıklı bu tez ile bağlanabilir araçlarda veri işleme süreçlerinin kişisel verilerin korunması kapsamında incelenmesi ve otomotiv sektöründeki veri sorumlularının dikkat etmesi gerekenlerin tespit edilmesi amaçlanmıştır.

Tez üç ana bölümden oluşmakta olup birinci bölümde kişisel veri koruma mevzuatları ve Avrupa Birliği ilgili diğer mevzuatları ışığında bağlanabilir araçlarda kişisel veri işlenmesi ele alınmıştır. İkinci bölümde bağlanabilir araçlardaki güncel gelişmeler ele alınmış olup ayrıca bağlanabilir araçlarda işlenen kişisel veriler, işlenme amaçları, hukuki sebepler, aktarım tarafları ve ilgili kişi hakları incelenmiştir. Üçüncü ve son bölümde ise kişisel veri mevzuatındaki temel ilkeler doğrultusunda veri güvenliği riskleri ve önleyici tedbirler ortaya konulmuştur.

Avrupa Birliği’ndeki sektör uygulamaları ve veri koruma otoriterinin yayımladığı rehberler doğrultusunda bağlanabilir araçlarda kişisel veri işleme faaliyetlerinin, sektördeki veri sorumlularınca kişisel verilerin korunması mevzuatıyla uyumluluğunun sağlanması amaçlanmıştır.

Anahtar Kelimeler: Kişisel Veriler, Bağlanabilir Araç, Veri Güvenliği, Veri Aktarımı, Kişisel Verilerin İşlenmesi

ABSTRACT

Digital transformation increases the use of connected vehicles in the automotive sector and the digital transformation effect increases new business models and the volumes of personal data processed. This increase of personal data processed in connected vehicles increases the importance of personal data protection every day and creates the need for legal regulations in this area.

The aim of this thesis, entitled 'Data Processing in Connected Vehicles', is to examine the data processing processes in connected vehicles from a personal data protection perspective and to identify what data controllers in the automotive sector should be aware of.

The thesis consists of three main chapters. In the first chapter, personal data processing in connected vehicles is analysed in the light of personal data protection legislation and other relevant legislation of the European Union. In the second part, current developments in connected vehicles are discussed. In addition, the second part analyses the personal data processed in connected vehicles, the purposes of the processing, the legal grounds, the parties to the transfer and the rights of the data subjects. The third and final part analyses data security risks and preventive measures in line with the principles of personal data legislation.

In line with sectoral practices in the European Union and the guidelines published by the data protection authorities, the objective is to ensure that the processing of personal data in connected vehicles by data controllers in the sector complies with personal data protection legislation.

Keywords: Personal Data, Connected Vehicle, Data Security, Data Transfer, Processing of Personal Data

GİRİŞ

Dijital dönüşüm pek çok farklı sektörde olduğu gibi otomotiv sektörü üzerinde de önemli ve kapsamlı bir etkiye sahiptir. Öyle ki, bağlanabilir araçlar ve sürüş deneyimindeki teknolojik gelişmeler günümüzde mobilitayı yeniden şekillendirmekte ve yeni çevrim içi iş modelleri oluşturmaktadır. Bu etki ile giderek daha fazla ekonomik önem kazanan ve artan veri hacimleri oluşmaktadır. Özellikle bağlanabilir araçlardan veri toplayan ve bu verilere erişimi olan hizmet sağlayıcılar için yeni pazar fırsatları oluşmakta ve araçlarla ilgili yeni geliştirmeler ve sunulan hizmet teklifleri optimize edilmektedir.

Bağlanabilir araçlardan toplanan veriler; teknik bilgi içermesi, verilerin araç tarafından veya araç sürücüsünün eylemlerinden kaynaklı oluşturulması önemli olmaksızın genel veri koruma yaklaşımına uygun olarak kimliği belirli veya belirlenebilir gerçek bir kişiye ait bilgileri içermesi sebebi ile kişisel veri¹ olarak adlandırılmaktadır. Ancak, araç sürücülerinin araç ve sürüş verilerinin hangi sınırdan işleneceği, bu verilerin hangi üçüncü taraflarla ve ne şekilde paylaşılacağı, ölçülülük, şeffaflık ve veri minimizasyonu ilkelerinin nasıl uygulanacağı ve veri güvenliğinin sağlanması için hangi teknik ve idari tedbir kontrollerinin yapılacağı hususlarında belirli bir yasal düzenlemenin olmaması pek çok konunun detaylı olarak incelenmesini zorunlu kılmaktadır.

Gelinen noktada bağlanabilir araçlar ve bu araçların kullanımından kaynaklı veri işlenmesi kaçınılmaz bir teknolojik gelişme olarak yeni düzenlemelerin yapılması zorunluluğunu doğurmuştur. Pek çok veri koruma otoritesi, bu alandaki inovatif ekosistemi desteklemenin yanı sıra araç sürücülerine ait kişisel verilerin korunması için çalışmalar yürütmekte ve rehberler yayımlamaktadır.

Bu tezde, bağlanabilir araçlarda veri işlenmesi kapsamında işlenen kişisel veriler dikkate alınarak bağlanabilir araçlarda veri işleme süreçlerinin kişisel verilerin korunması kapsamında baştan sona detaylı olarak incelenmesi hedeflenmektedir.

¹ 6698 sayılı Kişisel Verilerin Korunması Kanunu madde 3/1-e altında yer alan kişisel veri tanımı.

Tezdeki ana inceleme alanı Avrupa Birliđi Genel Veri Koruma Yönetmeliđi ile 6698 sayılı Kişisel Verilerin Korunması Kanunu ışığında bağlanabilir araçta kişisel verilerin işlenmesidir. Tez kapsamında yapılan incelemede 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Avrupa Birliđi Genel Veri Koruma Yönetmeliđi'ndeki yaklaşımlar ve ilgili düzenlemeler ortaya konulmakla beraber, iki mevzuatta yer alan farklılıklar da tartışılmaktadır. Söz konusu veri koruma mevzuatlarına ek olarak birinci bölümde ayrıca Avrupa Birliđi'ndeki veri işlenmesi ile ilgili diğerk mevzuatlar da ele alınmakta ve bağlanabilir araçlarda veri işlenmesi bakımından etkileri tartışılmaktadır.

Tez içerisinde inceleme üç ana başlık altında yapılmıştır. Birinci bölümde tezin ana inceleme kapsamını oluşturan kişisel veri koruma kavramı ve Avrupa Birliđi ve Türkiye'deki güncel kişisel veri koruma mevzuat gelişmeleri ve Avrupa Birliđi'ndeki veri işlenmesi ile ilgili diğerk mevzuatlar incelenmektedir. İkinci bölümde ise bağlanabilir araçlarda ve buna bağlı gelişen teknolojilerdeki güncel gelişmeler ele alınmaktadır. Ayrıca ikinci bölümde kişisel veri kavramı, bağlanabilir araçlarda işlenen veriler, işleme amaçları, hukuki sebepleri, verilerin aktarım tarafları ve ilgili kişi hakları özelinde ele alınmaktadır. Üçüncü ve son bölümde ise işlenen kişisel verilerin güvenliğinin sağlanması adına kişisel veri mevzuatında yer alan temel ilkelerin uygulanma alanları aktarılmaktadır. Son bölümde ayrıca bağlanabilir araçlarda karşılaşılan veri güvenliği riskleri ve bu risklerin sebepleri üzerinde durularak, çeşitli uygulama senaryoları üzerinden riskleri önleyici tedbirlerin neler olduđu incelenmektedir.

Tez kapsamında mevzuat incelemelerinin yanı sıra özellikle bağlanabilir araçlar ile ilgili Avrupa Birliđi'nde yayımlanan rehberler kapsamında yapılan incelemeler ile uygulamada araç üreticileri ve hizmet sağlayıcılar gibi veri sorumluları tarafından dikkat edilmesi gerekenlerin tespiti ve analizi hedeflenmektedir.

BİRİNCİ BÖLÜM

YASAL GELİŞMELER

Günümüzün yeni “altını”² olarak adlandırılan kişisel veriler, modern dünyanın en değerli varlıklarından biri haline gelmiştir. Bu veriler, kimliğimizden alışveriş alışkanlıklarımıza, finans bilgilerimizden parmak izimiz gibi biyometrik verilere kadar ilgili kişileri belirli veya belirlenebilir kılan her bilgiyi kapsamakta ve kullanım alışkanlıklarımızın etkisiyle dijital dünyada iz bırakmamızı sağlamaktadır.

Ancak bu değerli varlık, aynı zamanda yasal düzenlemeler aracılığıyla yüksek bir korumaya ihtiyaç duymaktadır. Kişisel verilerin yasal düzenlemelere aykırı bir şekilde işlenmesi, ifade özgürlüğü ve haberleşme özgürlüğü gibi temel hakların zedelenmesine, ilgili kişilerin veri işleme faaliyeti ve amaçları ile ilgili uygun şekilde bilgilendirilmemesine ve dolayısıyla kişisel veri işleme mevzuatlarında düzenlenen haklarını kullanamamalarına sebep olmaktadır. Teknolojinin gelişmesi, bilgiye erişimi kolaylaştırırsa da özel hayatın gizliliği ve mahremiyeti için yeni tehditler de yaratmaktadır. Teknolojik gelişmelerin yanı sıra verilerin elde edilme hızı da artmakta ve kullanılan elektronik cihazların geneli günümüzde veri üretimine sebebiyet vermektedir³. Verilerin elde edilmesinde ulaşılan bu hızla baş etmek de bir sorun olarak karşımıza çıkmaktadır. Bu bakımdan kişisel verilerin korunması alanındaki yasal düzenlemeler bu tehditlere karşı durarak özel hayatın korunması ve dijital dünyada güvenli bir alan oluşturulmasına yardımcı olmaktadır. Yasal düzenlemelere paralel olarak yasal düzenlemelerin doğru uygulanmasını ve ilgili kişi haklarının korunmasını temin etmek adına Kişisel Verileri Koruma Kurumu ve Avrupa Veri Koruma Otoritesi (“European Data Protection Board”) (“EDPB”) gibi yetkili otoritelerin kurulması da önemlidir.

²<https://www.forbes.com/sites/forbestechcouncil/2023/03/27/how-to-make-use-of-the-new-gold-data/> (e.t. 29.10.2020)

³ **Mesut Serdar Çekin**, 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi, İÜHFİM, C. LXXIV, S. 2, 2016, 629-644, s.630;

1.1 KİŞİSEL VERİLERİN KORUNMASI ALANINDA AVRUPA'DAKİ GELİŞMELER

Teknolojinin ve küresel ticaretin hızla gelişmesi, kişisel verilerin korunması konusunu ulusal sınırların ötesine taşımıştır. Ülkelerin kendi yasaları, artan veri akışı karşısında yetersiz kalmaya başlamış olup, kişisel verilerin korunması, günümüzde küresel bir sorun haline gelmiştir. Farklı ülkelerde uygulanan kişisel veri koruma kanunlarının ve ikincil mevzuatın birbirinden farklı olması ve her ülkenin kişisel veriler için koyduğu sınırlamaların kapsam ve içeriğinin çeşitlilik göstermesi, özellikle ülkeler arası veri aktarımlarında önemli engellere yol açmaktadır. Bu durum birbirinden farklı mevzuatlara tabi olan ülkeler arasındaki veri aktarımlarını karmaşık ve zor hale getirmektedir. Bu sorunun çözümü için uluslararası iş birliği ve ortak düzenlemelere ihtiyaç duyulmaktadır. Kişisel verilerin korunması alanındaki yasal düzenlemelerde küresel bir anlayışın yerleşmesi adına Ekonomik İş birliği ve Kalkınma Örgütü (“Organization for Economic Cooperation and Development”) (“OECD”), Birleşmiş Milletler, Avrupa Konseyi⁴ ve Avrupa Birliği gibi kuruluşlar rehber ilkeler⁵ ve bağlayıcı yasal düzenlemeler ortaya koymaktadır⁶. Uluslararası düzenlemeler, ilgili kişi haklarının daha iyi korunması, veri işleyenler için adil bir rekabet ortamı oluşturulması ve

⁴ Avrupa İnsan Hakları Sözleşmesi, kişisel verilerin korunması ile ilgili açık bir hüküm içermemektedir. Ancak, kişisel verilerin korunması hakkının kişilik haklarıyla ilişkisi değerlendirilerek düzenlenmesinin amacı göz önüne alındığında, bu hakkın AIHS’in 8. maddesinde sayılan hakların bir parçası olduğu kabul edilecektir. 4 Kasım 1950 tarihinde kabul edilen Avrupa İnsan Hakları Sözleşmesi’nin (AIHS) “Özel ve aile hayatına saygı hakkı” başlıklı 8. maddesi: (1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

⁵ OECD, 1980 yılında kişisel verilerin korunması konusunda bağlayıcı olmayan kendi rehber ilkelerini yayımlamıştır. Guidelines on the protection of privacy and transborder flows of personal data, Eylül, 1980, ilgili rehbera ulaşmak için: <https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1712410558&id=id&accname=guest&checksum=966017718BF7B781F54D210627D333B9> (e.t. 05.03.2024).

⁶ Nevzat Ali Anı, “Kişisel Verilerin İşlenmesi ve Açık Rıza”, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 2018, (“Anı”) s. 6, ilgili teze ulaşmak için: <http://nek.istanbul.edu.tr:4444/ekos/TEZ/58103.pdf> (E.t. 25.03.2024).

küresel ticaret ve veri akışının kolaylaşması yoluyla kişisel verilerin korunmasında daha tutarlı ve etkin bir yaklaşım sağlamaktadır.

Kişisel verilerin korunması alanında yapılan ilk somut düzenleme, 1981 yılında kabul edilen “108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunmasına Dair Sözleşme”dir (“108 nolu Sözleşme”)⁷. 108 nolu Sözleşme’ye Avrupa Konseyi üye ülkelerinin yanı sıra üye olmayan ülkeler de taraf olabilmektedir ve imzalayan üye devletler açısından bağlayıcıdır. Türkiye, 28 Ocak 1981 tarihinde 108 nolu Sözleşme’yi imzalayan ilk ülkelerden birisi olmuş; bu sözleşme, Resmi Gazete’de yayımlanarak iç hukuka dâhil edilmiştir⁸. Kapsayıcı ve etkin bir koruma sağlamamakla birlikte 108 nolu Sözleşme, kişisel verilerin korunmasında önemli bir kilometre taşı olan ve hukuken bağlayıcılığı olan ilk uluslararası belge olarak önemli bir düzenlemedir⁹. 108 nolu Sözleşme’nin amacı, üye ülkelerin iç hukukta benzer düzenlemeleri kabul ederek ilgili kişilerin temel hak ve özgürlüklerinin, özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayatın gizliliği hakkının güvence altına alınmasının sağlanmasıdır¹⁰.

108 nolu Sözleşme, Avrupa Konseyi’nin 108 sayılı Kişisel Verilerin İşlenmesine İlişkin Olarak Bireylerin Korunması Sözleşmesi’ni yenileyen protokolün 18 Mayıs 2018’de Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilmesi ile Sözleşme No 108+ olarak güncellenmiştir. Sözleşme No 108+, daha güçlü bir veri koruma mekanizmasını öngörmekte ve bilişim teknolojilerindeki gelişmeleri dikkate alarak güncellenmemiş haline kıyasla önemli farklılıklar taşımaktadır¹¹.

⁷ **Avrupa Konseyi**, Kişisel Verilerin Otomatik İşlenmesine İlişkin Olarak Bireylerin Korunması Hakkındaki Avrupa Konseyi Sözleşmesi (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), T. 28.01.1981, No:108, ilgili sözleşmeye ulaşmak için: <https://rm.coe.int/1680078b37> (e.t. 05.03.2024)

⁸ RG T. 17.03.2016, S. 29656.

⁹ **Ayşe Çiğdem Ayözger**, “Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması”, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, İstanbul, 2016, (yayımlanmamış doktora tezi) s. 74 (e.t. 05.04.2024).

¹⁰ **Özer Deniz**, s. 26.

¹¹ **Elif Küzeci**, “Avrupa Konseyi’nin 108 sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter kararı ve diğer bazı gelişmelere ilişkin bir değerlendirme”, Medium,

Kişisel verilerin korunması konusunda Avrupa Birliği (“AB”) öncü bir rol oynamaktadır. 1990’lı yıllarda başlayan çalışmalar sonucunda, bireylerin kişisel verilerin işlenmesi ve serbest dolaşımı karşısında korunmasına ilişkin Avrupa Parlamentosu’nun 24 Ekim 1995 tarihli ve 95/46/EC sayılı Direktifi (“95/46 Sayılı Direktif”) kabul edilmiştir. 95/46 Sayılı Direktif, ulusal yasalarda ve 108 nolu Sözleşme’de yer alan veri koruma ilkelerini yansıtırken, genellikle bunları genişletmektedir¹². Bu direktif, uzun yıllar boyunca AB ülkelerinde kişisel verilerin korunmasına ilişkin temel çerçeveyi oluşturmuş olsa da 95/46 Sayılı Direktif’in yürürlüğe girmesinden sonra her üye devlet, 95/46 Sayılı Direktif’e uygun olmakla birlikte kendi iç hukukunda kişisel verileri korumaya yönelik farklı kanuni düzenlemeler yapmıştır. Bu da 95/46 Sayılı Direktif’in üye devletler arasında ortak şekilde uygulanabilmesinin önüne geçmiş ve benzer veri işleme faaliyetlerinin farklı sonuçlarının doğmasına sebep olmuştur¹³.

AB ülkelerinin iç hukuklarında yaşanan uygulama farklılıklarının sona erdirilmesi ve AB’nin “Dijital Tek Pazar Stratejisi”nin uygulanabilmesi¹⁴ için 27 Nisan 2016 tarihli ve 2016/679 sayılı “Kişisel Verilerin İşlenmesi ve Verilerin Serbest Dolaşımında Gerçek Kişilerin Korunmasına ve 95/46/EC sayılı Direktif’in Yürürlükten kaldırılmasına Dair”¹⁵ Tüzük (“General Data Protection Regulation”) (“GDPR”) 4 Mayıs 2016 tarihinde yayımlanıp 25 Mayıs 2018 tarihinde yürürlüğe girmiştir¹⁶. GDPR ve 95/46/EC sayılı Direktif arasındaki önemli farklardan biri, GDPR’ın doğrudan uygulanabilir olmasıdır. 95/46/EC sayılı Direktif ile güdülen

Temmuz, 2018, ilgili yazıya ulaşmak için: <https://medium.com/@elfkzc/avrupa-konseyinin-108-say%C4%B1%C4%B1-ki%C5%9Fisel-verilerin-korunmas%C4%B1-s%C3%B6zle%C5%9Fmesi-yenilendi-bc8daad9decc> (e.t. 05.04.2024).

¹² **FRA**, Avrupa Veri Koruma Mevzuatı El Kitabı, Nisan, 2018, (Türkçe Tercümesi İstanbul Bilgi Üniversitesi, Mart, 2020), s. 26. İlgili metne ulaşmak için: https://itlaw.bilgi.edu.tr/media/2020/3/30/Bilgi_Avrupa_Veri_Koruma_Mevzuat%C4%B1_El_Kitab%C4%B1_2018_TR_v01_16022019.pdf (e.t. 05.04.2024).

¹³ **Özer Deniz**, s. 27.

¹⁴ **European Commission**, Questions and Answers - Data protection reform, Aralık, 2015, x İlgili metne ulaşmak için: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_6385 (E.t. 05.04.2024).

¹⁵ GDPR maddelerine ulaşmak için: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (e.t. 05.04.2024).

¹⁶ **Seldağ Günes Peschke, Lutz Peschke**, “Artificial Intelligence and the New Challenges for EU Legislation”, Yıldırım Beyazıt Hukuk Dergisi, Ağustos, 2022, s. 1273.

üye devletlerde geçerli olacak asgari veri koruma ölçütlerinin belirlenmesi amacı¹⁷ GDPR ile çok daha somut şekilde sağlanmıştır. Bu sayede, her ülkede farklı uygulamaların olması durumunun ortadan kaldırılması ve AB üye devletlerinde kişisel verilerin korunması alanında birlik sağlanması amaçlanmıştır. Bu bakımdan değerlendirildiğinde GDPR'ın doğrudan uygulanabilir olmasının, kişisel verilerin korunması alanında daha tutarlı bir yaklaşım sağladığı görülmektedir.

AB veri koruma hukuku, aynı zamanda, üçüncü ülkelerin AB modeline dayalı veri koruma yasaları benimsemesi yoluyla küresel bir etki yaratmaktadır. Dünyanın dört bir yanındaki birçok ülke, 95/46/EC sayılı Direktif modeline¹⁸ dayalı veri koruma yasaları çıkarmış olup, bu durum ilgili direktifi veri koruma alanında "şu ana kadarki en etkili uluslararası politika aracı" olarak nitelendirmiştir¹⁹. 95/46/EC sayılı Direktif'in etkisi, Orta ve Doğu Avrupa ülkelerinde veri koruma yasalarının benimsenmesi, Kanada'da 2000 yılında federal gizlilik yasalarının geçmesi ve Asya ülkelerinde gizlilik yasalarının yaygınlaşması gibi gelişmelere de yansımaktadır. AB veri koruma hukukunun etkisi, bazı Afrika ülkelerinde veri koruma yasalarının kabul edilmesinde ve özel sektörde gizlilik standartlarının uygulanmasında da görülmektedir²⁰.

1.2. ÜLKEMİZDE KİŞİSEL VERİLERİN KORUNMASI ALANINDAKİ GÜNCEL GELİŞMELER

Ülkemizde kişisel veri kavramına ilk olarak 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu ("TCK") ve 5271 sayılı Ceza Muhakemesi

¹⁷ **Elif Küzeci**, "Kişisel Verilerin Korunması", T.C. Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku (Genel Kamu Hukuku) Anabilim Dalı, Doktora Tezi, Ankara, 2010, s. 179, ilgili teze ulaşmak için: https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=RYan9_S-Z7Eir3xdWGXBiGDRjcmOMffAR9wKmmwadGB7sOCDHavHBVRiy4uyCtR5 (e.t. 05.04.2024).

¹⁸ **Graham Greenleaf**, "The influence of European data privacy standards outside Europe: implications for globalization of Convention 108", International Data Privacy Law, Sayı: 2, 2012, s. 68.

¹⁹ **Colin J. Bennett, Charles D. Raab**, "The Governance of Privacy: Policy Instruments in Global Perspective", 2006, s. 93.

²⁰ **Christopher Kuner**, "The Internet and the Global Reach of EU Law", Oxford University Press, 2019, s. 18.

Kanunu'nda²¹ yer verilmiştir. TCK'nın 135. maddesinde “hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası” verilmesi, 136. maddesinde “kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası” ile cezalandırılması, 138. maddesinde “kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası” verilmesi düzenlenerek²² kişisel veri kavramına yer verilmiştir. Yargıtay kararları incelendiğinde suç kapsamındaki fiiller değerlendirilirken kişisel veri tanımının yapılarak, verileri hukuka aykırı olarak verme veya ele geçirme suçunun tespitinin yapıldığı görülmektedir. Örneğin, bir kişiye ait fotoğrafın başka bir kişinin sosyal medya hesabından izinsiz paylaşılması²³, ilgili kişinin rızası olmaksızın telefon numarasının üçüncü kişilerle paylaşılması²⁴ bu suç kapsamına girmektedir. Ancak belirtmek gerekir ki, kişisel verilere ilişkin ayrı bir yasal düzenleme yapılmadan önce Yargıtay kararlarında; TCK'da kişisel veri tanımının yapılmamış olması nedeniyle, suçta ve cezada kanunilik ve belirlilik ilkesine bağlı kalınması gerekliliği gözetilerek veri ile ilgili suç düzenlemelerinin Anayasaya aykırı olacağına ilişkin karşı oy gerekçeleri²⁵ de yer almaktaydı.

Teknolojik gelişmeler ile kişisel verilerin işlenme hızı ve boyutu arttıkça temel hak ve hürriyetlere müdahale edilmesinin kolaylaşması, bu konuda yasal düzenlemeler yapmayı gerekli kılmıştır. Anayasanın kişinin temel hak ve ödevlerinin düzenlendiği ikinci kısmında yer alan 20. maddesinde özel hayatın gizliliği güvence altına alınmaktadır. 5982 sayılı “Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun” ile 2010 yılında yapılan değişiklik sonrası Anayasanın 20. maddesine eklenen fıkra ile

²¹ RG T. 17.12.2004, S. 25673.

²² **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, Ankara, Nisan, 2018, s.12. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler> (e.t. 30.03.2024)

²³ Yargıtay Kararı - 12. CD., E. 2016/9759 K. 2017/10938 T. 26.12.2017.

²⁴ Yargıtay Kararı - 12. CD., E. 2014/607 K. 2014/16665 T. 7.7.2014.

²⁵ Yargıtay Kararı - 12. CD., E. 2014/607 K. 2014/16665 T. 7.7.2014.

kişisel veriler, “özel hayatın gizliliği ve korunması hakkı” ile Anayasal güvence altına alınmıştır²⁶. İlgili fıkra ile; “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” hükmü düzenlenmiştir.

Anayasada kişisel verilerin korunması kapsamında detaylı düzenlemelerin kanunla yapılacağı hükmolunmaktadır. Bu kapsamda, ülkemizde kişisel verilerin korunması için kanun çalışmaları esasen Anayasa değişikliğinin de öncesinde başlamış olmakla beraber bu alandaki ilk önemli adım Kişisel Verilerin Korunması Kanunu Tasarısı’nın 26 Aralık 2014 tarihinde Türkiye Büyük Millet Meclisi Başkanlığına sunulması ile atılmıştır. Takiben tasarı, 24 Mart 2016 tarihinde kabul edilmesi sonrası kanunlaşmış ve “6698 sayılı Kişisel Verilerin Korunması Kanunu” (“KVKK”) Resmi Gazete’de²⁷ yayımlanarak hukuk sistemimizde yerini almıştır²⁸. KVKK’nın hazırlanma aşamasında, 25 Mayıs 2016 tarihinde kabul edilen GDPR hükümleri esas alınmaksızın, yürürlükten kalkan 95/46 Sayılı Direktif hükümlerinin esas alınması uygulamada, özellikle özel nitelikli kişisel verilerin işlenmesi ve yurt dışına veri aktarımı hususlarında sıkıntılar doğurmaktadır. KVKK hazırlanırken ve kabul edildiği sırada GDPR henüz yürürlüğe girmemiş olduğundan ve GDPR’ın esas alınabilecek kesinleşmiş bir metin olmaması nedeniyle kanun koyucunun 95/46 Sayılı Direktif’i esas aldığı sonucuna varılmaktadır²⁹. Bu bakımdan geçmiş yıllarda doğan GDPR ile uyumlaşma gerekliliği kapsamında uzun

²⁶ **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, s.9.

²⁷ RG T. 07.04.2016, S. 29677.

²⁸ **Serdar Çelikel**, “Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri”, T.C. Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Doktora Lisans Tezi, Ankara, 2021, (“Çelikel”) s. 16, ilgili teze ulaşmak için: https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=RjZwH00oMG4iNa5Sgylgg8n_7mNZ8NqHZRTxHGB-vGqr6bdxh8Yrdt8mLfnSMkhF (E.t. 30.03.2024).

²⁹ Çelikel, s. 16,17.

bir hazırlık ve görüş sürecini takiben KVKK'ya yönelik hükümler de içeren “Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun”³⁰ 33. ilâ 36. maddeleri ile KVKK'nın “Özel nitelikli kişisel verilerin işlenme şartları” başlıklı 6. maddesi, “Kişisel verilerin yurt dışına aktarılması” başlıklı 9. maddesi ve “Kabahatler” başlıklı 18. maddesinde değişiklik yapılmış ve KVKK'ya yeni bir geçici madde eklenmiştir³¹.

KVKK'nın yürürlüğe girmesini takiben kişisel verilere ilişkin hükümler içeren yönetmelik ve tebliğler de yayımlanmıştır. İlgili yönetmelik ve tebliğler; Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik³², Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik³³, Kişisel Verileri Koruma Uzmanlığı Yönetmeliği³⁴, Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği³⁵, Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Unvan Değişikliği Yönetmeliği³⁶, Veri Sorumluları Sicili Hakkında Yönetmelik³⁷, Kişisel Verileri Koruma Kurumu Disiplin Amirleri Yönetmeliği³⁸ yürürlüğe girmiş ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ³⁹, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ⁴⁰ ve Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ⁴¹ hususlarına düzenlemek amacıyla yayımlanmıştır.

³⁰ RG T. 12.03.2024, S. 32487.

³¹ 6698 Sayılı Kişisel Verilerin Korunması Kanununda Yapılan Değişiklikler Hakkında Kamuoyu Duyurusu, ilgili duyuruya ulaşmak için: <https://www.kvkk.gov.tr/Icerik/7834/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununda-Yapilan-Degisiklikler-Hakkinda-Kamuoyu-Duyurusu> (e.t. 05.04.2024).

³² RG T. 28.10.2017, S. 30224.

³³ RG T. 16.11.2017, S. 30242.

³⁴ RG T. 09.02.2017, S. 30327.

³⁵ RG T. 26.04.2018, S. 30403.

³⁶ RG T. 05.05.2018, S. 30412.

³⁷ RG T. 30.12.2017, S. 30286.

³⁸ RG T. 15.03.2022, S. 31779.

³⁹ RG T. 10.03.2018, S. 30356.

⁴⁰ RG T. 10.03.2018, S. 30356.

⁴¹ RG T. 06.12.2021, S. 31681.

KVKK'nın 19. vd. maddeleri uyarınca Kişisel Verileri Koruma Kurumu ("Kurum") kurulmuş olup Kurum, KVKK kapsamında kişisel verilerin korunmasını sağlamakla görevli kamu kurumudur⁴². Kurum, bağımsız bir idari otorite olarak faaliyet göstermektedir. Kurum, kişisel verilerin korunması alanında uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak⁴³ yolu ile kişisel verilerin hukuka aykırı şekilde işlenmesini önlemekte ve ilgili kişilerin haklarını korumaktadır. Bu bakımdan Kurum, veri sorumlularının kanuna uymasını sağlayarak güvenli bir veri işleme ortamı oluşturmaktadır. KVKK'nın 21. ve 23. maddelerinde Kişisel Verileri Koruma Kurulu ("Kurul") ve çalışma esasları düzenlenmektedir. Ayrıca KVKK'nın 22. maddesi başta olmak üzere çeşitli maddelerde Kurul'un görevleri düzenlenmektedir.

Kurul'un başlıca görevleri şunlardır⁴⁴:

- Özel nitelikli kişisel verilerin işlenmesi için gerekli ve yeterli olacak önlemleri almak (m. 6/4).
- Verilerin kanuni olmayan yollarla elde edilmesi durumunda, veri sorumlusu tarafından yapılan bildirimleri gerekmesi halinde kendi internet sitesinde ya da uygun göreceği diğer yöntemlerle duyurmak (m.12/5).
- Veri sorumlularına yapılan ilgili kişi başvurularının reddedilmesi, verilen cevabın yetersiz olması veya süresinde cevaplanmaması halinde kendisine iletilen şikayetleri incelemek (m.14).

⁴² **Miray Özer Deniz**, Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk, T.C. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Doktora Lisans Tezi, Adana, 2022, ("Özer Deniz") s. 16, ilgili teze ulaşmak için: https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=RsTB16RWK25OBMIKtIgYYUrajK5kg0Whjop-mbB3gUBeg-C6SdhUv_1KiSEKK5D8 (e.t. 05.04.2024).

⁴³ KVKK'nın 20/1-a maddesi.

⁴⁴ **Kişisel Verileri Koruma Kurumu**, Kişisel Verileri Koruma Kurulunun Yapısı ve Görevleri, Ankara, Mart, 2018, s.13,15. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/c6206722-f4dc-484d-9bff-63f99b840158.pdf> (e.t. 05.04.2024)

- Şikayet halinde veya resen harekete geçerek tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vermek (m. 15/5).
- Benzer ihlallerin yaygınlaşması halinde ilke kararları almak (m. 15/6).
- Telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar vermek (m. 15/7).
- Kişisel verilerin, bireylerin temel hak ve özgürlüklerine uygun şekilde işlenmesini temin etmek (m.22/1-a).
- Kurum'un işleyişi, veri güvenliği ile ilgili yükümlülükleri belirlemek ve veri sorumlusu ve varsa temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlemleri yürütmek (m. 22/1-e,f,g).
- Kişisel verilere ilişkin hüküm içeren ve diğer kurum ve kuruluşlarca hazırlanan mevzuat taslakları için görüş bildirmek (m.22/1-h).

Bağlanabilir araçlarda kişisel verilerin veri sorumluları tarafından kişisel veri koruma mevzuat yükümlülüklerine uygun şekilde işlenmesini temin etmek, sektörel olarak ilgili alanda düzenlemeler yaparak veri güvenliğini artırmak ve diğer kurum ve kuruluşların mevzuat taslaklarını inceleyerek oradaki hükümlerin veri koruma mevzuatına uygun işlenmesini sağlamak için Kurum'un etkin bir rol oynaması bakımından KVKK'daki görev tanımının kapsayıcı şekilde düzenlendiği görülmektedir.

1.3. AB VERİ YASASI

Teknolojinin gelişmesi ve farklı bilişim tekniklerine bağlı olarak veri işleme yöntemleri değişmiş ve verilere erişim her zamankinden daha kolay hale gelmiştir. Bu teknolojilerin bir sonucu olarak, büyük veri ve yapay zeka kavramları, hukukçular, hukuk bilimcileri ve yasa koyucular tarafından geniş ölçüde tartışılmaya başlanmıştır. Verinin kullanım alanı ve boyutu arttıkça hukuk

kurallarının ihtiyaçlara göre düzenlenmeleri amacıyla teknolojik gelişmelerin takibi daha önemli hale gelmiştir. Yeni elektronik cihazların üretilmesi ve robotların daha yaygın bir şekilde kullanılması, hukuki açıdan bazı soruları gündeme getirmektedir⁴⁵.

AB Veri Yasası⁴⁶, 11 Ocak 2024 tarihinde yürürlüğe girmiştir. AB Veri Yasası, Şubat 2020'de Avrupa Komisyonu ("Komisyon") tarafından açıklanan veri stratejisinin bir parçası olup, bağlanabilir ürünlerin üreticilerini belirli durumlarda kullanım ile ilgili verileri erişilebilir hale getirmeye zorunlu kılmaktadır. Ayrıca, bulut hizmetleri gibi veri işleme hizmeti sağlayıcılarının kullanıcıların farklı bir hizmet sağlayıcıya geçişini kolaylaştırmasını, örneğin asgari geçiş hizmetleri sağlamasını zorunlu kılmaktadır. AB Veri Yasası kapsamındaki yükümlülüklerin çoğu 12 Eylül 2025 tarihinden itibaren uygulanacaktır. Bağlanabilir ürünlerin tasarımı ve üretimine ilişkin yükümlülükler ise 12 Eylül 2026 tarihinden sonra piyasaya sürülen ürünler ve bağlanabilir hizmetler için geçerli olacaktır.

Genel amacına ulaşmak için AB Veri Yasası şu kuralları getirmektedir: (i) Veri kullanımında ve paylaşımında tüketiciler ve veri üreten şirketler için yasal güvenliği artırarak veri ekonomisini kolaylaştırmak, (ii) veri paylaşımını zayıflatabilecek sözleşmesel dengesizliklerden kaynaklanan suistimalleri önlemek, (iii) kamu sektörünün, bir kamu acil durumu sırasında veya yasal bir yetkiyi uygulamak amacıyla, bu verilerin başka türlü mevcut olmaması halinde, özel sektörün elindeki verilere erişimini ve bu verileri kullanımını sağlamak, (iv) tüketicilerin farklı veri işleme hizmet sağlayıcıları arasında kolayca geçiş yapabilmelerini sağlamak.

AB dijital egemenliği kavramı çerçevesinde benimsenen kararlı yaklaşımın bir yansıması olarak, AB Veri Yasası'nın birliğin normatif gücünü (Brüksel etkisi olarak da bilinen) güçlü bir şekilde yansıttığı değerlendirilmektedir. AB Veri

⁴⁵ **Lilian Edwards**, 'Data Protection and E-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling', Law, Policy and the Internet, Hart Publishing, 2019, s. 120.

⁴⁶ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828

Yasası, geniş bir dış etki alanı yaratma potansiyeline sahip bir uygulama kapsamı belirlemektedir⁴⁷. Nitekim, AB Veri Yasası'nın hükümleri, AB pazarında satılan ürünlerin üreticileri ve AB'de sunulan veri işleme hizmet sağlayıcıları için, bu kuruluşların bir Üye Devlet'te yer alıp almadıklarına bakılmaksızın uygulanabilirlik taşımaktadır. Bu durum, özellikle AB Veri Yasası'nın GDPR'ın 20. maddesini tamamlayarak veri taşınabilirliği haklarını IoT tarafından üretilen verileri de kapsayacak şekilde genişletmesiyle birlikte daha da kritik bir önem kazanmaktadır.

Kişisel veriler de dahil üretilen veriler AB Veri Yasası kapsamında kullanılırken aynı zamanda GDPR gerekliliklerinin de AB Veri Yasası'na ek olarak uygulanması gerekmektedir. Bu bakımdan ilgili kişilerin, bağlanabilir ürünlerin veya ilgili hizmetlerin kullanımı sonucunda üretilen verilerin hangi ticari sırlar ve kişisel verileri içerdiği ve dolayısıyla veri erişim ve paylaşım yükümlülüklerine tabi olup olmadığı hakkında aydınlatılması gerekmektedir⁴⁸.

AB Veri Yasası kapsamında bağlanabilir ürünler, kullanımları veya çevreleri hakkında veri elde eden, üreten veya toplayan ve bu verileri elektronik iletişim, fiziksel bağlantı veya IoT cihazlar gibi cihaz üzerinde erişim yoluyla iletebilen ürünleri kapsamaktadır. AB Veri Yasası kapsamındaki yükümlülükler, çoğunlukla AB pazarında yer alan bağlanabilir ürünlerin üreticilerine ve ilgili hizmet sağlayıcılarına, yerleşim yerlerinden bağımsız olarak uygulanacaktır. AB Veri Yasası kapsamına giren şirketler kullanıcı tarafından üretilen verileri kullanıcıya ve kullanıcının seçtiği üçüncü taraflara erişilebilir kılmakla yükümlü olmaktadır.

⁴⁷ **Kuner**, s. 2.

⁴⁸ **Hogan Lovells**, Deep Dive on the new EU Data Act, Lexology, Aralık, 2023. İlgili makaleye internet üzerinden şu link ile ulaşılabilir: <https://www.lexology.com/library/detail.aspx?g=454f1afc-8561-4949-a20c-b7a34548d77b> (e.t. 17.08.2024).

AB Veri Yasası'nda düzenlenen bağlanabilir araç üreticileri gibi üreticilerin ve bulut hizmetleri de dahil veri işleme hizmet sağlayıcılarının bazı yükümlülükleri aşağıda özetlenmektedir⁴⁹:

- Ürün veya hizmet, kullanıcı tarafından üretilen verilerin kullanıcı tarafından kolayca erişilebilir olacağı şekilde tasarlanmalıdır. Kullanıcının talebi üzerine, ürün veya ilgili hizmetten doğrudan erişilemeyen verilerin kullanıcıya veya bir üçüncü tarafa sağlanması gerekmektedir.
- Ürün veya hizmetin kullanımından kaynaklanacak veriler ve bu verilere nasıl erişileceği, geri alınacağı veya silineceği hakkında üyelik / kullanıcı sözleşmesinde kullanıcıya bilgi sağlanmalıdır.
- Üreticiler veya ilgili hizmet sağlayıcıları, belirli verilerin ticari sır olarak tanımladığı durumlarda, olay özelinde bu verilerin paylaşımını reddedebilirler. Verilerin paylaşımının reddi, yalnızca kullanıcının aldığı teknik ve idari tedbirlere rağmen ifşa edilmesinin ciddi ekonomik zarara yol açması durumunda ve istisnai hallerde geçerli olmaktadır. Ret, eldeki verilerin niteliği ve gizlilik seviyesi dahil olmak üzere, nesnel unsurlara dayandırılmalı, yazılı olarak kullanıcıya sunulmalı ve aynı zamanda ulusal yetkili makama bildirilmelidir.
- Üreticiler veya ilgili hizmet sağlayıcıları, veri paylaşımını otomatikleştirmek adına verilere yetkisiz erişimi önlemek amacıyla akıllı sözleşmeler ve şifreleme gibi uygun teknikte koruma önlemlerini uygulamalıdır.
- Verinin paylaşılacağı üçüncü taraflar, verileri yalnızca kullanıcı ile anlaşılan amaçlar ve koşullar altında kullanabilir. Kullanıcılar ve üçüncü taraflar, verilerin üretildiği ürünle rekabet eden ürünler geliştirmek ve üreticinin ekonomik durumu, varlıkları ve üretim yöntemleri hakkında çıkarımlar yapmak için verileri kullanmaktan menedilmiştir.

⁴⁹ <https://www.mayerbrown.com/en/insights/publications/2024/03/eu-data-act-new-rules-on-data-sharing-and-portability-of-cloud-services-now-in-force> (e.t. 10.08.2024).

AB Veri Yasası, yalnızca otomotiv endüstrisine özgü olmamakla birlikte, bağlanabilir araçların yaygınlaşması ve bu araçların veri üretim potansiyeli göz önüne alındığında, otomotiv sektörü için özel bir önem taşımaktadır. Bağlanabilir araçlar, günlük kullanım sırasında sürüş alışkanlıklarından navigasyon tercihlerine, araç içi sistemlerin güncellenmesinden araç parçalarının çalışma durumuna kadar geniş bir yelpazede veri üretmektedir. Bu verilerin, kablosuz güncellemeler oluşturmak, talep üzerine özellikler sunmak veya potansiyel arızaları ve onarım ihtiyaçlarını izlemek için kullanılması, veri yönetiminin araç üreticileri için değerini göstermektedir. Ancak, veri iletimi ve depolama süreçleri sürekli olarak gelişip karmaşıklaştığından, özellikle araçlar üzerinde üretilen verinin sahipliği ve kullanım hakkı da yeni yasal gelişme ihtiyacını getirmektedir.

AB Veri Yasası, özellikle bağlanabilir araçlardan elde edilen verilerin araç sahibi veya sürücüsü gibi kullanıcıların erişimine sunulması gerekliliğini vurgulamaktadır. Yasanın üçüncü, dördüncü ve beşinci maddeleri, bu konuda kilit öneme sahip düzenlemeleri içermektedir:

- AB Veri Yasası'nın 3. maddesinde bağlanabilir ürünlerden erişilen veya ilgili hizmetlerin sunumu sırasında üretilen verilerin kullanıcıya erişilebilir kılınması yükümlülüğü, araç üreticilerinin araç sahibi veya sürücülerinin üretici tarafından toplanan verilere erişimini sağlamak için gerekli düzenlemeleri yapmasını zorunlu kılmaktadır. Erişim yöntemi, aracın bir USB bağlantısı ile bilgisayara bağlanarak aynı veri akışının kullanıcı tarafından indirilebilmesi gibi basit ve kolay erişilebilir bir işlem olmalıdır.
- AB Veri Yasası'nın 4. maddesinde üreticiler ve ilgili kişilerin, bağlanabilir ürünlerden erişilen veya üretilen verilere erişim, kullanım ve paylaşma konusundaki hakları ve yükümlülükleri düzenlenmektedir. Özellikle eski araçlar için, araç sahibi / sürücülerin doğrudan veri erişimi sağlayamadığı durumlarda, üreticilerin uzaktan erişim sağlayabilmesi için yeni yöntemler geliştirmesi gerekmektedir.

- AB Veri Yasası'nın 5. maddesi kapsamında kullanıcıların, otomobil üreticisi tarafından toplanan verilerin üçüncü taraflarla paylaşımını sağlama hakkı, özellikle satış sonrası hizmetler açısından büyük önem taşımaktadır. Yasa ile bu verilere erişimin denetçisinin üretici yerine kullanıcı olması sağlanmaktadır. Örneğin, araç tamir işlemleri için kullanıcı onayı halinde tamircilerin verilere erişimi mümkün olmaktadır.

AB Veri Yasası, bağlanabilir araçlar ve genel olarak otomotiv endüstrisi için önemli bir yasal düzenleme olarak öne çıkmaktadır. Bu yasa, verinin sahipliğinin ve kontrolünün kullanıcıda olduğunu netleştirerek, kullanıcı merkezli yaklaşımının yanında veri yönetimi süreçlerinde şeffaflık ve adaleti sağlamayı amaçlamaktadır.

Komisyon, Şubat 2020'de dijital teknolojilerin hızla artan kullanımına yanıt olarak, AB'nin dijital dönüşüme hazır olması gerektiğini vurgulayan bir dizi politika belgesi yayımlamıştır. Bu belgeler arasında, AB Veri Stratejisi⁵⁰ de bulunmakta olup, AB Veri Stratejisi AB'de veri ekonomisini geliştirmeyi hedeflemektedir. Strateji, özellikle kaliteli veriye erişimin artırılması ve bu verilerin yeniden kullanımına odaklanmaktadır. Verinin ekonomik kalkınma için kritik bir kaynak olduğu kabul edilerek, AB genelinde tek bir veri pazarı oluşturma amacı vurgulanmaktadır. Bu doğrultuda, veri erişimi ve yönetimi için yeni mevzuat geliştirilmesi, veri yoğunlaşmasına karşı düzenleyici önlemler alınması ve standartlar, araçlar, altyapı ile becerilere yatırım yapılması öne çıkan unsurlardır.

AB Veri Stratejisi, sadece verilerin toplanması ve yönetilmesiyle sınırlı kalmayan, aynı zamanda verinin yeniden kullanımını ve paylaşımını da merkeze alan kapsamlı bir yaklaşımı temsil etmektedir. Bu bakımdan AB Veri Stratejisi'nin önemini anlamak için, verinin modern toplumdaki merkezi rolünü kavramak gerekmektedir. Veri, inovasyonun kaynağıdır; sağlık hizmetlerinden ulaşım sistemlerine, kişiselleştirilmiş hizmetlerden kamu sektöründeki verimlilik artışlarına kadar pek çok alanda devrim niteliğinde yeniliklere olanak tanımaktadır.

⁵⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020DC0066> (e.t. 11.09.2024).

AB Veri Stratejisi'nin en önemli hedeflerinden biri, gerçek bir veri tek pazarı oluşturmaktır. Bu pazar, hem kişisel hem de kişisel olmayan verilerin güvenli bir şekilde paylaşıldığı, işletmelerin ve kamu kuruluşlarının büyük miktarda yüksek kaliteli veriye kolay erişim sağlayabildiği bir ekosistem yaratmayı amaçlamaktadır. Böylelikle, yeni ürünler ve hizmetlerin geliştirilmesi teşvik edilerek, veriye dayalı inovasyonun önü açılacak ve AB'nin dijital egemenliği güçlendirilecektir. Strateji, aynı zamanda yapay zekâ gibi yeni teknolojilerin potansiyelini ortaya çıkararak, AB'yi bu alanda küresel bir lider haline getirmeyi hedeflemektedir⁵¹.

AB Veri Stratejisi, kullanıcı odaklı bir yaklaşım benimsenmesi gerektiğini ve bireylerin gizlilik haklarının korunmasının zorunlu olduğunu kabul etmektedir. Bu nedenle, GDPR diğer yasalar arasında yatay bir biçimde uygulanmakta ve veri paylaşımı, birlikte çalışabilirlik ve şeffaflık gibi konularda getirilen yükümlülükler, GDPR'ın gerekliliklerine zarar vermeden yerine getirilmektedir. Bu bakımdan AB Veri Yasası, kişisel verilerin toplanması veya kullanılması için bağımsız bir yasal dayanak oluşturmamakta, bu konuda GDPR uygulanmaya devam etmektedir. Her gün insanlar tarafından üretilen büyük miktardaki veri, haklar ve çıkarlar göz önünde bulundurularak toplanmalı ve kullanılmalıdır. GDPR ile AB, bireylerin verileri üzerinde tam kontrol sahibi olmasını sağlayarak, insan odaklı bir veri ekonomisi oluşturmuştur. AB Veri Stratejisi, bu yaklaşımı daha da güçlendirmekte ve ilgili kişilerin verileri üzerinde daha fazla söz sahibi olmasını hedeflemektedir.

AB Veri Stratejisi, bireylerin ürettikleri verilere kimlerin erişebileceği ve bu verilerin nasıl kullanılacağı konusunda daha fazla söz sahibi olmalarını sağlamakta olup buradaki kontrol kişisel veri alanları aracılığıyla yapılmaktadır. Bu kontrol, örneğin, gerçek zamanlı veri erişimi için arayüzlerde daha sıkı gereksinimler getirilmesi ya da kişisel veri alanlarının tarafsızlığının garanti edilmesi gibi yöntemlerle sağlanmaktadır. Bu yaklaşım kapsamında, AB Veri Stratejisi ile verinin ekonomik ve toplumsal potansiyelini ortaya çıkarmak amacıyla Şubat

⁵¹ European Commission, “Shaping Europe's digital future – Questions and Answers”, Şubat, 2020. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_264 (e.t. 30.09.2024).

2020'de, sađlık, tarım, enerji, mobilite, finans, kamu yönetimi gibi stratejik alanlarda AB veri alanları oluşturulması hedeflenmiştir. Bu veri alanları, veri paylaşımının kalitesini, kullanılabilirliğini ve birlikte çalışabilirliğini artırmayı amaçlamaktadır. AB veri alanlarının yönetimine dair genel düzenlemeler ise AB Veri Yasası ve sektöre özgü mevzuatlarda tanımlanmaktadır⁵².

AB veri alanlarının gelişimi, ilgili sektörlerdeki paydaşlar tarafından yönlendirilmektedir. Her sektördeki kullanıcılar, veri alanlarının şekillenmesine katkıda bulunarak, alanların benzersiz özellikler kazanmasına olanak tanımaktadır. Ancak, tüm veri alanlarının temelinde ortak veri altyapıları ve yönetim çerçeveleri yer almakta ve bu altyapılar verilerin toplanmasını, verilere erişimi ve verilerin paylaşımını kolaylaştırmaktadır. AB veri alanlarının temel özellikleri arasında aşağıda sıralanan hususlar yer almaktadır⁵³:

- Tüm kuruluşlar ve bireylerin katılımına açıktırlar.
- Verilerin toplanmasını, verilere erişimi ve verilerin paylaşımı gibi verilerin işlenmesi ve kullanılması bakımından güvenli ve veri gizliliğini temin eden bir altyapıya sahiptirler.
- Verilere erişim ve kullanım için açık ve pratik bir yapı sunarlar. AB veri alanları, iyi tanımlanmış ve güvenilir veri yönetim mekanizmaları sayesinde adil, şeffaf, ölçülü ve ayrımcılık yaratmayan erişim kurallarına sahiptir.
- AB kuralları ve değerleriyle, özellikle kişisel veri ve tüketici koruma ile rekabet mevzuatları ile uyumludurlar.

AB veri alanları, verilerin güvenli bir ortamda erişilebilirliğini ve yeniden kullanılabilirliğini artırarak AB işletmeleri ve vatandaşları için önemli faydalar sağlamayı hedeflemektedir. Bu alanlar, AB'nin dijital ekonomisinin gelişimine

⁵² <https://www.dataguidance.com/opinion/eu-overview-european-digital-strategy> (e.t. 11.09.2024).

⁵³ **European Commission**, "Shaping Europe's digital future – Questions and Answers", Şubat, 2020. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_264 (e.t. 30.09.2024).

katkı sağlayacak ve yeni veri odaklı ürün ve hizmetlerin önünü açacaktır. AB Veri Stratejisi, başlangıçta dokuz stratejik ekonomik sektörde ve kamu yararına alanlarda ortak veri alanlarının geliştirilmesini öngörmüştür. Bu sektörler, tarım, enerji, sağlık, finans, sanayi, kültürel miras, kamu yönetimleri, mobilite, araştırma ve yenilik alanlarını kapsamaktadır. 2024 yılı itibarıyla, beş stratejik sektör daha belirlenerek toplam sayı 14 AB veri alanına yükselmiştir⁵⁴.

Belirlenen AB veri alanlarından biri de mobilite veri alanı olup bağlanabilir araçlarda veri işlenmesi bakımından takibi ve uygulanması gerekmektedir. Bu alan, mevcut ve gelecekteki ulaşım ve mobilite veri kaynaklarına erişimi, veri havuzlarını bir araya getirmeyi ve veri paylaşımını kolaylaştırarak verimli ve birbirine bağlı çok modlu bir ulaşım sisteminin oluşumuna yardımcı olmayı hedeflemektedir⁵⁵. Bu bakımdan bu alan, kullanıcılarının ihtiyaçlarına uyum sağlayan sürdürülebilir, akıllı ve kapsayıcı bir mobilite ve ulaşım sektörü yaratılmasına katkıda bulunmaktadır.

Mobilite sektörü bakımından AB Veri Yasası, verilerin adil bir şekilde paylaşımının ve kullanımının teşvik edilmesi, tamir ve sigorta hizmetleri gibi araç verilerine dayalı hizmetlerin verilmesini kolaylaştırmıştır. AB, ulaşım sektöründe veri toplama, yönetme ve kullanma konularında ortak standartlar ve iyi uygulamaları geliştirmek amacıyla kamu ve özel sektör ile aktif iş birliğini teşvik etmektedir. Bu kapsamda çeşitli proje ve oluşumlar gündeme gelmiştir⁵⁶. Akıllı Ulaşım Sistemleri⁵⁷ (Intelligent Transport Systems) çerçevesi, ulusal erişim noktaları (NAPs) aracılığıyla temel ulaşım verilerine erişimi düzenlemektedir. NAPCORE projesi⁵⁸, bu erişim noktalarını AB genelinde uyumlu hale getirmeyi ve güçlendirmeyi amaçlamaktadır. Dijital Ulaşım ve Lojistik Forumu (Digital

⁵⁴ <https://www.arthurcox.com/knowledge/what-are-common-european-data-spaces/> (e.t. 11.09.2024).

⁵⁵ **European Commission**, “Commission Staff Working Document on Common European Data Spaces”, Ocak, 2024, s. 36. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://digital-strategy.ec.europa.eu/en/library/second-staff-working-document-data-spaces> (e.t. 30.09.2024).

⁵⁶ **European Commission**, “Unlocking the potential of mobility data”, Eylül, 2024. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://digital-strategy.ec.europa.eu/en/policies/mobility-data> (e.t. 30.09.2024).

⁵⁷ https://transport.ec.europa.eu/transport-themes/smart-mobility_en (e.t. 11.09.2024).

⁵⁸ <https://napcore.eu/> (e.t. 11.09.2024).

Transport and Logistics Forum), yük ve lojistik için veri paylaşımına yönelik birlikte çalışabilir ortamlar yaratmaktadır. Dijital Ulaşım ve Lojistik Forumu'nun ana hedefi, dijitalleşme yoluyla ulaşım sistemlerinin verimliliğini, sürdürülebilirliğini ve bağlantılılığını artırmak, yenilikçiliği teşvik etmektir. Ayrıca, Avrupa Bağlantı Tesisleri Dijital⁵⁹ (Connecting Europe Facility (CEF) Digital) programı, enerji ve ulaşım altyapısının yenilenmesini desteklemek ve yeni akıllı hizmetlerin geliştirilmesine yardımcı olmak için operasyonel dijital platformların⁶⁰ oluşturulmasına katkı sağlamaktadır. Avrupa Bağlantı Tesisleri, AB'nin dijital altyapının geliştirilmesini destekleyen bir programı olup AB genelinde yüksek kapasiteli dijital ağların, 5G bağlantısının ve güvenli dijital hizmet altyapılarının kurulmasını teşvik etmeyi amaçlamaktadır. Aynı zamanda, siber güvenliği iyileştirme ve dijital dönüşümü hızlandırma projelerini de finanse ederek, dijital ekonominin gelişmesine destek vermektedir.

Mobilite ve ulaşım sektöründe büyük miktarda veri üretilmesine rağmen, bu veriler büyük ölçüde parçalanmış durumdadır. Avrupa Mobilite Veri Alanı⁶¹ (European Mobility Data Space), AB'de ulaşım verilerinin güvenli ve verimli bir şekilde paylaşılmasını sağlamayı amaçlayan bir girişimdir. Bu program, ulaşım sektörü paydaşlarının birbirleriyle veri alışverişini kolaylaştırarak mobilite hizmetlerini iyileştirmeyi, inovasyonu teşvik etmeyi ve ulaşımında sürdürülebilirliği artırmayı hedeflemektedir. Avrupa Mobilite Veri Alanı, özellikle veri paylaşımı yoluyla dijitalleşmeyi hızlandırarak daha bütünleşmiş, verimli ve kullanıcı odaklı bir ulaşım ekosistemi oluşturmayı amaçlamaktadır.

Komisyon'un Avrupa Mobilite Veri Alanı'nın oluşturulmasına ilişkin duyurusu⁶², bu alanın oluşturulması için hedefleri, destekleyici önlemleri ve

⁵⁹ **European Commission**, "Connecting Europe Facility - CEF Digital", Mart, 2024. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://digital-strategy.ec.europa.eu/en/activities/cef-digital> (e.t. 11.09.2024).

⁶⁰ **European Commission**, "CEF Digital: Operational Digital Platforms", Ocak, 2022. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://digital-strategy.ec.europa.eu/en/news/cef-digital-operational-digital-platforms> (e.t. 11.09.2024).

⁶¹ <https://deployemds.eu/> (e.t. 11.09.2024).

⁶² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023DC0751> (e.t. 11.09.2024).

izlenecek yol haritasını açıklamaktadır. Dijital Avrupa Programı⁶³ (The Digital Europe Programme) kapsamında, Eylül 2023'te hazırlık çalışmaları tamamlanmış ve mevcut girişimler haritalanarak olası ortak yapı taşları belirlenmiştir. Dijital Avrupa Programı AB'nin dijital teknolojilerin geliştirilmesi ve yaygınlaştırılmasını destekleyen bir programıdır. Programın temel amacı, AB'nin dijital dönüşümünü hızlandırmayı, stratejik dijital kapasiteleri güçlendirmeyi ve bu teknolojilerin AB genelinde ekonomik ve toplumsal faydalar sağlamasını temin etmektir.

Sayılan AB girişimlerine ek olarak, üye devletler veya özel aktörler tarafından desteklenen girişim platformları ve pazar yerleri gibi çeşitli veri ekosistemleri, mobilite sektöründe veri paylaşımını kolaylaştırmayı amaçlamaktadır. Bu kapsamda Mobilite Veri Alanı⁶⁴, Alman hükümeti tarafından desteklenen ve mobilite veri sağlayıcılarının verilerini paylaşmasına olanak tanırken, aynı zamanda verilerin kontrolünü elinde tutmalarını ve mevcut mobilite veri platformlarını birbirine bağlamalarını sağlayan açık ve merkeziyetsiz bir ekosistemdir. Mobilite Veri Alanı ulaşım sektörü için güvenli ve şeffaf veri paylaşımını sağlayan bir platform olup farklı mobilite hizmet sağlayıcıları, endüstri temsilcileri ve teknoloji şirketleri arasında veri alışverişine imkan tanımaktadır. Amacı, mobilite ekosistemini desteklemek, ulaşım çözümlerini daha verimli hale getirmek ve yenilikçi projelere zemin hazırlamaktır.

Ana özellikleri şunlardır⁶⁵:

- Mobilite Veri Alanı, kullanıcıların ne tür verilerin paylaşıldığını ve bu verilerin ne amaçla kullanıldığını kontrol etmelerine olanak tanımaktadır. Veri sağlayıcıları, kimlerle hangi veriyi paylaştıklarını belirleyebilmektedir.

⁶³ **European Commission**, “The Digital Europe Programme”, Eylül, 2024. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://digital-strategy.ec.europa.eu/en/activities/digital-programme> (e.t. 30.09.2024).

⁶⁴ <https://mobility-dataspace.eu/> (e.t. 30.09.2024).

⁶⁵ <https://mobility-dataspace.eu/mobility-data-space#:~:text=The%20Mobility%20Data%20Space%20connects,data%20and%20for%20what%20purpose.> (e.t. 30.09.2024).

- Paylaşılan verilerin güvenliği ve gizliliği, gelişmiş güvenlik önlemleri ile korunur. Mobilite Veri Alanı, veri sağlayıcılarına hangi verilerin paylaşıldığını ve bu verilerin nasıl kullanıldığını takip etme imkanı sunmaktadır.
- Veri paylaşımı sayesinde, mobilite hizmetleri ve akıllı ulaşım çözümleri geliştirilmektedir. Bu sayede ulaşım ağlarının daha iyi yönetilmesi, karbon ayak izinin azaltılması ve ulaşım hizmetlerinin daha verimli hale gelmesi sağlanmaktadır.
- Mobilite Veri Alanı, veri paylaşımı yoluyla yeni iş modellerinin ve hizmetlerin geliştirilmesine katkı sağlamaktadır. Hem küçük hem de büyük şirketler, veri tabanlı çözümler üretebilmekte ve iş süreçlerini iyileştirebilmektedir.

Mobilite Veri Alanı aynı zamanda katılımcıların veri alışverişini özelleştirmesine ve kullanım haklarını belirlemesine izin vermekte olup böylece veri sağlayıcıları paylaştıkları bilgilere dair tam kontrol sahibi olmaktadır. Bu yapı, AB'nin dijital ve mobilite hedefleriyle uyumlu olarak, güvenli ve şeffaf bir veri ekosistemi oluşturmayı hedeflemektedir.

1.4. AB YAPAY ZEKA YASASI

Komisyon tarafından Nisan 2021'de önerilen ve Aralık 2023'te Avrupa Parlamentosu ve Avrupa Konseyi tarafından kabul edilen AB Yapay Zeka Yasası⁶⁶, yapay zekanın geliştirilmesi ve/veya kullanımını yönetecek bir yasadır. Yasa, risk temelli bir yaklaşım getirerek, yapay zeka uygulamalarına yarattığı risk seviyesine göre farklı kurallar uygulanmasını düzenlemektedir. Bu bakımdan 1 Ağustos 2024'te yürürlüğe giren AB Yapay Zeka Yasası, AB'de sorumlu yapay zeka

⁶⁶ European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts.

uygulamalarının geliştirilmesini ve uygulanmasını temin eden düzenlemelere sahiptir⁶⁷.

Yapay zeka birçok sektörü doğrudan etkileyerek bu alanlarda köklü değişimlere neden olma potansiyeline sahiptir⁶⁸. AB Yapay Zeka Yasası, yapay zeka sistemlerinin güvenli, şeffaf ve etik bir şekilde geliştirilmesi ve uygulanmasını sağlamaktadır. Yasa bu sistemleri dört farklı risk kategorisinde sınıflandırmaktadır; kabul edilemez risk, yüksek risk, sınırlı risk ve minimal risk. Özellikle, yüksek risk kategorisindeki yapay zeka sistemleri sıkı düzenlemelere tabidir ve bu sistemlerin geliştiricileri ve kullanıcıları, yasal uyumluluk süreçlerinde daha titiz bir değerlendirmeye tabi tutulmaktadır.

AB Yapay Zeka Yasası'nın, GDPR'ın veri koruma düzenlemelerinde olduğu gibi uluslararası bir kıstas olup olmayacağı belirsizdir. GDPR'ın teknoloji açısından tarafsız doğası göz önüne alındığında ilgili düzenleme, yapay zeka teknolojileri bağlamında kişisel verilerin işlenmesinde uygulanmaya devam etmektedir. Bununla birlikte AB Yapay Zeka Yasası, GDPR'daki bazı ilkelere de dayanmaktadır ve uygulamada bu iki mevzuat ve ilgili gereksinimler bir arada var olmaktadır. Bu nedenle yapay zeka sistemini geliştiren veya geliştirilmiş bir yapay zeka sistemini kendi adı veya ticari markası altında piyasaya süren veya hizmete sunan sağlayıcıların ve bu sistemleri kullananların her iki mevzuat arasındaki etkileşimi anlaması önemlidir.

Benzer şekilde yapay zeka uygulamalarında standartlaştırma, bu teknolojilerin güvenli, uyumlu ve etkili bir şekilde kullanılmasını sağlamak için kritik bir önem taşımaktadır. Standartlar, karmaşık dijital teknolojiler için temel "bilgi kuralları" olarak hizmet eder ve hem tarihsel hem de kurumsal bağlamda güçlü bir geçmişe

⁶⁷[https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en#:~:text=On%201%20August%202024%2C%20the,AI%20Act\)%20enters%20into%20force\(e.t. 11.08.2024\).](https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en#:~:text=On%201%20August%202024%2C%20the,AI%20Act)%20enters%20into%20force(e.t. 11.08.2024).)

⁶⁸ **Tayfun Acarer**, Endüstri'deki Gelişmelerin Denizcilik İşletmelerine Ait Gemilerin Yönetiminde Temin Ettiği Yeni Olanaklar ve İnsansız Gemiler, Mersin Üniversitesi Denizcilik ve Lojistik Araştırmaları Dergisi, Cilt:5, Sayı:2, 2023 ("Acarer").

sahiptir⁶⁹. AB'de, standartlaştırma giderek daha fazla düzenleyici bir araç olarak kullanılmakta ve özellikle yapay zeka ile ilgili yeni düzenlemelere uyum sağlama konusunda önemli bir rol oynamaktadır⁷⁰. Standartların bu rolü, teknolojilerin doğru, güvenli ve yasalara uygun şekilde kullanılmasını sağlarken, aynı zamanda sanayi politikası ve ulusal güvenlik gibi daha geniş kapsamlı endişeleri de ele almaktadır⁷¹.

Hem AB Yapay Zeka Yasası hem de GDPR, şeffaflık, hesap verebilirlik ve açıklanabilirlik gibi temel ilkelerin önemini vurgulamaktadır. Özellikle AB Yapay Zeka Yasası, belirli yapay zeka sistemleri için teknik dokümantasyon ve kayıt tutma gibi belgelerin sağlanması gerekliliklerini içermektedir. GDPR ise veri sorumlularının ve bazı durumlarda veri işleyenlerin kişisel veriler işlendiğinde hesap verebilirlik yükümlülüklerini desteklemek için çeşitli belgelendirmeleri hazırlamasını ve güncel tutmasını düzenlemektedir.

AB Yapay Zeka Yasası hem sağlayıcılar hem de kullanıcılar için şeffaflık yükümlülüklerini ortaya koymakta olup bu yükümlülükler arasında şunlar bulunmaktadır:

- AB Yapay Zeka Yasası, yapay zeka sistemlerinin bireylerle doğrudan etkileşime girmesi amaçlandığında, bu bireylerin bir yapay zeka sistemi ile etkileşimde bulunduklarının farkında olmalarını sağlayacak şekilde uygulama

⁶⁹ **David Paul, Shane Greenstein**, “The Economics Of Compatibility Standards: An Introduction To Recent Research”, *Economics of Innovation and New Technology*, 1990, Sayı: 1, s. 3–41. İlgili makaleye internet üzerinden şu link ile ulaşılabilir: http://neconomides.stern.nyu.edu/networks/David-Greenstein_The_Economics_of_Compatibility_Standards.pdf (e.t. 17.08.2024).

⁷⁰ **Nora von Ingersleben-Seip**, “Competition and cooperation in artificial intelligence standard setting: Explaining emergent patterns”, *Review of Policy Research*, Sayı: 40, s. 781–810. İlgili makaleye internet üzerinden şu link ile ulaşılabilir: <https://doi.org/10.1111/ropr.12538> (e.t. 17.08.2024).

⁷¹ **Marta Cantero Gamito, Christopher T Marsden**, “Artificial intelligence co-regulation? The role of standards in the EU AI Act”, *International Journal of Law and Information Technology*, 2024, Sayı: 32. İlgili makaleye internet üzerinden şu link ile ulaşılabilir: <https://doi.org/10.1093/ijlit/eaee011> (e.t. 17.08.2024).

sağlayıcılar tarafından bu sistemlerin tasarlanmasını ve geliştirilmesini zorunlu kılmaktadır.

- Yapay zeka sistemleri sentetik ses, görüntü, video veya metin içeriği oluşturuyorsa, bu içeriğin makine tarafından okunabilir bir formatta işaretlenmesi ve yapay olarak üretildiğinin veya manipüle edildiğinin tespit edilebilir olması gerekmektedir. Aynı gereklilik, deep fake içeriklerin kullanılması halinde ve kamuoyunu ilgilendiren konularda yayımlanan metinlerin yapay zeka sistemleri ile üretildiği veya manipüle edildiği durumlarda da geçerlidir. Bu durumda yapay zeka sisteminin uygulandığının açıkça belirtilmesi gerekmektedir.
- Duygu tanıma sistemi veya biyometrik kategorilendirme sistemi sağlayıcıların, bu sistemin işleyişi hakkında kullanıcıları bilgilendirme yükümlülüğü bulunmaktadır. Yapay zeka sistemlerinin bireylerin duygusal durumlarını ya da biyometrik verilerini analiz etme amacıyla kullanılması, kullanıcıların bu süreçten haberdar edilmesini gerektirmektedir.

Yapay zeka sistemlerinin kullanılması bakımından dikkat edilmesi gereken bir diğer husus da sağlayıcılar tarafından önyargılı sonuçlara karşı sistemin sürekli olarak gözden geçirilmesi yükümlülüğüdür. Bu yükümlülük, ilgili sistemler ile elde edilen önyargılı sonuçların analiz edilerek bu sonuçların düzeltilmesi ve ortadan kaldırılması gerekliliğini kapsamaktadır. Örneğin, siyahiler hakkında önyargılı bir sonuç üreten bir yapay zeka sisteminin, bu sonuca nasıl ulaştığını anlamak ve kararı adil, tarafsız ya da açıklanabilir hale getirmek için bu sürecin detaylarının bilinmesi önemlidir. Önyargı, genellikle yapay zeka modelinin eğitildiği veri setlerine yerleşmiştir ve bu veri setleri çoğunlukla önyargılı insan davranışlarını veya toplumsal eğilimleri yansıtmaktadır. Bu nedenle, önyargıyı ortadan kaldırmak sadece algoritmanın düzeltilmesiyle mümkün olmayabilir; aynı zamanda eğitim veri setlerinin de gözden geçirilmesi ve bu tür sistemlerin geliştiricileri arasında

sosyal bilimler ve antropoloji gibi beşerî bilimler alanlarından çeşitli uzmanlıkların yer alması önerilmektedir⁷².

Yapay zeka sistem sağlayıcıların yükümlülükleri göz önüne alındığında AB Yapay Zeka Yasası kapsamında sağlanması gereken bilgiler, ilgili kişilere net ve ayırt edilebilir bir şekilde sunulmalıdır. Benzer olarak GDPR kapsamında da ilgili kişilere sağlanması gereken bilgiler kısa, şeffaf, anlaşılır ve kolayca erişilebilir bir formatta, açık ve sade bir dille sunulmalıdır. İki mevzuat arasındaki önemli bir fark, şeffaflık gerekliliklerine uyum sağlama zamanlamasıyla ilgilidir. AB Yapay Zeka Yasası kapsamında, bilgiler en geç ilgili kişilerin ilk etkileşimi veya yapay zeka sistem uygulamasına maruz kalması sırasında sağlanmalıdır. Ancak AB Yapay Zeka Yasası, GDPR'da olduğu gibi kişisel veriler elde edildiğinde, ilgili kişi ile ilk kez iletişime geçildiğinde veya makul bir süre içinde, ancak en geç bir ay içinde gibi alternatif zaman dilimleri sunmamaktadır. İlgili yasa, bir yapay zeka sistemi kullanılırken sağlayıcıların anında bildirimlerin yapılabileceği bir sistem ve altyapıya sahip olmasının teminini düzenlemektedir. Bu bakımdan yapay zeka sistemleri hakkında kullanıcılara derhal ve kapsamlı bir bilginin sunulma ihtiyacı, ilgili sistemlerin kullanıcı verilerini onları etkileyecek çeşitli yollarla kullanma kapasitesinin yüksekliğinin bir sonucudur.

İşlenen kişisel veriler özelinde incelendiğinde AB Yapay Zeka Yasası'nın biyometrik verilerle ilgili tanımı GDPR'daki tanımla uyumlu olmasına rağmen, AB Yapay Zeka Yasası bu tanımı daha geniş bir perspektiften ele almakta ve biyometrik verilerin kategorize edilmesi, doğrulanması gibi ek terimler barındırmaktadır. Bu durum, farklı tanımların farklı yorumlanma riskini beraberinde taşır ve bu fark, her iki mevzuat için aynı denetim otoritesinin olması durumunda daha az sorun yaratabilecekken, farklı otoritelerin olması uygulamalar arasında farklılıklara yol açmaktadır. Bu bakımdan EDPB, Temmuz 2024 tarihli kurul toplantısında, veri koruma otoritelerinin AB Yapay Zeka Yasası kapsamındaki rolü bakımından ilgili

⁷² **Alicia de Manuel**, "Ethical Assessments and Mitigation Strategies for Biases in AI-systems Used During the COVID-19 Pandemic", Big Data & Society, 2023, s.9.

otoritelerin yapay zekanın temel haklar üzerindeki etkisi konusunda deneyime sahip olduğunu ve bu nedenle birçok durumda “Pazar Gözetim Otoritesi” olarak atanması gerektiğini vurgulamıştır. Bu durum, otoriteler arasında daha iyi koordinasyonu sağlayacak, yasal belirsizlikleri azaltacak ve AB Yapay Zeka Yasası ile AB veri koruma mevzuatının denetimini ve uygulanmasını güçlendirecektir⁷³.

AB Yapay Zeka Yasası ile veri koruma mevzuatları arasındaki ilişki incelendiğinde, GDPR ve KVKK kapsamında gerek birbiriyle uyumlu düzenlemeler olduğu gerekse yapay zeka uygulamalarını da etkileyen yaklaşımlar bakımından ayrışma olduğu görülmektedir. KVKK’da yapay zekaya veya bu teknolojiyi kullanan sistemlere yönelik özel bir hüküm yer almamakla birlikte, genel veri koruma ilkeleri, ikincil düzenlemeler ve Kurul kararları, yapay zeka aracılığıyla kişisel verilerin işlenmesine de uygulanmaktadır. Bu bağlamda, yapay zeka ile işlenen kişisel verilerle ilgili belirleyici hususlar ve GDPR’dan farklılık gösteren noktaların da ele alınması gerekmektedir⁷⁴.

KVKK’nın 4. maddesinde belirtilen genel veri koruma ilkeleri, 108 Sayılı Sözleşme ve 95/46/EC Sayılı Direktif ile uyumlu olarak “hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlarla işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” şeklinde düzenlenmektedir. Bu ilkeler, kişisel verilerin işlenmesinin her aşamasında gözetilmelidir⁷⁵.

⁷³ **European Data Protection Board**, EDPB adopts statement on DPAs role in AI Act framework, EU-U.S. Data Privacy Framework FAQ and new European Data Protection Seal, Temmuz, 2024. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_en (e.t. 19.08.2024).

⁷⁴ **Ezgi Turgut Bilgiç**, Genel Veri Koruma İlkelerinin Yapay Zeka Karşısında Uygulanabilirliği Sorunu, Türkiye Adalet Akademisi Dergisi, Ocak, 2024, s. 247-282. İlgili makaleye internet üzerinden şu link ile ulaşılabilir: <https://dergipark.org.tr/tr/download/article-file/3654085> (e.t. 19.08.2024).

⁷⁵ **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, KVKK Yayınları No 1, Ankara, Aralık, 2019.

KVKK kapsamında yapay zeka ile verilerin işlenmesinde kullanılacak modelin, kişisel verileri işleme sebebi ve amacı açıkça belirtilmelidir. Örneğin, yapay zeka geliştirme çalışmaları gibi genel amaçlar yerine, iş süreçlerinde raporlama faaliyetlerinin yürütülmesi gibi daha spesifik ve belirli amaçlar seçilmelidir. Bu noktada, olay bazında ve seçilen algoritmaya özel bir değerlendirme yapılması önemlidir. Ayrıca, olası bir veri işleme gerekçesiyle kişisel verilerin gerekli olma ihtimali üzerinden depolanması, belirli ve açık amaç ilkesine aykırı olacaktır⁷⁶.

GDPR’ın 6. maddesinin dördüncü fıkrasına göre, kişisel verilerin işlenmesi için belirtilen sebebe bağlı olarak veya bu sebep doğrultusunda diğer amaçlar için de hukuka uygun bir işlem yapılabilecekken, KVKK açısından aynı durum geçerli değildir. Bu nedenle, KVKK kapsamında bireylerin kendi verileri üzerindeki kontrolü kaybetmemesi adına yapay zeka kullanan sistem ve araçların kişisel veri toplama amaçlarının her bir veri işleme faaliyeti için ayrı ayrı belirtilmesi gerekmektedir. KVKK gereği bir veri işleme faaliyetinin hukuka uygun bir zeminde yapılmasının koşulu, sonraki veri işleme amacının ilk veri işleme amacı ile uyumlu olmasıdır⁷⁷. Yeni yapay zeka modellerinde henüz karşılaşılmamış veri işleme amaçlarının ortaya çıkması, veri koruma mevzuatlarının genel ilkelerine uyumlu olarak veri işleme faaliyetinin sürdürülmesi adına karşılaşılan zorluklardan biridir⁷⁸.

Yapay zeka sistemlerinin geliştirilme sürecinde veri koruma etki analizi ve tasarımıyla veri koruma ve varsayılan ayarlarla veri koruma ilkelerinin dahil edilmesi, kişisel verilerin korunması açısından büyük fayda sağlamaktadır. Örneğin, bir yapay zeka uygulaması geliştirildiğinde, kullanıcıların kişisel verilerini işlemek yerine anonimleştirilmiş veya takma isim kullanılmış verilerle çalışacak şekilde ve sadece veri işleme amacının gerektirdiği asgari düzeyde kişisel veriyi işlemek için programlanabilecektir. Ancak, bu ilkelerin uygulanmasının ne kadar etkili olduğu

⁷⁶ **Elif Küzeci**, “Kişisel Verilerin Korunması”, On İki Levha Yayıncılık, 4. Baskı, 2020, s.231.

⁷⁷ **Nafiye Yücedağ**, “Kişisel verilerin korunması kanunu kapsamında genel ilkeler”, Kişisel Verileri Koruma Dergisi, 2019, s.59.

⁷⁸ **Osman Gazi Güçlütürk**, “Yapay Zeka ve Verinin Kullanımı”, On İki Levha Yayıncılık, 2022, s.308.

ve yapay zeka sistemlerinin veri koruma düzenlemelerine uyumu sürekli olarak denetlenmeli ve teknik konular mümkün olduğunca hukuki çerçeveye oturtulmalıdır⁷⁹.

Kişisel verilerin kapsamının geniş olması, yapay zeka uygulamalarında veri işleme sınırlarını belirlemeyi zorlaştırmaktadır. Yapay zeka sistemlerinde kullanılan veriler, teknolojik gelişmeler karşısında korunaksız kaldığında bu durum, kişisel verilerin güvenliğini riske atmaktadır. Bu noktada yapay zeka tarafından elde edilen çıkarımların kişisel veri sayılıp sayılmayacağı hususundaki belirsizliğin de özellikle veri sorumluları tarafından çözülmesi adına yapay zeka kullanılan uygulamaların doğru şekilde analiz edilmesi önemlidir. İlgili kişilerin bilgi edinme ve verilere erişim hakları ile ilgili olarak, yapay zekanın karmaşıklığı ve çıktılarının çeşitliliği, veri sorumlularının kişisel veri mevzuatlarından kaynaklanan bu yükümlülüklerini yerine getirmekte zorlanmasına sebep olmaktadır⁸⁰. Bu nedenle, GDPR ve KVKK gibi kişisel veri mevzuatlarına uygun yapay zeka kullanımı sağlamak için, yapay zeka sistemleri tarafından işlenen kişisel verilerle ilgili bilgi edinme hakkının kapsamının hem veri koruma otoriteleri hem de veri sorumluları tarafından daha net bir şekilde tanımlanması gerekmektedir.

1.5. NIS2 DİREKTİFİ

NIS2 Direktifi (2022/2555 sayılı Direktif)⁸¹, AB genelinde siber güvenlik konusunda düzenlenmiş bir mevzuat olup, AB'deki siber güvenlik seviyesini artırmak için yasal tedbirler sunmaktadır. NIS2 Direktifi, AB'de sektörel çapta uygulanan ilk siber güvenlik yasası olan önceki NIS Direktifi'ni (2016/1148 sayılı Direktif) değiştirmektedir. Üye devletler, bu direktifin hükümlerini Ekim 2024'e kadar ulusal hukuklarına entegre etmek zorundadır.

NIS Direktifi ve NIS2 Direktifi arasındaki temel değişikliklerden bazılarını şu

⁷⁹ **Oğuz Gökhan Yılmaz**, “Yargı Uygulamasında Yapay Zeka Kullanımı- Yapay Zeka Hâkim Cübbesini Giyebilecek mi?”, Adalet Dergisi, sayı 66, 2021, s. 408.

⁸⁰ **Frederike Ufert**, “AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?”, European Papers, 2020, s. 1095.

⁸¹ https://www.europarl.europa.eu/doceo/document/TA-9-2022-0383_EN.html (e.t. 27.08.2024).

şekilde sıralamak mümkündür⁸²:

- NIS2 Direktifi, ekonomi ve toplum için kritik öneme sahip daha fazla sektörü kapsamaktadır. Direktif Ek I’de yüksek kritik öneme sahip sektörler, Ek II’de ise diğer kritik sektörler belirlenmektedir.
- Direktif, düzenlenen kuruluşların tespitinde genel bir kural olarak "büyüklük sınırı" kuralını getirmektedir, bu da direktif kapsamında yer alan sektörlerde faaliyet gösteren veya hizmet sağlayan tüm orta ve büyük ölçekli kuruluşların bu kapsamda değerlendirileceği anlamına gelmektedir.
- NIS2 Direktifi, siber güvenlik ile ilgili olarak yönetim organları için yönetim ve hesap verebilirlik yükümlülükleri getirmektedir. Üye devletler, temel ve önemli kuruluşların yönetim organlarının, bu kuruluşlar tarafından alınan siber güvenlik risk yönetimi önlemlerini onaylamasını, bu önlemlerin uygulanmasını denetlemesini ve direktifin 21. maddesinde belirtilen ihlallerden sorumlu tutulabilmesini sağlamalıdır.
- NIS2 Direktifi, 21. maddede uygulanması gereken temel teknik ve idari tedbirlerin bir listesini içermektedir. Bu önlemler arasında olay yönetimi, iş sürekliliği ve kriz yönetimi önlemlerinin yanı sıra, çok faktörlü kimlik doğrulama, şifreleme ve kriptografi gibi teknik tedbirler yer almaktadır.
- NIS2 Direktifi, NIS Direktifi kapsamında zaten mevcut olan sınır ötesi etkiyi genişletmektedir.
- Tedarik zincirleri ve tedarikçi ilişkilerinin güvenliğine daha fazla vurgu yapılmaktadır.

NIS2 Direktifi, aşırı raporlama ve ilgili kuruluşlar üzerinde aşırı yük

⁸² **Andrew Moir, Kate Macmillan, Hywel Jenkins, Cat Dankos**, “Building Cyber Security Resilience: NIS 2 Enters Into Force”, Mondaq, Şubat, 2023. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://www.mondaq.com/uk/security/1283104/building-cyber-security-resilience-nis-2-enters-into-force> (e.t. 27.08.2024).

oluşturmaktan kaçınmak amacıyla raporlama yükümlülüklerini de düzenlemektedir. Ancak, kapsam dahilindeki hizmetler üzerinde önemli bir etkiye sahip olan olaylar, en geç 24 saat içinde ilgili denetleyici otoritelere bildirilmek zorundadır. Denetleyici otoritenin talebi üzerine ara rapor sunulmalı ve ilk bildirimin yapılmasından en geç bir ay sonra nihai rapor sunulmalıdır. Bir olay, hizmetlerin ciddi şekilde kesintiye uğramasına, ilgili kuruluş için mali kayıplara ya da diğer gerçek veya tüzel kişiler için maddi veya maddi olmayan zararlara yol açmış veya yol açabilecekse önemli olarak kabul edilmektedir.

Bu direktif, artan dijitalleşme ve gelişen siber güvenlik tehditleri karşısında mevcut yasal çerçeveyi çağdaşlaştırmaktadır. Siber güvenlik kurallarının kapsamını yeni sektörler ve kuruluşları da içerecek şekilde genişleterek, kamu ve özel kuruluşların, yetkili otoritelerin ve AB genelinin dayanıklılık ve olaylara müdahale kapasitelerini daha da geliştirmektedir.

AB genelinde yüksek bir ortak siber güvenlik seviyesi için tedbirler içeren NIS2 Direktifi, AB'deki siber güvenlik seviyesini artırmak amacıyla Üye Devletlerin uygun şekilde donatılmasını gerektirerek, örneğin, bir Bilgisayar Güvenliği Olaylarına Müdahale Ekibi (CSIRT) ve yetkili bir ulusal ağ ve bilgi sistemleri (NIS) otoritesi ile hazırlıklı olmalarını hedeflemektedir. Ayrıca Üye Devletler tarafından hayati hizmet operatörleri olarak tanımlanan işletmelerin, uygun güvenlik tedbirlerini alma ve ciddi olayları ilgili ulusal otoritelere bildirme zorunluluğu doğmuştur. Arama motorları, bulut bilişim hizmetleri ve çevrimiçi pazar yerleri gibi kilit dijital hizmet sağlayıcıları da direktif kapsamında güvenlik ve bildirim gereksinimlerine uymakla yükümlü olacaktır⁸³.

Teknolojiye ve dijitalleşmeye artan bağımlılığın olduğu bir dönemde, Avrupa Birliği, NIS2 Direktifi'nin yürürlüğe girmesiyle siber güvenlik çerçevesini önemli ölçüde geliştirmiştir. NIS2 Direktifi, NIS Direktifi'nin temel ilkeleri üzerine inşa

⁸³ Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), European Commission, Eylül, 2023. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive> (e.t. 27.08.2024).

edilmiştir. NIS Direktifi, AB üye devletleri genelinde siber güvenlik uygulamalarının oluşturulmasında bir adım niteliği taşıırken, NIS2 Direktifi bu yaklaşımı daha da ileriye taşımaktadır. NIS Direktifi'nden NIS2 Direktifi'ne olan bu geçiş, AB'nin güçlü siber güvenlik önlemleri sağlamaya, daha sıkı güvenlik protokollerini uygulamaya ve kritik kuruluşlar için olay raporlama mekanizmalarını geliştirmeye olan bağlılığını vurgulamaktadır.

NIS2 Direktifi, şu temel amaçları belirlemektedir⁸⁴:

- Enerji, ulaşım, bankacılık ve sağlık gibi temel sektörler de dahil olmak üzere, kritik kuruluşların genel siber güvenlik duruşunun iyileştirilmesi ve güvenlik önlemlerinin güçlendirilmesi.
- Şeffaflığı artırmak ve siber tehditlere karşı koordineli bir yanıt sağlamak amacıyla, olay raporlama gerekliliklerinin standart hale getirilmesi.
- Siber risklerin gelişen doğasını yansıtarak, daha geniş bir sektör ve dijital hizmet sağlayıcı yelpazesini kapsayacak şekilde düzenlemenin kapsamının genişletilmesi.
- Ulusal denetim önlemlerinin güçlendirilmesi ve siber olaylara etkili bir şekilde yanıt vermek için AB genelinde iş birliğinin artırılması.

NIS2 Direktifi, dijital tehditlerin artan çeşitliliğini ve birçok sektörde dijital sistemlere olan yüksek bağımlılığı ele alarak AB siber güvenlik kurallarını önemli ölçüde genişletmektedir. NIS2 Direktifi, risk yönetimi, olay raporlama ve tedarik zinciri güvenliğini kapsayan daha katı uyum gereklilikleri getirmektedir. Özellikle küçük kuruluşlar ve yeni kapsama alınan sektörler için uyum sağlamak önemli bir kaynak yatırımı gerektirirken, aynı zamanda önemli fırsatlar da sunmaktadır. Siber güvenlik sektörü için, direktife uyumla ilgili çözümler için yeni pazarlar

⁸⁴ **Vlerë Hyseni**, “A Comprehensive Guide: Understanding the NIS 2 Directive”, PECB, Kasım, 2023. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://www.mondaq.com/uk/security/1283104/building-cyber-security-resilience-nis-2-enters-into-force> (e.t. 27.08.2024).

açılmaktadır.

NIS 2 Direktifi, siber güvenlik risk yönetiminin önemini vurgulamakta ve kilit kuruluşların kapsamlı uygulamaları benimsemesini zorunlu kılmaktadır. Bu, siber risklerin tanımlanması, değerlendirilmesi ve azaltılmasını, ileri güvenlik önlemlerinin entegrasyonunu ve düzenli denetimleri içermektedir. Ayrıca direktif, modern dijital altyapıların birbirine bağlı doğasını yansıtarak tedarik zinciri güvenliğinin önemini kabul etmektedir. Genel olarak, NIS2 Direktifi'nin risk yönetimine verdiği önem, daha güvenli ve dayanıklı bir dijital ortam oluşturmak için kritik olmaktadır.

NIS2 Direktifi'nin 21. maddesi, Üye Devletlerin, temel ve önemli kuruluşlar için siber güvenlik risk yönetimi önlemlerini uygulamasını zorunlu kılmaktadır. Bu önlemler, kuruluşun risk maruziyetine, boyutuna ve potansiyel olay etkisine göre uyarlanarak, sektör standartları ve maliyet değerlendirmeleri ile uyumlu teknik, operasyonel ve idari stratejiler gerektirmektedir.

NIS2 Direktifi, risk analizi, olay yönetimi, iş sürekliliği ve tedarik zinciri güvenliğini kapsayan kapsamlı siber güvenlik önlemlerini belirlemektedir. Uyum sağlamayan kuruluşlar düzeltici eylemler almak zorundadır. Komisyon, spesifik hizmet sağlayıcılar ve kuruluşlar için teknik ve metodolojik gereksinimlerin benimsenmesinden sorumludur ve bu süreçte ENISA ile istişarelerde bulunarak AB ve uluslararası standartlarla uyumu sağlamaktadır.

NIS2 Direktifi'nin uygulanmasının, AB dijital pazarında önemli bir etkiye sahip olması beklenmektedir. Bu yönüyle Direktif, üye devletler genelinde birleşik ve güçlü siber güvenlik standartları belirleyerek sadece dijital altyapının güvenliğini artırmakla kalmamakta, aynı zamanda dijital alanda faaliyet gösteren işletmeler için eşit şartlar sağlamaya katkıda bulunmaktadır.

NIS2 Direktifi, AB dijital pazarında siber güvenlik standartlarını güçlendirmekte ve dijital altyapının güvenliğini artırarak işletmeler için eşit şartlar sağlamaktadır. Artan siber güvenlik önlemleri, şirketlerin yeni çözümler geliştirmesine olanak

tanýarak sektörde yenilięi teřvik etmektedir.

1.6. AB SİBER DAYANIKLILIK YASASI

1 Aralık 2023 tarihinde, 2020 AB Siber Güvenlik Stratejisi'nde Komisyon tarafından duyurulan yeni AB Siber Dayanıklılık Yasası konusunda bir siyasi anlaşmaya varılmıştır. Takiben yasa, Mart 2024'te Avrupa Parlamentosu tarafından resmi olarak onaylanmıştır. Avrupa Konseyi tarafından nihai versiyonunun onaylanmasını takiben AB Resmi Gazetesi'nde yayımlandıktan sonra AB Siber Dayanıklılık Yasası'nın çoęu hükmü yürürlüęe girmesinden 36 ay sonra uygulanmaya başlayacaktır.

AB Siber Dayanıklılık Yasası, dijital bileřenlere sahip ürünlerin ve yazılımların siber güvenlięini saęlayarak tüketicileri ve işletmeleri korumayı hedeflemektedir. Yasa, AB'de giderek daha fazla kullanılan bağlanabilir ürünlerdeki güvenlik açıklarına ilişkin endişeleri ele alarak ürün yaşam döngüsü boyunca karşılanması gereken zorunlu siber güvenlik gereksinimlerini belirlemektedir. Yasanın hedefinde, siber güvenlik olaylarının sayısını azaltarak olay yönetimi ve şirketlerin itibar kaybı maliyetlerinin düşürölmesi de mevcuttur. Bu durum, tüketicilerin şirketlere ve ürünlere olan güvenlięini artırarak, AB içinde ve dışında dijital bileřenlere sahip ürünlere olan talebi artıracaktır. Daha az güvenlik riski ve olayı sayesinde, tüketiciler ve vatandaşlar veri koruma ve gizlilik gibi temel hakların daha iyi korunmasından yararlanacaktır.

Siber Dayanıklılık Yasası, ayrıca AB'nin iç pazarı dışında uluslararası bir referans noktası haline gelme potansiyeline de sahiptir. Bu yasaya dayalı AB standartları, yasanın uygulanmasını kolaylařtırmakta ve küresel pazarlarda AB'li üreticiler için bir avantaj saęlamaktadır.

AB Siber Dayanıklılık Yasası, doğrudan veya dolaylı olarak başka bir cihaza veya aęa bağlanan tüm ürünlere, yazılım ve donanım dahil olarak uygulanacaktır. Uyumsuzluk durumunda, piyasa denetim otoriteleri, üreticilerin uyumsuzluęu sona erdirmesini ve riski ortadan kaldırmasını, bir ürünün piyasada bulunmasını

yasaklamasını veya kısıtlamasını ya da ürünün geri çekilmesini veya toplatılmasını karara bağlayacaktır. Ayrıca kurallara uymayan şirketlere para cezası uygulaması da söz konusudur.

AB Siber Dayanıklılık Yasası kapsamında yer alan dijital bileşenlere sahip ürünlerin üreticilerinin temel yükümlülükleri aşağıda sayılmaktadır⁸⁵:

- Ürünleri AB pazarına sunmadan önce dijital bileşenlere sahip ürünlerin tasarımı, geliştirilmesi ve üretimi için bir dizi kurala uymak.
- Bu ürünlerle ilgili siber güvenlik risklerinin değerlendirilmesini belgelemek.
- Dijital bileşenlere sahip ürünler için uygunluk değerlendirmesi yapmak veya yaptırmak, bir AB uygunluk beyanı hazırlamak ve ürüne CE işareti eklemek.
- Üçüncü taraf bileşenleri, açık kaynaklı yazılımlar dahil, entegre ederken gerekli özeni göstermek.
- Aktif olarak istismar edilen güvenlik açıklarını CSIRT'a ve etkilenen kullanıcılara bildirmek.
- Destek süresi boyunca, prensip olarak beş yıl, ilgili güvenlik güncellemeleri dahil olmak üzere, uyumlu güvenlik açığı yönetim süreçlerini uygulamak.

Bu ürünlerin ithalatçıları ve dağıtıcıları da ilgili süreçlere ilişkin yükümlülüklerle tabidir.

AB Siber Dayanıklılık Yasası'nın kapsamı incelendiğinde, hizmet olarak sunulan yazılımların yer almadığı görülmektedir. Bunun nedeni, yasanın yalnızca AB tek pazarında satılan dijital bileşenlere sahip ürünleri kapsaması ve bu ürünlerin üreticileri için somut siber güvenlik gereksinimleri ve yükümlülükleri

⁸⁵ <https://www.dlapiper.com/en/insights/topics/cyber-resilience-act> (e.t. 28.08.2024).

belirlemesidir. Bununla birlikte, AB genelinde yüksek düzeyde siber güvenlik sağlamak için alınan tedbirlere ilişkin NIS2 Direktifi ve diğer sektörel mevzuatlar, hizmet olarak sunulan veya kurum içi geliştirilen sistemlerin siber güvenlik için eşdeğer teknik gereksinimleri karşılamasını sağlamaktadır. AB Siber Dayanıklılık Yasası'nın NIS2 Direktifi'ni tamamlayıcı düzenlemeleri olup, NIS2 Direktifi temel ve önemli kuruluşlar için tedarik zinciri güvenliği önlemleri ve olay raporlama yükümlülükleri dahil olmak üzere siber güvenlik gereksinimlerini ortaya koymakta ve bu kuruluşların sağladıkları hizmetlerin dayanıklılığını artırmayı amaçlamaktadır. Bu nedenle, dijital bileşenlere sahip ürünlerin artırılmış siber güvenlik düzeyi, NIS2 Direktifi kapsamındaki kuruluşların uyumunu kolaylaştıracak ve tüm tedarik zincirinin güvenliğini güçlendirecektir⁸⁶.

Piyasa gözetim otoriteleri, AB Siber Dayanıklılık Yasası'nın getirdiği yükümlülüklerle uymayan kuruluşlardan, uyumsuzluğu gidermelerini, riski ortadan kaldırmalarını, ürünlerin piyasaya sunulmasını yasaklamalarını veya geri çekmelerini talep edebilmektedir. Ayrıca bu otoriteler, uyumsuzluk durumunda idari para cezası uygulama yetkisine de sahiptir. AB Siber Dayanıklılık Yasası'na uymayan kuruluşlara verilebilecek azami ceza, 15 milyon Euro'ya veya teşebbüslerin dünya çapındaki yıllık cirosunun %2,5'ine kadar olarak belirlenmiş olup, hangisi daha yüksekse o ceza bedeli uygulanacaktır⁸⁷.

1.7. YASAL GELİŞMELERİN BAĞLANABİLİR ARAÇLARDA VERİ İŞLENMESİ KAPSAMINDA İNCELENMESİ

Bağlanabilir araçlarda veri gizliliği kapsamındaki çalışmalar incelendiğinde, AB'de yürürlüğe giren çalışmaların başı çektiği görülmektedir. Kişisel verilerin korunmasına yönelik AB'de yürürlükte olan temel mevzuat, kişisel verilerin korunmasına ilişkin detaylı düzenlemeler getiren ve 95/46 Sayılı Direktifi yürürlükten kaldıran GDPR'dır. GDPR, AB içerisindeki genel veri koruma

⁸⁶ https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5375 (e.t. 30.08.2024).

⁸⁷ <https://www.gsg hukuk.com/tr/bultenler-yayinlar/duyurular/siber-dayaniklilik-yasasi.html> (e.t. 30.08.2024).

mevzuatı olarak kişisel veri işleme faaliyeti olan sektörlerin tümü için kişisel veri gizliliği ve korunması kurallarını düzenlemektedir. Ek olarak, kişisel verilerin korunmasına ilişkin düzenleme içeren e-Gizlilik Direktifi (“2002/58/EC sayılı Direktif”) ise elektronik iletişim sektöründeki kuralları düzenlemekte olup bağlanabilir araçta işlenen veriler araç dışında bulunan sunucuya, başka bir araca veya altyapıya iletilildiğinde bağlanabilir araçlar için de uygulanabilir olmaktadır.

İlerleyen teknoloji ile kişisel verilerin korunması alanında daha kapsamlı ve güçlü mevzuat taleplerindeki belirgin artış sonucu ortaya çıkan GDPR, dünyadaki en katı veri düzenleme mevzuatlarından biri olarak kabul edilmektedir. GDPR, bağlanabilir araç üreticilerini barındırdığı hüküm ve temel ilkelerle etkilemektedir. Kişisel veri işleme ilkeleri, özellikle veri minimizasyonu ilkesi, bağlanabilir araçlarda veri toplamanın yalnızca amaca uygun, sınırlı ve ölçülü verilerle sınırlı olmasını önererek uygulanmaktadır. Veri minimizasyonu ilkesi GDPR kapsamında açıkça belirtilmişken, KVKK’da bu ilke doğrudan ifade edilmemektedir. Ancak, uygulamadaki düzenlemeler ve temel ilkeler çerçevesinde, veri minimizasyonunun, amaçla bağlantılı, sınırlı ve müdahaleci olmayan veri işleme biçimlerinde yer bulduğu gözlemlenmektedir⁸⁸.

GDPR’a yanıt olarak, AB’de faaliyet gösteren bazı otomobil üreticileri, araçların güvenlik seviyelerini koruyabilmesi için ilgili kişilerin kişisel verilerine erişim hakkına sahip olmaması gerektiğini öne sürmüşlerdir. Ancak göz önünde tutulması gereken diğer bir görüş ise endüstrinin rekabetçiliği göz önüne alındığında, veri taşınabilirliği ihtiyacının olduğu ve ilgili kişilerin verilerine erişiminin engellenmesinin rekabeti zayıflatacağıdır. GDPR, bağlanabilir cihazlar tarafından üretilen verilere kimin erişebileceği ve bu verileri kullanabileceği konusunda netlik sağlamamaktadır ve küçük ve orta ölçekli işletmeler, daha güçlü oyuncularla veri paylaşım anlaşmaları müzakere etme konusunda genellikle zayıf bir konumda bulunmaktadır. Bu durum da dengesiz anlaşmaların ortaya çıkmasına neden

⁸⁸ Bkz. Kişisel Verileri Koruma Kurumu, “İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık)” (e.t. 31.07.2024).

olmaktadır. Ayrıca, GDPR gibi yasal düzenlemelerin sektörel etkisi olan diğer mevzuatlarla beraber ele alınmaması çerçevesinde, farklı sektörlerden gelen verilerin birleştirilmesi sınırlanmakta, bu da ekonomide verilerin yeterince kullanılmamasına, tüketici tercihlerinin, kamu hizmetlerinin sunumunun ve yeniliğin olumsuz etkilenmesine yol açmaktadır⁸⁹. Örneğin, Komisyon tarafından yürütülen beş yıllık bir çalışma, geçtiğimiz dönemlerde otomobil üreticilerinin üçüncü taraf hizmet sağlayıcıların dijital hizmetlerde rekabet etme yeteneğini zayıflattığını ortaya koymuştur. Kullanıcılar ve hizmet sağlayıcılar, araç verilerine erişim konusunda etkin piyasa rekabeti, yenilikçilik ve gerçek tüketici tercihi sağlayan düzenleyici çerçeveye ihtiyaç duymakta olup Komisyon'un bu çerçeveyi sunamaması, araç üreticilerinin adil rekabete zarar vermesine ve AB Veri Yasası ile doğrudan çelişecek şekilde kendilerini dayatmasına olanak sağlamaktadır⁹⁰.

Bu eksiklikleri gidermeyi amaçlayan AB Veri Yasası'nın başlıca amaçlarından biri, verilerin yeniden kullanımı için daha erişilebilir hale getirilmesidir. GDPR'dan farklı olarak, yalnızca kişisel verilerle sınırlı olmayan AB Veri Yasası hem kişisel hem de kişisel olmayan verileri kapsamakta, bu da daha geniş bir uygulama alanına sahip olduğu anlamına gelmektedir. AB Veri Yasası'nda yer alan bazı hükümler bağlanabilir araç sektörünü de doğrudan etkilemektedir. Örneğin, dış organizasyonlarla veri paylaşımıyla ilgili olarak yasa, araç üreticisi gibi verileri elinde tutan tarafların ilgili verileri makul, ayrımcı olmayan ve adil şartlar altında üçüncü taraflara sağlamasını zorunlu kılmaktadır.

AB Veri Yasası'nda bağlanabilir araçları etkileyecek bir diğer koşul, hizmet değiştirme ve birlikte çalışabilirlik gereksinimidir. Bu durum üreticilerin, kullanıcıların hizmet sağlayıcılar arasında kolayca geçiş yapmasına veya birden fazla hizmet sağlayıcıyı aynı anda kullanmasına yardımcı olmak için belirli önlemler almasını zorunlu kılmaktadır. Fédération Internationale de l'Automobile (FIA) Avrupa Bürosu tarafından yapılan değerlendirmede, otomobil gibi pahalı

⁸⁹ <https://iapp.org/resources/article/connected-cars-canada/> (e.t. 10.08.2024).

⁹⁰ <https://www.theparliamentmagazine.eu/partner/article/europe-on-the-move-access-to-vehicle-data-legislation-is-urgently-needed> (e.t. 10.08.2024).

araçların tamir ve bakımında adil rekabetin sağlanması ihtiyacı göz önüne alındığında, otomotiv sektörünün geleneksel olarak sektöre özgü mevzuatla yönetildiği ve her ne kadar dijitalleşme ile araçların kullanımı, bakımı, onarımı ve sigortalanması konusunda önemli uygulama ve gelişmeler gündeme gelse de bu yeni uygulamaların araç sahibi veya sürücülerin araçlarını kullanarak ürettikleri veri akışlarını kontrol etmekten ve yönetmekten mahrum bırakmaması gerektiği belirtilmektedir⁹¹. Bu bakımdan AB Veri Yasası ile, araç sahibi ve sürücüler gibi kullanıcıları merkeze koyan kurallar tanımlanarak, sektörler arasında işletmelerin, kullanıcıların ve hükümetlerin haklarını belirleyen veri alışverişleri için uyumlu bir çerçeve oluşturulması mümkün kılınmaktadır.

Öte yandan AB Veri Yasası'nın otomotiv endüstrisine uygulanması, bazı zorlukları da beraberinde getirmektedir. Avrupa Otomotiv Tedarikçileri Birliği ("CLEPA"), otomotiv sektörünün karmaşıklıklarını yansıtarak, özellikle tedarikçilerle ilgili olarak daha sektör spesifik mevzuatın gerekli olduğunu vurgulamaktadır. CLEPA, hizmet sağlayıcıların veri odaklı gelişmelerden tam anlamıyla faydalanabilmeleri ve üreticilerle daha dengeli bir ilişki kurabilmeleri için sektörel düzenlemelerin gerekli olduğunu belirtmektedir⁹².

Otomotiv endüstrisinde yapay zeka teknolojileri de pek çok yeni uygulamaya kapı açmıştır. Sürücüsüz araçların üretimi 1950'lerden sonra başlamıştır. Yapay zekanın ilk örnekleri akıllı araçlarda kullanılmıştır. 1958'de General Motors ve 1977'de Japonya'daki Tsubuka Mekanik Mühendislik Laboratuvarı gibi büyük otomobil şirketleri kendi prototiplerini üretmişlerdir. Bu faaliyetler, Ernst Dickmann'ın otonom kara aracı ve birçok başka örnekle devam etmiştir. Güncel gelişmelere bir örnek olarak, Elon Musk, Tesla'nın tamamen kendi kendine sürüş

⁹¹ <https://www.theparliamentmagazine.eu/partner/article/europe-on-the-move-access-to-vehicle-data-legislation-is-urgently-needed> (e.t. 10.08.2024).

⁹² <https://autovista24.autovistagroup.com/news/european-data-act-empowers-users-connected-vehicles/> (e.t. 11.08.2024).

yapabilen bir oto pilot sistemini hayata getirmiştir⁹³.

Özellikle bağlanabilir araçlar, bu teknolojilerin etkin bir şekilde uygulanmasına olanak tanıyan yenilikleri bünyesinde barındırmaktadır. Bağlanabilir araçlar, sürüş güvenliğinden sürücü asistanlarına, eğlence sistemlerinden otonom sürüş özelliklerine kadar geniş bir şekilde yapay zeka destekli sistemlere sahiptir. Bu durum, veri toplama ve işleme süreçlerini daha karmaşık hale getirmekte ve dolayısıyla bu süreçlerin düzenlenmesi ihtiyacını doğurmaktadır. AB Yapay Zeka Yasası bu bakımdan, bağlanabilir araçların tasarımı, geliştirilmesi ve kullanımı üzerinde önemli etkiler yaratacak olan kapsamlı bir düzenlemedir.

Bağlanabilir araçlar, yapay zeka teknolojileri açısından genellikle yüksek risk kategorisine girmektedir. Bu araçlar, sürüş güvenliğini sağlamak, sürücü davranışlarını izlemek ve araç performansını optimize etmek için yapay zeka sistemlerinden yoğun bir şekilde yararlanmaktadır. Dolayısıyla, AB Yapay Zeka Yasası, bu sistemlerin hem geliştirilmesi hem de uygulanması sırasında sıkı bir denetim ve uyumluluk süreci gerektirmektedir.

Bağlanabilir araçlarda kullanılan yapay zeka sistemleri, genellikle sürücü asistanları, otonom sürüş sistemleri, güvenlik sistemleri ve eğlence sistemleri gibi çeşitli alanlarda söz konusu olacaktır. Bu sistemlerin çoğu, insan güvenliği, veri gizliliği ve etik değerler açısından yüksek risk taşıdığından, AB Yapay Zeka Yasası'nın katı düzenlemelerine tabidir. Örneğin otonom sürüş sistemleri, bağlanabilir araçlarda kullanılan yapay zeka teknolojilerinin en kritik uygulamalarından biridir. Bu sistemler, aracın çevresini algılamak, sürüş kararları almak ve gerektiğinde tehlikelerden kaçınmak için büyük miktarda toplanan veriyi işlemektedir. AB Yapay Zeka Yasası kapsamında, bu tür yüksek riskli sistemler, güvenlik ve performans standartlarına uygunluk açısından titizlikle değerlendirilmelidir. Ayrıca, bu sistemlerin geliştirilmesi sırasında yapay zeka

⁹³ **Scott McLachlan, Evangelia Kyrimi, Kudakwashe Dube, Norman E. Fenton, Burkhard Schafer:** “The Self-Driving Car: Crossroads at the Bleeding Edge of Artificial Intelligence and Law”, Cornell University, Workingpaper, 2022.

modellerinin eğitilmesi ve test edilmesi aşamalarında veri koruma ve güvenlik önlemlerine de dikkat edilmesi gerekmektedir.

Yüksek riskli yapay zeka sistemleri için etik ve şeffaflık gereksinimleri, bağlanabilir araçlarda kullanılan yapay zeka sistemlerinin şeffaf bir şekilde tasarlanmasını ve kullanıcılara bu sistemlerin nasıl çalıştığına dair açık ve anlaşılır bilgiler verilmesini zorunlu kılmaktadır. Ayrıca, bu sistemlerin karar alma süreçlerinin izlenebilir olması ve gerektiğinde bu kararların nasıl alındığının açıklanabilir olması gerekmektedir. Özellikle otonom sürüş sistemleri gibi hayati kararlar alan yapay zeka uygulamaları için bu husus kritik bir öneme sahiptir.

AB Yapay Zeka Yasası, yapay zeka sistemlerinin geliştirilmesi ve uygulanması sırasında GDPR gereklilikleriyle de yakından ilişkilidir. Özellikle, yapay zeka sistemleri kişisel verileri işlediğinde, bu verilerin korunması ve gizliliğinin sağlanması büyük bir önem taşımaktadır. Bu bakımdan GDPR'ın ilgili maddelerinin AB Yapay Zeka Yasası kapsamında incelenmesi gerekmektedir.

Bağlanabilir araçlarda yapay zeka sistemlerinin otomatik kararlar alması durumunda, GDPR'ın 22. maddesi devreye girmektedir. Bu madde, ilgili kişiler üzerinde yasal sonuçları olan veya benzer şekilde önemli bir etki yaratan otomatik kararların alınmasını düzenleyerek bu tür işlemlerin rıza gerektirdiğini belirtmektedir. Dolayısıyla, yapay zeka sistemlerinin araç sahibi / sürücüsü veya yolcusu hakkında otomatik kararlar alması durumunda, bu süreçlerin GDPR ile uyumlu olması ve gerekli rızanın alınması gerekmektedir.

Bağlanabilir araçlarda kullanılan yapay zeka sistemleri, büyük miktarda kişisel veri işlemektedir. AB Yapay Zeka Yasası, bu verilerin güvenliğini sağlamak için sıkı güvenlik önlemleri alınmasını düzenlemektedir. Ayrıca, verilerin anonimleştirilmesi ve takma adlandırılması gibi veri koruma yöntemlerinin kullanılması, veri güvenliğini artırılmasına katkı sağlamaktadır. Bu yöntemlerin kullanılması özellikle araç içi sistemlerde toplanan verilerin üreticiler veya üçüncü taraflarla paylaşılması durumunda büyük bir önem taşımaktadır. Bağlanabilir araç

üreticilerinin yapay zeka sistemlerini tasarım aşamasından itibaren AB Yapay Zeka Yasası ve GDPR gibi uygulanabilir mevzuatlara uyumlu hale getirmesi adına yasal danışmanların erken aşamada sürece dahil edilmesi ve yapay zeka sistemlerinin düzenlemelere uygunluğunun değerlendirilmesi gerekmektedir. Bu bağlamda yapay zeka teknolojilerinin etik ve güvenli bir şekilde geliştirilmesi, otomotiv endüstrisinin dijital dönüşümünde önemli bir kilometre taşı olacaktır.

GDPR'daki düzenlemelere ek olarak, Kurum'un "Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler" başlıklı dokümanında, yapay zeka sistemi geliştiricileri, üreticiler, karar alıcılar ve hizmet sağlayıcılar için tavsiyeler sunulmakta ve uygulamada karşılaşılabilecek zorluklara karşı kişisel verilerin korunmasını sağlayan yöntemlere işaret edilmektedir⁹⁴.

2024 yılı Nisan ayında CNIL, yapay zeka sistemlerinin geliştirilmesi sırasında kişisel veri işleme faaliyetlerine ilişkin pratik kılavuzlar⁹⁵ yayımlamıştır. Kılavuzlarda, yapay zeka tabanlı sistem sağlayıcılarının, GDPR'a uyumlu olabilmeleri için ele almaları gereken dört temel konu öne çıkmaktadır:

- Yapay zeka sistem sağlayıcısının, verilerin seçimi ve sistem geliştirmesi gibi inisiyatifler alması durumunda veri sorumlusu olarak hareket ettiği kabul edilmektedir. Bununla birlikte, belirli talimatlar doğrultusunda araç üreticisi adına sistem geliştiriyorsa, veri işleyen olarak da değerlendirilebileceğinden bu rol, her durum özelinde değerlendirilmelidir.
- GDPR'ın amaç sınırlaması ilkesi uyarınca, kişisel verilerin toplanması belirli, açık ve meşru amaçlar için olmalıdır. Yapay zeka sisteminin geliştirme aşamasında nihai amacın belirli olması durumunda uyum sağlamak daha kolaydır, ancak bu her zaman mümkün olmamaktadır. CNIL, belirli bir sistem türü ve teknik fonksiyonlar ile ilgili olarak işleme faaliyetlerinin yeterince

⁹⁴ **Kişisel Verileri Koruma Kurumu**, "Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler" (Erişim Tarihi: 31.07.2024).

⁹⁵ <https://www.cnil.fr/fr/tenir-compte-de-la-protection-des-donnees-dans-la-collecte-et-la-gestion-des-donnees> (e.t. 31.08.2024).

belirlenmiş olması haline sistemin meşru kabul edilebileceğini belirtmektedir.

- GDPR'a göre kişisel verilerin işlenmesi ancak yasal dayanaklardan birinin varlığı durumunda mümkündür. Geçerli bir rıza sağlanamadığında, alternatif bir yasal dayanak gereklidir. Söz konusu hukuki sebep genellikle meşru menfaat olacaktır, ancak bu durumda da veri sorumlusunun menfaatleri ile ilgili kişilerin hakları arasında denge testi yapılması gerekmektedir.
- Yapay zeka sisteminin tasarım aşamasında, veri minimizasyonu gibi GDPR veri koruma ilkelerine uyulması önemlidir. Verilerin yalnızca ilgili ve gerekli olanlarının toplanması, anonimleştirme süreçlerinin uygulanması ve düzenli olarak veri tabanının izlenmesi gibi önlemler alınmalıdır. Ayrıca, verilerin saklama süreleri belirlenmeli ve uygun teknik ve idari tedbirler uygulanmalıdır.

Bağlanabilir araçlarda veri işlemeye yönelik AB'deki veri koruma otoriteleri çalışmalar yürütmekte ve bu alanı düzenleyici rehberler yayımlamaktadır. EDPB tarafından 9 Mart 2021 tarihinde yayımlanan “Bağlanabilir Araçlar Kapsamında Kişisel Verilerin İşlenmesine İlişkin Rehber” bağlanabilir araçlarda kişisel veri işlenmesi alanında yayımlanan en önemli kaynaklardanır.

Fransa'da veri koruma otoritesi olan CNIL (“Commission Nationale de l'Informatique et des Libertés”) tarafından Ekim 2017'de sektör paydaşlarına tasarımıyla veri koruma ve varsayılan ayarlarla veri koruma ilkelerine uygun olarak nasıl entegre edileceği konusunda yardım sağlamak ve ilgili kişinin verileri üzerinde kontrole sahip olmaları amacıyla “Connected vehicles and personal data” isimli uyum paketini yayımlamıştır. Alman Federal ve Eyalet Veri Koruma Otoriteleri Konferansı ve Alman Otomotiv Endüstrisi Birliği Ocak 2016'da bağlanabilir araçlarda veri koruma ilkelerinin de düzenlendiği ortak bir bildiri yayımlamıştır⁹⁶.

AB'de araçlarda otomatik olarak 112 acil çağrı sistemini devreye alan araç içi

⁹⁶ https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf (e.t. 20.05.2024).

acil çağrı sisteminin (“eCall”) ilk düzenlemeleri 2007 yılında gündeme gelmiştir. 2015/718 sayılı "Araç İçi 112 Çağrı Sistemlerine İlişkin Tıp Onayı Yönetmeliği" ise 31 Mart 2018 tarihinden itibaren AB ülkelerinde üretilen araçların bu sisteme uyumlu hale getirilmesini zorunlu kılmıştır.

AB, eCall sistemini tasarlarken gizliliği temel bir ilke olarak belirlemiştir. Sistem, bir kaza tetiklemediği sürece veri toplamayacağı, acil servislere yalnızca minimal ve belirlenmiş bir veri setini göndereceği ve bu verileri saklamayacağı veya ikincil amaçlar için kullanmayacağı şekilde tasarlanmıştır⁹⁷. Tüm yolcu araçlarının bir kaza durumunda otomatik acil çağrı yapabilme yeteneği ile donatılması zorunluluğuna karşı Komisyon gizlilik konularını göz ardı etmeyerek yeni eCall sisteminin gizlilik etkilerinden endişe duyan vatandaşlara yanıt olarak sunulan bilgi yazısında⁹⁸, sayılan veri koruma önlemlerini belirtmiştir:

- eCall araç içi sistemi aracılığıyla yapılan herhangi bir kişisel veri işleme faaliyeti, 95/46/EC ve 2002/58/EC sayılı Direktiflerde öngörülen kişisel veri koruma kurallarına uygun olmaktadır.
- Araç üreticileri, eCall tetiklenmeden önce eCall araç içi sisteminin izlenmeye tabi tutulamayacağını temin etmelidir.
- eCall araç içi sisteminin dahili hafızasında aracın önceki konumlarının saklanmasına izin verilse de yalnızca aracın mevcut konumunu ve seyahat yönünü belirlemek için gerekli olan verilerin saklanmasını sağlamak amacıyla bu verilerin sürekli olarak silinmesi gerekmektedir. Bu veriler, eCall tetiklenmeden önce araç içi sistemin dışındaki herhangi bir kuruma sunulmamalıdır.

⁹⁷ **Philippa Lawson**, “The Connected Car: Who is in the Driver’s Seat?”, The BC Freedom of Information and Privacy Association (“FIPA”), İlgili rapora internet üzerinden şu link ile ulaşılabilir: https://fipa.bc.ca/wp-content/uploads/2018/01/CC_report_lite.pdf (e.t. 30.08.2024).

⁹⁸⁹⁸ **European Commission**, “eCall – Do you have any concerns for your privacy? You shouldn't ...”, Haziran, 2014. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://digital-strategy.ec.europa.eu/en/library/ecall-do-you-have-any-concerns-your-privacy-you-shouldnt> (e.t. 30.08.2024).

- eCall kullanıcılarına uygun düzeyde gizlilik koruması sağlamak ve izleme ve kötüye kullanımı önlemek için araç içi eCall sistemine veri güvenliğini artırıcı teknolojiler entegre edilmelidir.
- eCall araç içi sistemi tarafından gönderilen minimum veri seti, yalnızca EN 15722:2011 "Akıllı ulaşım sistemleri - eSafety - eCall minimum veri seti (MSD)" standardında belirtilen minimum verileri içermelidir.
- eCall araç içi sistemine dahil edilen kişisel veriler, ilgili Kamu Güvenliği Yanıt Noktası'na (PSAP) iletilmeleri için gerekli olan süre boyunca saklanmalıdır. Gönderilen veriler yalnızca gönderildikleri amaç için kullanılmalı ve işleme amaçları sona erdiğinde imha edilmelidir.

AB'de bağlanabilir araçlarda siber güvenliğin sağlanması için ENISA⁹⁹ tarafından faaliyetler yürütülmektedir. ENISA tarafından 2019'da yayımlanan "Akıllı Araçların Güvenliği için İyi Uygulamalar" raporu, bağlanabilir araç sahibi / sürücülerinin araç kullanım süreçlerini iyileştirmeye yönelik ve bağlanabilir araç güvenliğine yönelik iyi uygulamaları tanımlamaktadır.

NIS2 Direktifi, bağlanabilir araçlarda siber güvenlik standartlarının uygulanmasında kritik bir rol oynamaktadır. Bu direktif, otomotiv sektörü gibi dijital sistemlere dayanan kritik öneme sahip sektörleri kapsayarak, siber güvenlik önlemlerinin güçlendirilmesini hedeflemektedir. Bağlanabilir araçlar, veri üretimi ve paylaşımı açısından büyük önem taşımaktadır ve bu nedenle NIS2 Direktifi, araç üreticilerinin bu verilerin güvenliğini sağlamak için gerekli teknik ve idari tedbirleri almasını zorunlu kılmaktadır.

Bağlanabilir araçlar, yüksek düzeyde dijitalleşmiş sistemlerdir ve bu araçların güvenliği, sadece kullanıcıların güvenliği için değil, aynı zamanda tüm dijital altyapının korunması için de kritik öneme sahiptir. NIS2 Direktifi, araç üreticilerinin bu sistemlerin güvenliğini sağlamak için olay yönetimi, iş sürekliliği

⁹⁹ ENISA, Good Practices for Security of Smart Cars.

ve kriz yönetimi gibi temel siber güvenlik önlemlerini uygulamasını gerektirmektedir. Ayrıca, tedarik zinciri güvenliği de direktifin önemli bir parçasıdır, bu da araç üreticilerinin tedarikçileri ve diğer iş ortakları ile olan ilişkilerini güvence altına almasını zorunlu kılmaktadır.

NIS2 Direktifi'nin getirdiği bir diğer önemli yenilik, siber güvenlik yönetimi ve hesap verebilirlik yükümlülüklerinin araç üreticilerinin yönetim organlarına getirilmesidir. Bu, üst düzey yöneticilerin siber güvenlik risklerini aktif olarak yönetmelerini ve olası ihlallerden sorumlu tutulmalarını gerektirir. Bu yükümlülük, bağlanabilir araçlarda siber güvenlik yönetiminin daha sistematik ve entegre bir şekilde ele alınmasını sağlayarak olası güvenlik açıklarını minimize etmektedir.

NIS2 Direktifi'nin bağlanabilir araçlarda uygulanması, sadece araç üreticilerini değil, aynı zamanda tüm ekosistemi kapsayacak şekilde geniş bir etkiye sahiptir. Bu etki hem tüketicilerin hem de ticari kullanıcıların siber tehditlere karşı daha iyi korunmasını sağlamakta ve dijital pazarda güvenliğin artırılmasına katkıda bulunmaktadır. Bu bağlamda, bağlanabilir araçların güvenliğini sağlamak için NIS2 Direktifi'nin getirdiği yükümlülöklere uyulması, tüm paydaşlar için hayati önem taşımaktadır.

Bağlanabilir araçlarda AB Siber Dayanıklılık Yasası'nın uygulama alanı da incelenmelidir. AB Siber Dayanıklılık Yasası, doğrudan veya dolaylı olarak internete veya başka bir ağı bağlı olan tüm dijital bileşenlere sahip ürünleri kapsamaktadır. Otomobiller, giderek artan bir şekilde karmaşık dijital sistemlerle donatılmakta ve bu sistemler arasında bilgi-eğlence sistemleri, GPS navigasyon sistemleri, otonom sürüş özellikleri ve güvenlik sistemleri (örneğin, otomatik frenleme ve şerit takip asistanları) yer almaktadır. Dolayısıyla, otomobiller de AB Siber Dayanıklılık Yasası'nın genel kapsamına giren dijital bileşenler içermektedir.

Ancak, otomobiller gibi karmaşık ürünler için AB Siber Dayanıklılık Yasası'nın nasıl uygulanacağı konusunda bazı istisnalar ve özel durumlar vardır:

- Otomotiv sektörü, halihazırda sıkı bir şekilde düzenlenmiş bir sektördür ve

birçok yönden halihazırda belirli güvenlik ve kalite standartlarına tabidir. Özellikle otomotiv sektörü, Birleşmiş Milletler Avrupa Ekonomik Komisyonu (UNECE) tarafından belirlenen regülasyonlara ve AB'nin Araç Tip Onayı Direktifi gibi çeşitli AB mevzuatlarına tabidir.

- Otomobil üreticilerinin yükümlülükleri bakımından AB Siber Dayanıklılık Yasası, dijital bileşenlere sahip ürünlerin üreticilerinin, ürünlerinin yaşam döngüsü boyunca siber güvenlikten sorumlu olmasını şart koşmaktadır. Bu nedenle otomobil üreticileri, sadece araçlarını piyasaya sürerken değil, araçların kullanım süresi boyunca da güvenlik güncellemelerini sağlamalı ve mevcut siber güvenlik önlemlerini ve süreçlerini değerlendirmelidir.
- AB Siber Dayanıklılık Yasası, özellikle tıbbi cihazlar, havacılık ve otomobiller gibi halihazırda düzenlenmiş ürünleri belirli durumlarda kapsam dışı bırakabilecektir¹⁰⁰. Bunun sebebi, otomobil sektörünün mevcut düzenlemeler çerçevesinde yeterli siber güvenlik önlemlerine sahip olmasıdır. Eğer mevcut düzenlemeler AB Siber Dayanıklılık Yasası'ndan daha az katıysa veya otomobil üreticileri dijital bileşenlerle ilgili belirli gereksinimlere uyum sağlayamamışsa, AB Siber Dayanıklılık Yasası'nın hükümleri geçerli olacaktır.

¹⁰⁰ **Pam Baker**, What Is the Cyber Resilience Act? Secure EU Compliance Simplified, Information Week, Nisan, 2024. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://www.informationweek.com/cyber-resilience/what-is-the-cyber-resilience-act-secure-eu-compliance-simplified#close-modal> (e.t. 30.08.2024).

İKİNCİ BÖLÜM

VERİ İŞLEME VE BAĞLANABİLİR ARAÇLAR

2.1. BAĞLANABİLİR ARAÇLAR: TANIM VE ÖZELLİKLER

Bağlanabilir araçlar, günümüzde araç sürücü tercihlerinin de etkisiyle veri işlemenin etkisinin oldukça yoğun gözlemlendiği ve gerek diğer araçlarla gerek de dış çevre ile etkileşimleri nedeniyle kendine özgü yeni veri çeşitlerinin ortaya çıktığı taşıtları ifade etmektedir. 1996 yılında General Motors, OnStar sistemiyle bağlanabilir araç özelliklerini tanıtan ilk otomobil üreticisi olmuştur. OnStar, acil durumlarda güvenliği artırmak amacıyla geliştirilen ve tıbbi yardımın sürücülere daha hızlı ulaşmasını sağlamak için acil çağrıları bir çağrı merkezi aracılığıyla yönlendiren bir sistem olarak geliştirilmiştir. 2001 yılında uzaktan teşhis teknolojisi tanıtılmıştır. 2003 yılına gelindiğinde, bağlanabilir araç teknolojisi, sürücülere araç durumu raporları ve yol tarifi gibi hizmetler sunabilecek bir seviyeye ulaşmıştır. 2007 yılında Continental, sadece veri tabanlı telematik sistemlerini tanıtmıştır. 2014 yazında Audi A3, 4G LTE Wi-Fi Hotspot erişimi sunan ilk otomobil üreticisi olurken, General Motors ise 4G LTE'nin ilk kitlesel dağıtımını gerçekleştirmiştir¹⁰¹. 2015 yılına gelindiğinde ise OnStar'ın, o tarihe kadar araç sahiplerinden / sürücülerinden gelen 1 milyar talep işlediği duyurulmuştur¹⁰².

Geçmişten günümüze gelen başlangıçta sadece kilometre bilgisi ve konum verisi toplayan bağlanabilir araçlar, son yıllarda topladıkları veri türlerini ve miktarını önemli ölçüde artırmıştır. Günümüzde birçok şirket, araç sahibi / sürücüleri ile yolcular ve yayalarla ilgili verileri işlemekte, ayrıca Google Maps gibi bağlanabilir uygulamalardan gelen verilere erişim sağlamaktadır¹⁰³.

¹⁰¹ <https://www.autoconnectedcar.com/definition-of-connected-car-what-is-the-connected-car-defined/> (e.t. 30.08.2024).

¹⁰² <https://www.autoconnectedcar.com/2015/07/onstar-celebrates-1-billion-requests-with-free-premium-service-for-loyal-users/> (e.t. 30.08.2024).

¹⁰³ **Clara Mustata**, “Connected Cars: The legislative environment, potential reform and privacy issues”, IAPP, Haziran, 2024. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://iapp.org/resources/article/connected-cars-canada/> (e.t. 30.08.2024).

Bağlanabilir araçlar, kullanıcıların araçlarıyla nasıl etkileşimde bulunduklarına ilişkin bilgilere, araç içindeki hizmetlerden, kullanılan uygulamalardan ve üçüncü taraf kaynaklardan gelen bilgilere erişmektedir. Otomobil üreticileri, bağlanabilir araçlardan elde edilen verilerin kârlılığını artırmak ve şerit kontrolü ve frenleme gibi yeni özellikleri geliştirmek adına teknoloji şirketleriyle iş birliği yapmaktadır.

Şekil 2. 1. Bağlanabilir Araç Özellikleri Gelişimi¹⁰⁴



Bağlanabilir araçlar özellikle sahip oldukları iç ve dış sensörler ve araç yazılımları ile sürekli bir veri akışına aracılık etmektedir. Toplanan bu bilgiler ile araç donanım ve sistemlerinde iyileştirmeler yapılmakta, bu yönüyle de özellikle otomotiv sektöründeki gelişmelerin en önemli kaynaklarından biri olmaktadır.

Bağlanabilir araç teknolojisi geliştikçe de gerek aracı gerek de dış çevreyi daha iyi tanıyan ve bu şekilde çok daha fonksiyonel ve kullanıcı dostu olan taşıtlar otomotiv piyasasında öne çıkmaktadır.

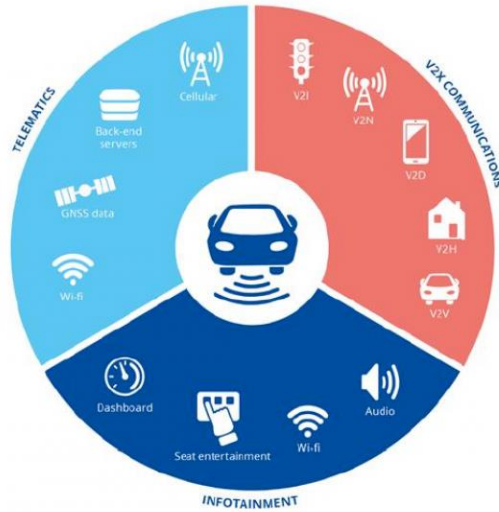
Geniş bir yelpazede özellik barındıran bağlanabilir araçlar ile sürücüler aracın iç fonksiyonları, hava ve yol durumu, aracın park durumu gibi bilgilerin yanı sıra araç kullanım şekillerine bağlı olarak işlenen sürüş verilerini de düzenli olarak takip edebilmektedir. Özellikle sürücünün araç kullanımına bağlı işlenen sürüş verileri,

¹⁰⁴ Kaynak: <https://www.autoconnectedcar.com/definition-of-connected-car-what-is-the-connected-car-defined/> (e.t. 05.08.2024)

araç sürücüsüne ait araç kullanım alışkanlıkları, yorgunluk belirtisi, ani fren ve araç sürüş hızı gibi sürücü kimliğini belirleyebilir bilgileri içerdiğinden bu veriler kişisel veri mahiyetindedir. Bu araçlar aynı zamanda araç sürücülerinin diğer akıllı cihazları ile ve üçüncü taraf uygulamalarla da eşleştiğinden yoğun bir veri paylaşımına sebep olmaktadır.

Bu bağlamda, bağlanabilir araçların kişisel veri koruma yaklaşımları açısından incelenmesi gereken bir konu olduğunu vurgulamak gerekir. Bu araçlar, sürekli ve kapsamlı bir veri setini işlediğinden, bu verilerin doğru bir şekilde işlenmesi, depolanması ve paylaşılması konularında özel bir dikkat ve düzenlenmiş yasal sınırlamalar gerekmektedir.

Şekil 2. 2. Bağlanabilir Araç Ekosistemi¹⁰⁵



¹⁰⁵ Kaynak: **ENISA**, Good Practices for Security of Smart Cars, European Union Agency for Cybersecurity, 2019. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.enisa.europa.eu/publications/smart-cars> (e.t. 30.03.2024).

2.2. BAĞLANABİLİR ARAÇ TEKNOLOJİSİNDEKİ GÜNCEL GELİŞMELER

Bağlanabilir araç teknolojisi, otomotiv sektörünün hızlı büyüyen ve gelişim gösteren alanları arasında başı çekmektedir. Bu teknolojinin en büyük getirisi bağlanabilir özelliği ile diğer araçlara ve internete bağlanarak sürüş deneyimini iyileştirmesi ve araçları daha fonksiyonel bir hale getirerek sürücülere yeni özellikler sunmasıdır.

Otomotiv endüstrisinin dijital dönüşümü, daha parlak bir gelecek için büyük vaatler sunsa da uzun yıllardır bireysel özgürlüğün simgesi olan arabalar, gizlilikle ilgili yeni tehditlere karşı giderek daha savunmasız hale gelmektedir. Akıllı telefonlardan sonra 21. yüzyılın bu araçları, insanların en sık kullandığı bağlı cihazlar arasında yer almaktadır. Bağlanabilir araçlar hizmet sağlamak veya sürüş fonksiyonlarını desteklemek amacıyla dış sistemlerle iletişim kurabilen araçlardır. Bu araçlar, sürücülere çeşitli ek özellikler sunmakta, karbon emisyonlarının azaltılmasını kolaylaştırmakta, uzaktan yapılan yazılım güncellemeleriyle yüksek onarım maliyetlerini ortadan kaldırmakta ve daha güvenli bir sürüş deneyimi sağlamaktadır. Son yıllarda, giderek daha otomatikleştirilmiş araçların piyasaya sürülmesi için dünya çapındaki yarış hız kazanmıştır. Danışmanlık firması McKinsey'e göre¹⁰⁶, 2030 yılına kadar dünya genelinde satılan yeni araçların %95'inin bağlantılı araçlar olması beklenmektedir.

Bağlanabilir araç teknolojisi incelenirken yapay zeka sistemleri ve makine öğrenimi kavramları da ele alınmalıdır. “Yapay zeka sistemleri, bireysel yaşamlarımızı, sosyal hayatı ve ekonomiyi dönüştürmektedir. Bu sistemlerin kullanımı eğitim, sağlık ve mobilite gibi çok sayıda alanda insanlık için faydalar sağlamaktadır.”¹⁰⁷ Bağlanabilir araç teknolojisindeki gelişmelere paralel olarak yapay zeka sistemleri ve makine öğrenimi teknolojilerindeki gelişmelerin de takibi

¹⁰⁶ <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data> (e.t. 18.08.2024).

¹⁰⁷ **Leyla Keser Berber, Ayça Atabey**, “Yapay Zeka Sistemlerinin Çocuk Haklarına Etkilerinin Değerlendirilme Yöntemi: Çocuk Hakları Etki Analizi”, Adalet Dergisi, Sayı: 66, 2021, s. 55.

ve bu alanlardaki güncel uygulamaların da bağlanabilir araç teknolojisini beslemesi ile araçların çeşitli sürüş ve güvenlik senaryolarına daha iyi adapte olması sağlanmaktadır. Örneğin, yapay zeka sistemlerinin sürüş alışkanlıklarını öğrenmesi ve bu kapsamda önerilerde bulunması ile araç sürücülerini için daha kişiselleştirilmiş bir sürüş deneyimi sunulacaktır. Bu sayede sürücülerin sürüş takibi yapılarak güvenli sürüş önerileri geliştirilmektedir. Yapay zeka alanındaki bu gelişmeler ile sürücünün sürüş davranışlarının tanınması ile araç sürüş destekleri kişiselleştirilerek güvenli sürüş deneyimi de arttırılacaktır. Bunun yanında, benzer güvenlik sistemleri için de yapay zekadan destek alınması olası tehlikelerin hızlı tespit edilerek kazaların önlemesine yardımcı olmaktadır.

Bir diğer önemli gelişme olarak, bağlanabilir araçlarda bulunan dış sensör teknolojilerindeki ilerlemeler, araçların çevresini algılamasında ve dolayısıyla araçların sunduğu güvenlik tedbirlerinin arttırılmasında etkin bir rol oynamaktadır. Örneğin, gelişmiş dış sensörler ile araçların çevresindeki araçları, yayaları ve diğer engelleri algılayarak bu bilgilerin sürücüye veya otonom sürüş sistemlerine iletilmesi sayesinde güvenli sürüş deneyimi sağlanarak trafik kazalarını azaltmaya yönelik önlemler artmaktadır. Araçlarda yer alan iç sensörler ile de sürücünün hareketleri izlenerek araç sürücüsüne daha iyi bir sürüş deneyimi sağlanmaktadır. Örneğin, iç sensörler ile bir sürücünün uyukladığı veya yorgunluk ve dikkat dağınıklığı belirtisi gösterdiği tespit edilerek uyarıda bulunulması, hatta gerekmesi halinde araç kontrolünün araç sürücüsünden devralınması tedbir olarak sağlanmaktadır. Yine, iç sensörler yardımı ile aracın performansı izlenerek yakıt verimliliğinin artırılması veya arızaların önceden tespiti mümkün olmaktadır. Güvenlik tedbirlerinin yanı sıra iç sensörler ile ayrıca, araç içindeki sıcaklık, ışık gibi çevresel faktörlerin algılanmasıyla araç sürüş konfor seviyesi otomatik olarak ayarlanmaktadır.

İç sensör kullanımı gibi gelişmeler otomotiv sektöründeki önemli diğer aktörlerin de bilgiyi işlemesi bakımından önemli sonuçlar doğurmaktadır. Örneğin, iç sensörler vasıtasıyla işlenen sürücü davranışları skorlanarak sigorta şirketlerine

aktarıldığında, sürücülerin sigorta primlerinin belirlenmesi ve sürüş skorlarına göre sigorta prim indirimlerinden yararlanmalarının sağlanması gibi bağlı sektörlerde ek faydalardan yararlanmaları sağlanmaktadır. Açıklanan senaryolar bakımından iç sensörler ile araç içindeki yolcuların ve sürücünün hareketlerinin, seslerinin ve belli hallerde sağlık verilerinin dahi toplanması ile iç sensörlerin veri gizliliği ve güvenliği açısından doğru şekilde tasarlanması ve kullanımı sebebiyle işlenen kişisel veriler bakımından ölçülü, şeffaf ve amaçla bağlı tasarımların en baştan doğru kurgulanması, kişisel veri mevzuat gereklilikleri bakımından oldukça önemlidir.

Bu alandaki önemli gelişmelerden bir diğeri de bağlanabilir araçlarda bulut bilişim teknolojilerinin kullanımının giderek artmasıdır. Özellikle bulut tabanlı yazılımlar ve hizmetlerin kullanımındaki bu artış, araçların sürekli olarak güncellenmesini sağlamak ve araçlara otomotiv sektöründeki yeni özelliklerin kolayca entegre edilmesine olanak tanımaktadır. Bulut tabanlı hizmetlerin kullanımındaki bir diğer avantaj ise sunduğu veri depolama çözümleri sayesinde araçların büyük veriyi güvenli bir şekilde saklamasını ve analiz etmesini sağlayarak araç sürücülerine sunulan hizmetlerin kalitesini arttırmasıdır.

2.3. BAĞLANABİLİR ARAÇLARIN KULLANIMI İLE İŞLENEN KİŞİSEL VERİLER

Bağlanabilir araçlar, dört tekerlek üstünde yer alan bilgisayar gibi çalışmakta ve düzenli olarak araç sürücüsü, yolcular ve aracın seyahat çevresinde bulunan insanların kişisel verilerini toplamakta ve bu verileri diğer araçlar, katma değerli hizmet sağlayıcı üçüncü taraflar ve yetkili kamu kurum ve kuruluşları ile paylaşmaktadır¹⁰⁸. Araç sürücüsü ve yolcular için aracın performansını iyileştirici navigasyon hizmetinin sunulması, aracın uzaktan kontrolünün sağlanması, iletişim ve eğlence hizmetlerinin sunulması faydaları sağlamak adına bağlanabilir araçlar

¹⁰⁸European Data Protection Supervisor, TechDispatch #3: Connected Cars, Aralık, 2019, (“EDPS Bağlanabilir Araç”) ilgili yazıya ulaşmak için: https://edps.europa.eu/data-protection/ourwork/publications/techdispatch/techdispatch-3-connected-cars_en (e.t. 07.04.2024).

üzerinden işlenen kişisel verilerin kapsamından ve veri işleme amaçlarının genelinden araç sürücüsü gibi ilgili kişilerin habersiz olması riski de işlenen veri boyutunun fazlalığının doğal fakat istenmeyen bir sonucu olarak ortaya çıkmaktadır.

Bağlanabilir araçlar vasıtasıyla işlenen veriler, bir gerçek kişiyi belirli veya belirlenebilir kıldığı sürece kişisel veri kabul edilmektedir. Dolayısıyla, kişisel veriler, tek başına veya diğer verilerle birlikte ele alındığında, özellikle araç seri numarası veya araç plaka numarası aracılığıyla, veri sorumlusu tarafından belirli veya belirlenebilir bir kişiyi ilişkilendirilebilen tüm verileri içermektedir¹⁰⁹. Örnek olarak, araç sürücüsünün kimliği, parmak izi gibi doğrudan ilgili kişiyi belirli kılan veriler ve araç seyahatleri, araç parçalarındaki aşınma ve yıpranma, aracın hızı, kat edilen mesafe gibi aracın hareketlerine ilişkin teknik veriler, sürüş tarzı gibi araç kullanım verileri, motor soğutma suyu sıcaklığı, motor devri, lastik basıncı gibi aracın durumuna ilişkin veriler, teknik kontrollerin tarihleri veya araç kimlik numarası gibi bilgiler veri sorumlusu, bir gerçek kişi ile ilişkilendirebildiği müddetçe kişisel veri olarak ele alınmalıdır. Bu bakımdan bağlanabilir araçlar kapsamında işlenen kişisel veriler belirlenirken bu verilerin yalnızca isim, soy isim, adres gibi bilgiler olmadığı göz önünde bulundurulmalıdır.

Bağlanabilir araçlar kapsamında veri işleme faaliyetleri değerlendirildiğinde, işlenen kişisel veriler CNIL tarafından¹¹⁰ aşağıdaki gibi sıralanmıştır:

- Araç sahibi/sürücüsü verileri (ad, soyad, adresi, e-posta adresi, telefon numarası, vb.).
- Araç kimlik numarası veya araca ait diğer bilgiler (araç plaka numarası vb.).

¹⁰⁹ CNIL, Connected vehicles: a compliance package for a responsible use of data, Ekim, 2017, ("CNIL Rehberi") s. 5. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data> (E.t. 17.03.2024).

¹¹⁰ CNIL Rehberi, s. 6.

- Araç sürücüsünün biyometrik verileri.
- Coğrafi konum verileri.
- Araç sürücüsü veya yolcuları hakkında aracın kullanımından kaynaklı veriler (sürüş tarzı, koltukta oluşan ağırlık, araçtaki seyahat süresi vb.).
- Aracın ve parçalarının durumuna ilişkin teknik veriler.

EDPB de yayımladığı Bağlanabilir Araçlar Kapsamında Kişisel Verilerin İşlenmesine İlişkin Rehber’de (“Rehber”)¹¹¹ bağlanabilir araçlar kapsamında işlenen kişisel verilere ilişkin detaylı bir analize yer vermiş ve araç üreticileri, katma değerli hizmet sağlayıcılar gibi veri sorumlularınca yürütülen faaliyetlerde işlenirken dikkat edilmesi gereken üç kişisel veri kategorisi belirlemiştir. İlgili veri kategorileri; konum verileri, biyometrik veriler ve cezai suçları veya diğer ihlalleri ortaya çıkaran verilerdir. EDPB yaptığı bu belirlemede yalnızca biyometrik veri ile sınırlı kalmayarak GDPR’ın 9. maddesi¹¹² kapsamında sayılan diğer özel nitelikli kişisel verilerin de işlenirken özen gösterilmesi gerektiğini vurgulamaktadır.

Aynı maddede özel nitelikli kişisel verilerin işlenmesinde dayanan hukuki sebepler de sayılmaktadır. “Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun” ile KVKK’nın “Özel nitelikli kişisel verilerin işlenme şartları” başlıklı 6. maddesindeki yeni düzenleme sonrası özel nitelikli kişisel verilerin işlenmesi hukuki sebepleri GDPR’daki düzenlemeye yaklaşmıştır. Nitekim, eski hali ile KVKK’nın 6. maddesindeki düzenleme uyarınca sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin işlenebilmesi, sadece ilgili kişinin açık rızasının bulunması veya kanunlarda öngörülmesi halinde

¹¹¹ **Avrupa Veri Koruma Kurulu**, Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Mart, 2021, s. 15 (“Rehber”). İlgili rehber internet üzerinden şu link ile ulaşılabilir: https://www.edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf (e.t. 10.03.2024).

¹¹² GDPR’ın “Processing of special categories of personal data” başlıklı 9/1 maddesi kapsamında özel nitelikli kişisel veriler şu şekilde sayılmıştır: “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”.

mümkündü. Sağlık verileri ve cinsel hayata ilişkin veriler ise açık rıza ile veya sadece kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetlerinin finansmanı, yönetimi ve planlanması hukuki sebeplerine dayanılarak işlenmekteydi. Yapılan değişiklik ile özel nitelikli kişisel verilerin işlenme şartları, GDPR'daki düzenleme ve güncel ihtiyaçlar göz önünde bulundurularak düzenlenmiştir. Maddenin ikinci fıkrasında özel nitelikli kişisel verilerin işlenmesinin yasak olduğu hükmü korunarak özel nitelikli kişisel verilerin işlenebileceği hukuki sebepler sayılmaktadır¹¹³.

KVKK'da yapılan değişiklik sonrası özel nitelikli kişisel verilerin işlenmesi; “ilgili kişinin açık rızasının olması, kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, ilgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması, bir hakkın tesisi, kullanılması veya korunması için zorunlu olması, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması, istihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması, siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması”¹¹⁴ halinde mümkün olacaktır.

¹¹³ **Mehmet Bedii Kaya**, KVKK Reformu: 2024 Değişiklikleri (Dijital Baskı 1.0), 2024, s.10. İnternet üzerinden şu link ile ulaşılabilir: <https://mbkaya.com/hukuk/kvkk-reformu.pdf> (e.t. 23.05.2024).

¹¹⁴ KVKK'nın 6/3. maddesi.

Verilerin türü ve toplama yöntemleri göz önüne alındığında, bağlanabilir araçlarda işlenen kişisel veriler iki temel kategoriye ayrılarak inceleme yapılmaktadır:

- Araç sahibi / sürücüsü işlem verileri; kimliği belirleyici bilgiler, iletişim bilgileri, ödeme bilgileri vb.
- Kullanım verileri; araç tarafından üretilen kişisel veriler, sürüş alışkanlıkları, konum verileri vb.

EDPB Rehber’de¹¹⁵ ayrıca araç sürücüsü, yolcular, araç sahipleri ve aracın seyahat çevresinde bulunan ilgili kişilerin bağlanabilir araçlar vasıtasıyla işlenen kişisel verilerinin toplanma yöntemlerini de aşağıdaki şekilde sıralamaktadır:

- Araç içinde işlenen veriler (araç sensörleri, telematik kutuları vasıtasıyla toplanan veriler vb.).
- Araç ile ona bağlı kişisel cihazlar arasında aktarılan veriler (kullanıcının akıllı telefonu ile bağlanabilir araç arasındaki veri akışı vb.).
- Araç içinde toplanıp daha sonra işlenmek üzere dış birimlere aktarılan veriler (araç üreticileri, altyapı yöneticileri, sigorta şirketleri, araç tamircileri vb. aktarım tarafları).

Bağlanabilir araçlarda işlenen kişisel veriler göz önünde tutulduğunda, özellikle araç sürücüsünün sürüş ve kullanım davranışlarının ham veri olarak üçüncü taraflarla paylaşılmasının, sürücü profili oluşturulması gibi farklı sonuçları doğmaktadır. Bu bakımdan, telematik kutusu aracılığıyla toplanan sürüş davranışına ilişkin ham verilerin ya aracın içinde telematik kutularında ya da sürücünün akıllı telefonunda işlenerek üçüncü taraflarla amaca uygun şekilde paylaşılması ile ayrıntılı ham verilerden ziyade, yalnızca sonuç verilerinin paylaşılması gibi ek kontrollerle sürücü profilinin oluşturulmasının önüne

¹¹⁵ Rehber, s. 8.

geçilmektedir. Örneğin, sigorta şirketleri ile ham verinin paylaşılması yerine sürüş alışkanlıklarına ilişkin bir puanın paylaşılması halinde veri minimizasyonu ilkesi de gözetilerek sigorta şirketleri sadece sürücü puanlarını ve toplam kilometreyi almakta, bu puanları üretmek için kullanılan ham verileri görüntülememektedir.

2.3.1. Konum Verisi

Bağlanabilir araçlarda işlenen kişisel veriler dikkate alındığında, EDPB Rehber’de otomotiv sektör üreticileri, katma değerli hizmet sağlayıcıları gibi veri sorumlusu taraflarca işlenirken özellikle dikkat edilmesi gereken verileri üç kategori olarak sıralamaktadır; konum verileri, biyometrik veriler ve cezai suçları veya diğer ihlalleri ortaya çıkaran veriler.

Veri sorumluları bağlanabilir araç üzerinden konum verisini toplarken bu verinin özellikle ilgili kişilerin yaşam alışkanlıklarını ortaya koyduğunu göz önünde tutmalıdır. Gerçekleştirilen yolculuklar araç sürücüsü ve yolcuları gibi ilgili kişilerin özel hayatlarına yönelik pek çok bilgi sağlamakta olup bu yönüyle doğrudan özel hayata dokunmaktadır. Konum verisi ile bir sürücünün iş ve ikamet yerinin yanı sıra boş zamanlarında vakit geçirdiği yerlerin bilinmesi ile ilgi alanlarına ilişkin çıkarımlarda bulunulması sağlanmaktadır. Ayrıca ibadet yeri aracılığıyla dini inanç bilgisine de ulaşılması mümkündür. Öyle ki, ilgili kişilerin ziyaret ettiği yerler aracılığıyla cinsel yönelimi gibi hassas bilgileri dahi açığa çıkabilmektedir. Bu nedenle, otomotiv sektör üreticileri, katma değerli hizmet sağlayıcıları gibi veri sorumluları, işleme amacı için kesinlikle gerekli olmadığı sürece konum verilerini toplamamak adına gerekli özeni göstermelidir. Örneğin, veri işleme faaliyeti bağlanabilir aracın hareketinin tespit edilmesinden ibaret olduğunda, konum verisinin toplanmasına gerek olmaksızın bu işlevi yerine getirmek için kilometre sensörü aracılığıyla toplanan verilerin işlenmesi yeterli olmaktadır.

Konum verisi, ařağıdaki hususlara uygun řekilde iřlenmelidir¹¹⁶:

- Konum verisi yalnızca iřleme amacına ve veri minimizasyonu ilkesine uygun olarak iřlenmelidir. Ayrıca iřlenen konum verilerine ne sıklıkta eriřileceğı de belirlenmelidir. Örneğın, bir hava durumu uygulaması, ilgili kiřinin rızası olsa dahi, aracın konumuna her saniye eriřmemelidir.
- İlgili kiřinin konum verisinin iřlenme amacı, konum gemiřinin saklanıp saklanmadığı, saklanıyorsa ne sürede saklandığı gibi iřleme faaliyetinden doğrudan etkilenen hususlar hakkında řeffaf řekilde bilgilendirilmesi saėlanmalıdır. Bunun için baėlanabilir araç içi ekranı gibi konum verisi iřlenen ilgili kiřilerin kolayca eriřebileceğı ortamlardan faydalanılmalıdır.
- Konum verisi hassas bilgiler arasında sayıldığından veri iřleme hukuki sebebinde açık rızanın temin edilmesine dayanıldığında, baėlanabilir araç içi ekranında genel satıř veya kullanım kořullarından farklı olarak konum verisinin iřlenmesine iliřkin bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızanın temini gerekmektedir.
- Özellikle simgeler kullanarak, örneğın baėlanabilir araç ekranında yer verilen bir sembol vasıtasıyla araç konumunun etkinleřtirildiğı konusunda araç sürücüsü ve yolcular bilgilendirilmelidir.
- Konum verisi, araç alıřtırıldığında varsayılan ve sürekli olarak deėil, yalnızca araç sahibi / sürücüsü aracın konumunun bilinmesini gerektiren bir iřlevi bařlattığında etkinleřtirilmelidir.
- Ara sahibine / sürücüsüne konum verisini herhangi bir zamanda devre dıřı bırakma seeneğı sunulmalıdır. Ayrıca, konum verisinin devre dıřı kaldığına iliřkin olarak baėlanabilir araç ekranında da bilgilendirme yapılmalıdır.

¹¹⁶ Rehber, s. 16.

- İşlenen konum verisi geçmişine ilişkin sınırlı ve belirli bir saklama süresi tanımlanmalıdır.

2.3.2. Biyometrik Veri

Biyometrik veriler bağlanabilir araçlar kapsamında KVKK'nın 6. maddesi ve GDPR'ın 9. maddesinde yer alan özel nitelikli kişisel veri işleme şartları dikkate alınarak, ilgili kişiyi belirli ve belirlenebilir kılacak şekilde aracın kullanımına izin vermek, araç sahibinin / sürücüsünün kimliğini doğrulamak, araç sürücüsünün profil ayarlarına ve araç tercihlerine erişimine izin vermek gibi amaçlar kapsamında işlenmektedir. Biyometrik veri bazlı sistemlerin kullanılması halinde, veri işlemenin KVKK'da düzenlenen hukuki sebeplere dayandırılması gerekliliği Kurul kararlarında vurgulanmaktadır¹¹⁷. Biyometrik verilerin kullanımını değerlendirirken, ilgili kişilerin işlenen verileri üzerinde tam kontrolünün sağlanmasını garanti etmek, ayrıca sunulan hizmete yönelik bir kısıtlama olmadan biyometrik verinin alternatifi olacak bir yöntemin, örneğin, parmak izi ile aracın açılmasına alternatif olarak fiziksel anahtar veya kod kullanımının sağlanması kontrolü gerekmektedir. İlgili kişinin kimliğini doğrulamak için kullanılan parmak izi veya yüz tanıma verileri gibi biyometrik verilerin işlenmesinde alınacak güvenlik tedbirleri bakımından ilgili verilerin şifrelenmesi, bu verilerin yetkisiz erişime karşı korunmasını sağlamaktadır. Ayrıca biyometrik verilerin, araç içinde veya başka bir yerel cihazda depolanması ile dışarıdan erişilemez şekilde saklanması sağlamaktadır. Bu şekilde biyometrik veriler, harici bir okuma / karşılaştırma terminali tarafından işlenmemesi ve verilerin bulutta veya başka bir uzak konumda depolanmaması yoluyla korunmaktadır. Bu yaklaşım, veri güvenliğini artırarak ilgili kişilerin verileri üzerinde daha fazla kontrol sahibi olmalarını sağlamaktadır.

¹¹⁷ **Kişisel Verileri Koruma Kurulu**, "İlgili kişinin 'el geometrisi' bilgisinin bir işletmenin hizmet binasına giriş yapabilmek amacıyla veri sorumlusu tarafından açık rıza alınmaksızın işlenmesi" hakkında kararı, T: 07/07/2022, K: 2022/662. İlgili karara internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/Icerik/7399/2022-662> (e.t. 20.05.2024).

Biyometrik verilere ilişkin kimlik doğrulama çözümünün yeterince güvenilir olması kritik öneme sahiptir. Bu güvenilirliği sağlamak için belli kontrollerin yapılması gerekmektedir¹¹⁸:

- Biyometrik veriler işlenirken kullanılan çözüm, gereken erişim kontrolünün güvenlik seviyesine uygun olacak şekilde yanlış kabul ve red oranlarını düşürmelidir. Örneğin, yüksek güvenlik gerektiren bir işlem için düşük hata oranına sahip bir çözüm tercih edilmelidir.
- Bağlanabilir araçlarda kullanılan sensörlerin saldırılara karşı dayanıklı olması gerekmektedir. Örneğin, parmak izi tanımada düz bir baskının kullanılması gibi sahtecilik yöntemlerine karşı koyabilen sensörler tercih edilmelidir.
- Biyometrik veriler kullanılarak yapılan kimlik doğrulama denemelerinin sayısı sınırlandırılmalıdır. Bu durum yetkisiz kişilerin birden fazla denemeyle sisteme girme riskini azaltmaktadır.
- Biyometrik verilere ilişkin şablon / model, bağlanabilir araç içerisinde en son teknolojiye uygun kriptografik algoritmalar ve anahtar yönetimi kullanılarak şifreli bir şekilde saklanmalıdır.
- Biyometrik verilere ilişkin oluşturulan şablon / modelleri oluşturmak ve araç sahibi / sürücüsü kimlik doğrulaması için kullanılan ham veriler, yerel olarak dahi saklanmayacak şekilde, gerçek zamanlı olarak işlenmelidir.

Bu ilkeler, biyometrik verilerin güvenliğini ve kullanıcıların verileri üzerindeki kontrolünü artırmaktadır. Araç üreticilerinin ve katma değerli hizmet sağlayıcıların, KVKK ve GDPR gibi veri koruma mevzuatları ile uyumlu güvenilir biyometrik kimlik doğrulama çözümleri kullanmaları önemlidir.

¹¹⁸ Rehber, s. 17.

Örneğin, bağlanabilir araçlardaki sanal sesli asistanlar¹¹⁹, ses tanıma teknolojisi sayesinde kullanıcıları seslerine göre ayırt edebilmektedir. Bu işlem, bir "ses modeli" oluşturarak kullanıcının kimliğini doğrulamayı sağlayan "ses modeli tanıma" olarak adlandırılmaktadır. Ses modelinin oluşturulması ve kullanılması sırasında işlenen ses verileri, bir kişinin kimliğini benzersiz bir şekilde tanımlayacağı için biyometrik veri olarak kabul edilmektedir. Bu nedenle, sesli asistanın kullanımı için ilgili kişilerin açık rızasının alınması değerlendirilmelidir. Rızanın geçerli olması için ise kullanıcılara biyometrik verilerinin işlenmesi dışında alternatif bir kimlik doğrulama yöntemi sunulmalı ve rızanın özgürce verildiğinden emin olunmalıdır.

Veri güvenliği açısından, sesli asistanların ses kayıtlarını nerede depoladıkları, bu modellere kimlerin erişebildiği ve bu verilerin diğer cihazlara aktarılıp aktarılmadığı gibi konular şeffaf bir şekilde ilgili kişilere açıklanmalıdır.

Bununla beraber, ses tanıma teknolojisinin yalnızca kayıtlı araç sahibi / sürücüsü gibi ilgili kişilerin sesini algılamakla kalmayıp, aynı ortamda bulunan diğer kişilerin seslerini de işlediği dikkate alınmalıdır. Bu durum, haberleri olmadan kişilerin biyometrik verilerinin işlenmesine yol açmaktadır. Bu tür durumları önlemek için, ses tanıma özelliğinin sadece araç sahibi / sürücüsü gibi ilgili kişilerin inisiyatifiyle aktif hale gelmesi ve sürekli olarak ortam seslerini dinlememesi tercih edilmelidir. Örneğin, biyometrik doğrulamayı başlatmak için ilgili kişi önceden belirlenmiş bir anahtar kelime söyleyebilmeli veya asistan kimlik doğrulaması yapıp yapmayacağını sorarak kullanıcının onayını almalıdır¹²⁰.

2.3.3. Cezai Suçları veya Diğer İhlalleri Ortaya Çıkaran Veriler

Bağlanabilir araçlar, suçların veya diğer ihlallerin tespitinde kullanılabilecek özel nitelikli kişisel veriler toplayabilmektedir. Suçla ilgili verilerin farklı

¹¹⁹ Virtual voice assistant.

¹²⁰ **European Commission**, Guidelines 02/2021 on virtual voice assistants, Version 2.0, Temmuz, 2021, İlgili metne internet üzerinden şu link ile ulaşılabilir: https://www.edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf (e.t. 20.04.2024).

kaynaklardan birleştirilmesi, ilgili kişilerle ilgili daha geniş bir profil oluşmasına yol açmaktadır. Anlık hız, konum bilgileri gibi veriler farklı amaçlar için işlendiğinde ve başka veriler ile değerlendirilmediğinde bir ihlalin tespiti mümkün olmayacakken bu verinin toplanma amacı ve bağlamı, onu suçla ilişkili bir veri haline getirebilmektedir. Örneğin, belirli bir bölgede yüksek hızda seyreden bir aracın konum bilgisi, yetkililer tarafından bir trafik ihlali veya daha ciddi bir suçun soruşturmak için kullanılabilir. Bu bakımdan kişisel verilerin potansiyel olarak suçla ilgili veriler olarak kabul edilebileceği işleme sebeplerinin dikkatli bir şekilde değerlendirilmesi ve bu tür verilerin işlenmesinde ölçülülük ve veri minimizasyonu ilkelerine uyulması gerekmektedir.

Bağlanabilir araçlarda suçla ilgili verilerin toplanması ve işlenmesi, veri koruma ve siber güvenlik standartlarına uygun şekilde yapılmalıdır. Yetkisiz erişim, veri sızıntısı veya kötüye kullanımı önlemek için gerekli teknik ve idari tedbirlerin alınması gerekmektedir. Bu hassasiyet göz önüne alındığında EDPB, suçla ilgili verilerin yerel olarak işlenmesini önermektedir. Yerel veri işleme, araç üreticileri ve katma değerli hizmet sağlayıcılar gibi veri sorumlularının mümkün oldukça kişisel verileri kullanmadan veya kişisel verileri araç dışına çıkarmadan, bağlanabilir araçta işlemleri anlamına gelmektedir. Yerel veri işlemede, verisi işlenen ilgili kişiler, kişisel verilerinin işlenmesi üzerinde tam kontrole sahiptir. Bu sayede, ilgili kişilerin özel hayatlarına ve temel haklarına saygı gösterilirken, aynı zamanda yetkili kamu kurum ve kuruluşlarının sağlayacağı cezai incelemelerde gerekli bilgiye erişimi mümkün kılınmaktadır.

Yerel veri işlemenin yanı sıra, suçla ilgili verilerin işlenmesinde aşağıdaki ek kriterlerin de göz önünde bulundurulması ve kontrolü önemlidir:

- Verilerin toplanması ve işlenmesi için hukuki sebebin bulunması gerekmektedir. İlgili hukuki sebep kanunlarda açıkça öngörülmesi, hukuki yükümlülüğün yerine getirilmesi veya ilgili kişinin açık rızasının temini olabilecektir.

- Kişisel veriler veri minimizasyonu ilkesi uyarınca sadece sınırlı ve ölçülü olarak toplanmalı ve işlenmelidir. Bu şekilde, yapılan cezai inceleme için gereken minimum veri miktarının toplanması ve işlenmesi temin edilmelidir.
- Uygun teknik tedbirler alınarak veriler güvenli bir şekilde saklanmalı ve yetkisiz erişime karşı korunmalıdır. Bu tedbirler arasında güçlü şifreleme ve yetki erişimlerinin düzenli kontrolü gibi güvenlik önlemleri yer almaktadır. Bu şekilde verilerin yalnızca yetkili kişiler tarafından ve sınırlı amaçlarla erişilebilir olması sağlanmaktadır.
- Kişisel verilerin işleme sebebinin ortadan kalkmasını veya yasal bir yükümlülüğün gerektirdiği sürenin sona ermesini takiben verilerin imha edilmesi gerekmektedir.

Bağlanabilir araçlardan elde edilen suçla ilgili verilerin işlenmesi, veri koruma mevzuatları ve kamu güvenliğinin temini arasında hassas bir denge kurmayı gerektirmektedir. Yukarıda belirtilen kriterlere uymak, bu dengeyi gözeterek ilgili kişilerin haklarını korumayı ve yetkili kamu kurum ve kuruluşlarının sağlayacağı cezai incelemeleri sağlamayı mümkün kılmaktadır.

2.4. BAĞLANABİLİR ARAÇLARIN KULLANIMI İLE İŞLENEN KİŞİSEL VERİLERİN İŞLEME AMAÇLARI

Bağlanabilir araçlarda kişisel veriler, araç sürücüsü güvenliği, sigorta, verimli ulaşım ve kullanım rahatlığı, eğlence gibi katma değerli hizmetlerin sunulması da dahil olmak üzere çeşitli amaçlarla işlenmektedir. KVKK uyarınca veri sorumluları, veri işleme amaçlarının "belirli, açık ve meşru" olmasını, işleme faaliyetinin bu amaçlarla bağlantılı, sınırlı ve ölçülü olmasını ve KVKK'nın 5. ve 6. maddelerinde belirtilen işleme için geçerli bir hukuki sebebin varlığını sağlamalıdır.

Bağlanabilir araçlar genellikle araç sahibine / sürücüsüne hizmet sağlanması için gerekli olan kişisel verileri işlemektedir. Bu hizmetlerden bazıları temel hizmetler olup, araç sahipleri veya sürücüler, bağlanabilir aracın sistemlerinin düzgün

çalışması için belirli kişisel verileri sağlamalıdır. Temel hizmetler dışında kalan diğer hizmetler, özellikle araç sahibi veya sürücüsü tarafından talep edilen ve bağlanabilir aracın sistemlerinin çalışması için gerekli olmayan isteğe bağlı ek hizmetler olarak ele alınmaktadır. Bazı bağlanabilir araç üreticileri ve katma değerli hizmet sağlayıcılar, hedefli reklamlar sunmak ve makine öğrenimi algoritmalarını eğitmek gibi kendi amaçları için de kişisel veri toplayabilmekte olup, özellikle bu amaçlarla yürütülen veri işleme faaliyetlerinde dayanan hukuki sebebin titizlikle tespiti oldukça önemli olmaktadır.

Kişisel verilerin işlenmesinden önce, araç sahibi, sürücü veya yolcular gibi ilgili kişilerin araç ve ekipman üreticisi veya katma değerli hizmet sağlayıcısı gibi veri sorumluları tarafından işlenen kişisel verileri ve veri işleme faaliyetleri kapsamında bilgilendirilmesi gerekmektedir. Yapılacak bilgilendirmede KVKK'nın 10. maddesinde ve GDPR'ın 13. ve 14. maddelerinde veri sorumlularının aydınlatma yükümlülüğünü yerine getirmelerini sağlamak adına gereken bilgiler ilgili kişilere sunulmalıdır.

Bağlanabilir araçlar, içinde yer alan elektronik kontrol üniteleri ve sensörler ile donatılmış araçlar olup, aracın hem içindeki hem de dışındaki diğer cihazlarla bilgi paylaşmasına olanak tanımaktadır. Bağlanabilir araçların veri alışverişine elvermesi de bu araçlar vasıtasıyla işlenen kişisel verilerin pek çok amaçla işlenebilmesine olanak sağlamaktadır. Bağlanabilir araçlar vasıtasıyla karşılaşılan uygulamalar ve sundukları hizmetler bakımından, aşağıdaki yedi temel uygulama kategorisi sıralanmaktadır¹²¹:

- Mobilite yönetimi: Gelişmiş navigasyon sistemleri, potansiyel olarak tehlikeli çevre koşulları (örneğin buzlu yollar), optimize edilmiş yakıt tüketimi veya yol fiyatlandırması hakkında zamanında bilgi sağlayarak sürücülerin bir varış noktasına hızlı ve uygun maliyetli bir şekilde ulaşmasına olanak tanıyan

¹²¹ **European Commission**, Public support measures for connected and automated driving final report, Temmuz, 2017, İlgili metne internet üzerinden şu link ile ulaşılabilir: <https://op.europa.eu/en/publication-detail/-/publication/0f3e5c98-66ad-11e7-b2f2-01aa75ed71a1/language-en> (e.t. 13.04.2024)

geliştirmeler.

- Araç yönetimi: Araç durumu ve servis hatırlatıcıları, kullanım verilerinin aktarımı, yakıt yönetimi ve bakım bilgileri, uzaktan çalıştırma (örneğin ısıtma sistemi) veya profil yapılandırmaları (örneğin koltuk konumu).
- Eğlence: Gömülü WLAN bağlantı noktaları, müzik/video akışı, sosyal medya entegrasyonu gibi sürücüye ve yolculara bilgi sağlayan ve eğlenceyi içeren işlevler, akıllı telefon arayüzleri (örneğin eller serbest telefon görüşmeleri, sesle oluşturulan metin mesajları).
- Yol güvenliği: Trafik sıkışıklığı veya olumsuz hava koşulları için uyarı sistemleri, çarpışma koruması, tehlike uyarıları, şeritten ayrılma uyarıları, eCall¹²² veya çarpışma inceleme olay veri kaydedicisi gibi sürücüyü harici tehlikeler ve dahili tepkiler konusunda uyaran işlevler ve yol yardımı hizmeti.
- Otonom sürüş: Yoğun trafikte sürücü yardımı veya oto pilot, şeritten ayrılma uyarı sistemleri, otomatik park sistemleri ve uyarlanabilir hız sabitleyici.
- Sağlık: Yorgunluk tespit sistemleri ve tıbbi yardım için uyarılar gibi sürücünün konforunu, sürüş kabiliyetini ve zindeliğini izleyen işlevler.
- Ev entegrasyonu: Mobil ofis veya akıllı ev hizmetleri gibi sürücüye ve yolculara bilgi sağlayan işlevler.

¹²² eCall sistemi, araçlarda acil durumlarda otomatik veya manuel olarak devreye giren ve 112 Acil Çağrı Merkezine bağlantı sağlayarak kazazedelere yardım ulaşmasını hızlandıran bir araç içi acil çağrı sistemidir. Ana Özellikleri: otomatik veya manuel aktivasyon, GPS ile konum tespiti ve kazanın şiddetini sensörler aracılığıyla tahmin etme gibi özellikleri mevcuttur. Avrupa Birliği'nde 2015/718 sayılı Araç İçi 112 Çağrı Sistemlerine İlişkin Tip Onayına Dair Regülasyon ile 31 Mart 2018'den itibaren AB ülkelerinde üretilen tüm yeni araçlarda eCall sistemi bulunması zorunlu hale getirilmiştir. 19 Ağustos 2016 tarihinde Bilim, Sanayi ve Teknoloji Bakanlığı, 2015/758 sayılı AB Regülasyonuna uyum sağlamak amacıyla "112 Acil Çağrı Servisi Tabanlı Araç İçi Acil Çağrı Sisteminin Yerleştirilmesi ile İlgili Tip Onayı Yönetmeliği"ni yayımladı. Yönetmelik, 31 Mart 2018 tarihinde yürürlüğe girerek eCall sisteminin Türkiye'de de zorunlu hale gelmesini sağladı. Bu yönetmelik, araç üreticilerinin 112 Tabanlı Araç İçi Acil Çağrı Sistemleri konusunda uymaları gereken yükümlülükleri ve yetkilendirme prosedürlerini detaylı bir şekilde ele almaktadır.

Yukarıda sıralanan kategorileri dikkate alındığında ve otomotiv sektöründe yer alan veri sorumlularının aydınlatma metinleri incelendiğinde¹²³ bağlanabilir araçlardaki veri işleme faaliyetleri kapsamındaki önemli temel ve ek veri işleme amaçlarını aşağıdaki şekilde sıralamak mümkündür:

- Bağlantılı hizmetlerin sağlanması: Bağlanabilir araçlar üzerinden sürücülere navigasyon ve uzaktan araç kilitleme / açma gibi çeşitli bağlantılı hizmetlerin sunulması ve bu hizmetlerin düzgün ve güvenli bir şekilde sürdürülmesi amaçlarıyla VIN, araç donanım modeli ve sistem durumu, parça numaraları ve kilometre sayacı gibi veriler işlenmektedir.
- Araç performans sorunlarının anlaşılması ve giderilmesi: Araç performansı verileri, arızaları önceden tahmin etmek, garanti kapsamındaki onarımları kolaylaştırmak ve genel araç kalitesini iyileştirmek amaçlarıyla işlenmektedir.
- Uzaktan problem tespiti yapılması: Araçtaki sensörler aracılığıyla potansiyel sorunların uzaktan tespit edilmesi ve araç sahibi ve sürücülerine bakım önerileri sunulması amaçlarıyla aracın performansı ile ilgili veriler işlenmektedir.
- Ürün araştırma ve geliştirme faaliyetlerinin yürütülmesi: Bağlanabilir araçlardan gelen kişisel veriler, yeni ürün ve hizmetlerin geliştirilmesine, mevcut ürünlerin iyileştirilmesine ve araç sürücüsünün gereksinimlerinin daha iyi anlaşılmasına katkı sağlanması amaçlarıyla işlenmektedir.
- Kişiselleştirilmiş ürün ve hizmetler sunulması: Veriler, araç sahibi veya sürücülerinin ilgi alanlarına ve kullanım alışkanlıklarına göre kişiselleştirilmiş

¹²³ Bağlanabilir araç hizmeti sunan veri sorumlularının incelenen aydınlatma metinlerine internet üzerinden şu linkler ile ulaşılabilir: <https://www.volvocars.com.cn/en-cn/legal/privacy/privacy-car2#167ea0396a05a393c0a80065655a9f16>; <https://www.ford.com.tr/sartlar-ve-kisisel-verilerin-korunmasi/baglantili-araclar-aydinlatma-metni>; https://login.bmwusa.com/pm2/pm-document-service/api/v1link/documents/policyName/BMW_CONNECTED_DRIVE_DPP/CA/PDF?language=en&KeyId=dbf0a542-ebd1-4ff0-a9a7-55172fbfce35#:~:text=We%20may%20use%20the%20information,is%20anonymized%20and%20not%20identifiable.&text=•,Partners.,with%20our%20approved%20BMW%20partners. (E.t. 18.05.2024).

ürün ve hizmetler sunulması amaçlarıyla işlenmektedir.

- Bağlanabilir aracın haberleşmesinin doğrulanması: Araç bağlantı sorunlarını tespit etmek ve veri aktarımının güvenliğini sağlamak amaçlarıyla SIM numarası ve modem elektronik seri numarasını tanımlayan bilgiler gibi veriler işlenmektedir.
- Yazılım güncellemelerinin sağlanması: Bağlanabilir araç yazılımını güncel tutmak, siber güvenlik açıklarını kapatmak ve araç için en son özellikleri sunmak amaçlarıyla bağlanabilir aracın güncel yazılım ve diğer araç modüllerinin yazılım bilgileri işlenmektedir.
- Müşteri hizmetleri desteği sunulması ve hizmet kalitesinin değerlendirilmesi: Ürün ve hizmetlere ilişkin müşteri hizmetleri desteği sunulması ve kullanıcı memnuniyetinin artırılması ile sunulan hizmetlerin ve tedarikçilerin performansının ölçülmesi amaçlarıyla işlenmektedir.
- Pazar analizinin yapılması: Sektör trendlerini anlamak ve yeni pazar fırsatları belirlemek amacıyla araç sahibi / sürücüsü işlem verileri işlenmektedir.
- Profilleme yapılması ve kişiselleştirilmiş pazarlama faaliyetlerinin yürütülmesi: Pazarlama kampanyalarının yürütülmesi ve araç sahibi ve sürücülerine ilgi alanlarına uygun ürün ve hizmetler hakkında bilgi verilmesi amaçlarıyla araç sahibi / sürücüsü işlem verileri işlenmektedir. Bağlanabilir araçlar aracılığıyla toplanan veriler veri sorumluları tarafından kişileri veya nesneleri tanımlamak amacıyla veri tabanlarında halihazırda depolanan verilerle ilişkilendirilerek araç sahiplerini / sürücülerini kullandıkları bağlanabilir araçlara ve adreslerine göre takip edip tanımlayarak hedefli reklamcılık faaliyeti yürütebilmektedir¹²⁴.

¹²⁴ **Florin Costinel Dima**, Drone technology and human rights, University of Twente, Temmuz, 2017, s. 27. İlgili metne internet üzerinden şu link ile ulaşılabilir: https://essay.utwente.nl/73105/1/DIMA_BA_EPA.pdf (e.t. 18.05.2024).

- eCall işlevinin sağlanması: Araç sürücüsü ve yolcuların güvenliğinin sağlanması, bir kazadan sonra kurtarma önlemlerinin uygun ve daha hızlı bir şekilde başlatılması, araç içindeki bir veya daha fazla sensörün etkinleştirilmesiyle tespit edilen ciddi bir kaza durumunda acil durum çağrısı işlevinin etkinleştirilmesi amaçlarıyla araç kimlik numarası, aracın hareket yönü, araç model özellikleri, araçtaki yolcu sayısı, araç hızı, olayın gerçekleştiği zaman ve olayın olduğu yer gibi kişisel veriler işlenmektedir.
- Talep ve şikayetlerin yönetilmesi: Araç sahibi / sürücüsü geri bildirimlerini toplamak ve sorunları çözmek amaçlarıyla araç sahibi / sürücüsü işlem verileri ve araç kullanım verileri işlenmektedir.
- Yasal yükümlülöklere uyulması: Bağlanabilir aracın veri işleme faaliyetini gerçekleştirdiği ölkelerdeki kişisel veri koruma yasaları ve diğör yasal gereksinimlere uyulması ve güvenlik operasyon hizmetlerinin ve yönetiminin sağlanması amaçlarıyla araç sahibi / sürücüsü işlem verileri ve araç kullanım verileri işlenmektedir.

Bağlanabilir araçlarda kişisel veri işlemenin birden çok amacı olması yanı sıra veri işleme faaliyetleri araç üreticileri ve katma değeri hizmet sağlayıcılar gibi veri sorumlularının sundukları ürün ve hizmetlerin geliştirilmesi adına da birçok fayda sağlamaktadır. Ancak, ilgili kişilerin özel hayatlarının gizliliğini ve güvenliğini korumak için veri işleme amaçlarının açık ve şeffaf bir şekilde belirlenmesi ve veri işleme faaliyetlerinin kişisel veri koruma mevzuat gereksinimlerine uygun şekilde yapılması gerekmektedir.

2.5. BAĞLANABİLİR ARAÇLARIN KULLANIMI İLE KİŞİSEL VERİLERİN TOPLANMA YÖNTEMLERİ VE VERİ İŞLEMENİN HUKUKİ SEBEPLERİ

Bağlanabilir araçlarda kişisel verilerin toplanması, sıralanan üç ana yöntemle mümkün olmaktadır:

- Baęlanabilir araç ekranları ve baęlanabilir araç mobil uygulaması vasıtasıyla araç sahibi / sürücüsü tarafından doğrudan veri girişı yapılması: Baęlanabilir araç sahipleri / sürücöleri, araç içi ekranlar veya mobil uygulamalar aracılığıyla isim, adres, telefon numarası, e-posta adresi, seyahat rotasına ilişkin konum bilgisi gibi kişisel bilgileri manuel olarak girebilmektedir. Baęlanabilir araç sahipleri / sürücöleri, araç kullanım tercihlerini ve ayarlarını da ilgili ekranlardan manuel olarak belirleyebilmektedir.
- Baęlanabilir araçlarda bulunan sensörler vasıtasıyla kişisel verilerin işlenmesi: Baęlanabilir araçlarda bulunan sensörler, aracın hızı, konumu, araç sürücüsünün sürüş davranışları, aracın yakıt tüketimi gibi araç sürücüsü ve araç hakkında, aracın koltuklarında yer alan sensörler vasıtasıyla araçta bulunan yolcular hakkında ve baęlanabilir aracın dışında yer alan sensörler vasıtasıyla araç çevresinde olan ilgili kişiler hakkında kişisel verileri otomatik olarak toplamaktadır. Özellikle araç ile ilgili işlenen veriler, arızaları teşhis etmek, sürücüye tavsiyelerde bulunmak ve araç performansını optimize etmek için kullanılmaktadır.
- Kişisel verilere uzaktan erişim sağlanması: Araç baęlantı ayarları açık olduęu sürece, baęlanabilir araç mobil uygulaması veya Wi-Fi üzerinden baęlanabilir araca uzaktan erişerek veri işlenmesi mümkündür. Bu sayede, araç üreticileri ve yetkili servis sağlayıcılar, araç teşhisi, bakım ve servis hizmeti ve araç yazılım güncellemeleri gibi işlemleri gerçekleştirmektedir.

Kişisel verilerin işlenmesi için yasal bir gerekçe olması gerekmektedir. Bu bakımdan, kişisel verilerin toplandıęı andan imha sürecine kadar tüm veri işleme faaliyetlerinin hukuki bir sebebe dayanarak sürdürölmesi gerekmektedir. Kişisel verilerin korunması kapsamındaki mevzuat düzenlemelerinde, kişisel verilerin işlenmesi belirli koşullara baęlanmıştır. Bu kapsamda KVKK'nın 5. maddesinin ilk fıkrasında, kişisel verilerin işlenmesi için ilgili kişinin açık rızasının varlığı kural olarak belirlenmişken açık rızanın temin edilmeden veri işleme faaliyetinin yürütölmesi için aynı maddenin ikinci fıkrasında sayılan “kanunlarda açıkça

öngörülme, fiili imkânsızlık, bir sözleşmenin kurulması veya ifası için kişisel verilerin işlenmesinin gerekli olması, alenileştirilme, hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması ve veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” veri işleme hukuki sebeplerinden birine dayanılması gerekmektedir. Aynı şekilde GDPR’ın 6. maddesinde kişisel verilerin işleme şartları düzenlenmekte ve verilerin yalnızca belirli koşullar altında işlenebileceği belirtilmektedir¹²⁵. GDPR’ın 6. maddesi uyarınca, hukuka uygunluk temelinde gerçekleştirilen veri koruma faaliyetleri, bireylerin onurunu ve özerkliğini koruyarak, adil ve yasal işlemlerin gerçekleşmesini sağlamak için şeffaf ve güvenli bir şekilde uygulanmalıdır. Aksi halde özellikle dijital dünyada pek çok mahremiyet riski meydana gelmektedir¹²⁶. AİHS 8. maddesi kapsamında, özel hayata saygı hakkı çerçevesinde veri işleme faaliyetlerini de kapsayan çeşitli gizlilik ihlali vakaları bulunmaktadır¹²⁷.

Bağlanabilir araçlarda yürütülen veri işleme faaliyetleri incelendiğinde, ilgili faaliyetler genel olarak aşağıda sayılan hukuki sebeplere dayanmaktadır:

- Sözleşmenin kurulması ve ifası için veri işlemenin zorunlu olması: Kişisel verilerin işlenmesi, bağlanabilir araç satış ve servis sözleşmelerinin kurulması ve ifası için gereklidir. Örneğin, araç garantisi veya yol yardım hizmeti sunmak için araç sahibinin kimlik ve iletişim bilgilerinin işlenmesi gerekmektedir.
- Kanunlarda açıkça öngörülmesi: Bazı hallerde kişisel verilerin işlenmesi yasal bir zorunluluktur. Örneğin, trafik kazalarıyla ilgili veriler, kolluk kuvvetleri tarafından kazanın soruşturulması amacıyla işlenmektedir.
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için

¹²⁵ Michael O’Doherty, “Internet Law, Bloomsbury Professional”, Croydon, 2020, s.202.

¹²⁶ Tugay Arat, M. Mert Aslan, “Sosyal Medyada Veri Güvenliği ve Kişisel Mahremiyet Sorunu”, Akdeniz Üniversitesi İletişim Fakültesi Dergisi, S:35, 2021, p.390.

¹²⁷ Gaughran v. The United Kingdom (Başvuru No.45245/15), 3/06/2020; Breyer v. Germany (Başvuru n No. 50001/12) 07.09.2020; Case Of Szabó And Vissy v. Hungary (Başvuru No. 37138/14).

zorunlu olması: Kişisel veriler, bağlanabilir aracın güvenliğinin temini ve kontrol edilmesi ile ilgili yasal yükümlülüklerle uymak için işlenmektedir. Örneğin, araç arızası tespit edildiğinde, araç sahibini veya sürücüyü bilgilendirmek ve gerekli onarımların yapılması için kişisel verileri işlemek söz konusu olmaktadır.

- Veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması: Bağlanabilir araçlarda sürücü ve yolcu güvenliğinin sağlanması adına kişisel veriler, teknik ve yazılım geliştirmelerinin yapılması, araç üreticisi ve katma değerli hizmet sağlayıcılar gibi veri sorumlularının sunduğu ürün ve hizmetlerin iyileştirilmesi ve geliştirilmesi gibi amaçlar kapsamında veri sorumlusunun meşru menfaatleri için işlenmektedir. Örneğin, veri sorumluları tarafından araç sürücüsüne sunulan trafik bilgilerinin doğru ve güncel olması adına yazılım geliştirmesi yapılması için konum verileri, araçlara eklenecek yeni donanımsal özelliklerin tespiti adına araç verisi kullanılmaktadır.
- Açık rıza: Araç sahibi veya sürücü, kişisel verilerinin belirli amaçlar için işlenmesine açık rıza verebilmektedir. Örneğin, sürücü, araç kullanım istatistikleri ile tarafına pazarlama faaliyetlerinin yapılması veya ilgili verilere dayanarak yapılan analizlerin sigorta şirketleri ile paylaşılarak tarafına sürüş skoruna uygun poliçe tekliflerinin sunulması için rıza verebilmektedir.

Tezin devamında bağlanabilir araçlarda işlenen kişisel veriler bakımından uygulaması ve örnekleri geniş olan iki hukuki sebebin detaylı analizine yer verilmektedir.

2.5.1. Veri İşlemenin Açık Rızaya Dayanması

Bağlanabilir araçlar, sürücü ve yolcular hakkında büyük miktarda kişisel veri işlemektedir. Bu veriler arasında yer alan sürüş davranışı ve alışkanlıkları, konum bilgileri, araç içi kamera ve ses kayıtları, biyometrik veriler, iletişim bilgileri gibi verilerin işlenmesi, verilerin kullanım amacına göre yapılacak analizler sonucu açık rıza veri işleme sebebine dayanılmasını gerekli kılmaktadır.

KVKK'ya göre açık rıza, ilgili kişinin isteğiyle veya karşı tarafın talebi üzerine verisinin işlenmesine onay vermesi anlamına gelir. Bu onay, veri işleyen tarafa hangi verilerin nasıl işleneceği konusunda yol gösterir ve ilgili kişinin hukuksal değerlerine saygı gösterilmesini sağlar¹²⁸. KVKK'da yer alan tanımına göre açık rıza üç unsur barındırmakta olup bunlar; belirli bir konuya ilişkin olması, rızanın bilgilendirmeye dayanması ve özgür iradeyle açıklanmasıdır¹²⁹. Ancak unutulmaması gerekir ki kişisel veri işleme faaliyeti, KVKK'da bulunan ve açık rıza dışında sayılan başka bir hukuki veri işleme sebebine dayanıyorsa, bu durumda ilgili kişinin açık rızası alınmamalıdır. Şayet kişisel veri işleme faaliyetinin açık rıza dışında bir hukuki sebebe dayanarak yapılması mümkünken ilgili kişilerin açık rızası alınırsa ilgili kişinin yanıltılması ve yanlış yönlendirilmesi ile veri sorumlusu tarafından hakkın kötüye kullanılması söz konusu olacaktır¹³⁰. Bu bakımdan “ilgili kişinin rızasının alınmasında, mevzuatta kişisel verilerin işlenmesi veya aktarılması için öngörülmüş olan diğer hukuka uygunluk hallerinden daha geçerli veya öncelikli bir şart olmadığına dikkat edilmeli, her bir işleme süreci için geçerli olacak hukuka uygunluk şartı ayrıca belirlenmelidir.”¹³¹ Ayrıca, açık rıza hukuki sebebine dayalı olarak kişisel veri işlenen durumda ilgili kişi açık rızasını çektiğinde veri sorumlusu tarafından veri işleme faaliyetine son verilmesi gerekmektedir. Bu halde farklı bir hukuki sebebe dayanarak veri işlenmeye devam edilmesi hukuka ve dürüstlük kurallarına aykırı işlem yapılması anlamına gelmektedir¹³².

Açık rıza kavramı diğer kişisel veri koruma mevzuatlarında da yer alan ve ilgili kişinin iradesini yansıtan bir kavramdır. GDPR kapsamında “rıza” ve “açık rıza”

¹²⁸ **Kişisel Verileri Koruma Kurumu**, Açık Rıza Rehberi, Nisan, 2018, s.3. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf> (e.t. 24.03.2024).

¹²⁹ KVKK'nın 3/1/a maddesine göre açık rıza, belirli bir konuya dair bilgilendirilmeye dayanan ve özgür iradeyle açıklanması gereken rıza anlamına gelmektedir. Bkz. <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf> (e.t. 21.03.2024).

¹³⁰ **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin İşlenme Şartları Rehberi, Nisan, 2018, s.2,3. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/9feefe58-9b0f-49c9-a0c7-2b2eb8c012bb.pdf> (e.t. 24.03.2024).

¹³¹ **Anı**, s. 126.

¹³² **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin İşlenme Şartları Rehberi, Nisan, 2018, s.3.

kavramlarının her ikisine de yer verilmiş olmakla beraber, yalnızca rıza kavramı tanımlanmaktadır. GDPR'daki tanımı kapsamında rıza; ilgili kişinin kendisiyle ilgili kişisel verilerin işlenmesini kabul ettiğini bir beyanla veya açık bir olumlu eylemle belirttiği isteklerinin özgürce verilmiş, belirli, bilgilendirilmiş ve açık bir şekilde belirtilmesi¹³³ hallerini içermelidir. Bu tanımdan hareketle rızanın aktif bir eylemle verilmesi gerektiği ve zımni rızanın kabul edilmediği görülmektedir. Nitekim, bir sözleşmeye bağlı olarak rızanın da verilmiş sayılması gibi kullanımlar, rızanın özgürce verilmesi koşulunu sorgulatmaktadır¹³⁴. Ayrıca GDPR hükümleri incelendiğinde rıza ile veri işleme hukuki sebebine dayanan faaliyet için kişisel verilerin işlenmesinde rızanın (consent) varlığı, özel nitelikli kişisel verilerin işlenmesi bakımından ilgili kişinin açık rızasının (explicit consent) varlığı aranmaktadır¹³⁵. Açık (explicit) terimi, rızanın ilgili kişi tarafından ifade edilme şekline atıfta bulunur. Bu ifade, ilgili kişinin açık bir rıza beyanı vermesi gerektiği anlamına gelmektedir. Açık rızanın temin edildiğini ispatlayabilmenin en temel yolu ise rızayı yazılı bir beyanla açıkça teyit etmektir. Bu bakımdan uygun olduğu hallerde veri sorumlusu, gelecekte olası tüm şüpheleri ve potansiyel kanıt eksikliğini ortadan kaldırmak için ilgili kişinin veri işleme faaliyetine ilişkin açık rıza verdiği dair yazılı bir beyan almayı değerlendirmelidir. Ancak, bu tür bir yazılı beyan açık rıza almanın tek yolu olmayıp GDPR kapsamındaki uygulamalarda geçerli açık rıza gerektiren durumlarda yazılı ve imzalı bir beyan dışında da yöntemler ele alınmaktadır. Örneğin, ilgili kişi elektronik ortamda bir form doldurarak veya onay kutucuğu işaretleyerek, açık rızasına ilişkin bir e-posta göndererek, imzasını taşıyan taranmış bir belge yükleyerek veya elektronik imza kullanarak açık rızasını verebilmektedir. Hatta açık rızanın sözlü beyan olarak alınması da teoride mümkün olup, bu halde yalnızca veri sorumlusu için rızanın

¹³³ GDPR 4/11 maddesi kapsamında rıza tanımı şu şekildedir: “‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

¹³⁴ **Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler, "The EU General Data Protection Regulation (GDPR): A Commentary", Oxford University Press, Şubat, 2020, s. 330.**

¹³⁵ **Anı, s.129.**

kaydedildiği sırada geçerli bir açık rızanın alındığının ispatına ilişkin tüm koşulların sağlandığını kanıtlamak diğer yöntemlere kıyasen zor olabilecektir¹³⁶.

Veri sorumlusunun ilgili kişilerden aydınlatılmış bir şekilde rıza alması gerekliliği, yapay zeka sistemlerinin kullanılması kapsamında da bir sorunu da beraberinde getirmektedir. GDPR'ın 4. maddesine göre, rıza tanımı göz önünde tutularak yapay zeka sistemlerini kullanan ve büyük miktarda veriyi analiz eden veri sorumlularının kişisel verileri işleyebilmek için ilgili kişilerden rıza alacağı işleme faaliyetleri bakımından ilgili kişilerin, işlenen verilerin niteliği ve kaynağı konusunda açık ve yeterli şekilde bilgilendirmesi gerekmektedir. Ancak, kişisel verilerin yapay zeka sistemlerinde algoritmalar tarafından analiz edilmesi veya başlangıçta kişisel olmayan verilerin kombinasyonlarıyla elde edilmesi durumunda, verilerin kaynağını net bir şekilde belirlemek oldukça zorlaşmaktadır¹³⁷. Bu nedenle, GDPR'ın 14. maddesinde belirtilen aydınlatma yükümlülüğü, böyle bilgilerin ilgili kişilere sağlanmasının orantısız bir yük oluşturabileceği gerçeği ile çelişebilmektedir.

Rehber'de araç üreticileri ve hizmet sağlayıcılarının, veri işleme faaliyetlerinin çoğu, hatta tamamı için ilgili kişilerin onayını alması gerektiğine ilişkin açıklamalara¹³⁸ yer verilmektedir. Bağlanabilir araçlar ile kişisel verilerin işlendiği hallerde temel olarak GDPR baz alınsa da belirli bir sektörü hedefleyen düzenlemeleri içermekle beraber ek olarak kişisel verilerin korunması kapsamında da hükümler barındıran düzenlemeler de dikkate alınmalıdır. 2002/58/EC sayılı Direktif ile GDPR arasındaki etkileşim buna bir örnektir. Örneğin Rehber'de hem 2002/58/EC sayılı Direktif hem de GDPR kapsamında çift onayın alınması da değerlendirilmektedir. 2002/58/EC sayılı Direktif AEA'da bir kullanıcının cihazında bilgi depolamak veya cihazdaki bilgiye erişmek için özel kurallar

¹³⁶ **Avrupa Veri Koruma Kurulu**, Guidelines 05/2020 on consent under Regulation 2016/679, Mayıs, 2020, ("Rıza Rehberi"). İlgili rehber internet üzerinden şu link ile ulaşılabilir: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (e.t. 24.03.2024).

¹³⁷ Paal, s. 293.

¹³⁸ Rehber, s. 27.

belirlemektedir. Bağlanabilir araçlar ve bağlı cihazlar, 2002/58/EC sayılı Direktif kapsamında "terminal ekipmanı" olarak nitelendirilmektedir. Bu bakımdan, 2002/58/EC sayılı Direktif'in 5/3 maddesi, sadece elektronik haberleşme hizmetleri için değil, aynı zamanda bir kullanıcının telefon ve araba gibi cihazlarında bilgi depolamak veya erişmek için önceden rıza gerektiğini ve bunun yalnızca iletişim hizmeti sağlayıcıları için olmayıp, kamu veya özel ayrımı olmaksızın her kuruluş için geçerli olduğunu düzenlemektedir. Söz konusu bilgi kişisel veri ise, işlenen kişisel veriler için ayrıca GDPR'ın 6. maddesi kapsamında da veri işleme hukuki sebebinin analiz edilerek gerekmesi halinde rıza alınması gerekmektedir¹³⁹. Ancak, bu rızaların gerekliliği ve kapsamı, her iki düzenlemenin hüküm ve uygulamalarına bağlı olarak değişebileceğinden veri sorumluları veri işleme hukuki sebebini açık rızaya dayandırdığı halde her iki mevzuatın da gerekliliklerini analiz etmelidir.

2002/58/EC sayılı Direktif'in 5/3 maddesi, rıza gerekliliğinden istisnaları da düzenlemektedir. Bu kapsamda, (i) yalnızca bir elektronik iletişim ağı üzerinden bir iletişimin iletilmesi ve (ii) abone veya kullanıcı tarafından açıkça talep edilen bir bilgi toplumu hizmetinin sağlayıcısının hizmeti sunması için kesinlikle gerekli olması gibi durumlarda, terminal ekipmanındaki bilgilere erişim yoluyla elde edilen kişisel veriler de dahil olmak üzere kişisel verilerin işlenmesi GDPR'ın 6. maddesinde belirtilen hukuki sebeplerden birine dayanmaktadır. Unutmamak gerekir ki, 2002/58/EC sayılı Direktif rıza alınmasını gerektirmese de veri sorumlusunun hala GDPR'ın 6. maddesi kapsamında, ilgili veri işleme faaliyetine uygun hukuki sebebi belirleme yükümlülüğü bulunmaktadır. Örneğin, söz konusu hizmetler bilgi toplumu hizmetleri olarak nitelendirildiğinde, ilgili kişi tarafından talep edilen GPS navigasyon hizmetlerini sağlamak için veri işlemenin gerekli olduğu durumlarda rıza alınması gerekli olmayacaktır¹⁴⁰.

¹³⁹ **Avrupa Veri Koruma Kurulu**, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and Powers of data protection authorities, Mart, 2019. İlgili görüşe internet üzerinden şu link ile ulaşılabilir: https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf (e.t. 26.03.2024).

¹⁴⁰ Rehber, s.8.

Bu bakımdan, veri işleme faaliyetinin özellikle açık rıza veri işleme hukuki sebebine dayandığı durumlarda ilgili kişinin işlenen kişisel verilerinin veri sorumlusu tarafından nasıl kullanılacağına dair detayları bilmesi sağlanmalıdır. Bu bakımdan araç üreticilerinin bağlanabilir araçlardan elde edilen verileri, katma değerli hizmet sağlayıcı üçüncü taraflara ilgili kişi araç sahibi veya sürücüsünün açık rızasına bağlı olarak aktardığı durumlarda, rızaya ilişkin bilgi akışının araç üreticisi ve hizmet sağlayıcı diğer üçüncü kişiler arasında doğru ve güncel olarak sağlanması temin edilmelidir. Bu senaryoda, kişisel verilerin işlenmesine ilişkin şeffaflık hizmet sağlayıcının uygulamasında veya web sitesinde ilgili kişiyi bilgilendirmesi ve rızasını temini ile başlayabilmektedir. Hizmet sağlayıcı, sunduğu hizmet için gerekli olan kişisel verileri ve aydınlatma yükümlülüğünü yerine getirmesi için sunması gereken diğer bilgileri ilgili kişi araç sahibine / sürücüsüne sunarak açık rızasını alacak ve ilgili rızayı takiben araç üreticisine ileterek, rıza alınan süreçle sınırlı olarak bağlanabilir araç vasıtasıyla toplanan verilerin tarafına doğru ve güncel olarak aktarımı için gerekli teknik ve idari tedbirleri alacaktır. Benzer şekilde, araç üreticileri de doğrudan sundukları ve üçüncü taraf hizmet sağlayıcılar ile ortak sundukları açık rıza hukuki sebebine tabii hizmetler bakımından bağlanabilir araç ekranlarında ve bağlanabilir araç mobil uygulamasında bir ara yüz sağlayarak ilgili kişilerin açık rızasını temin etmelidir. Tüm bu süreçte araç üreticileri ile hizmet sağlayıcıların ilgili kişilerin rıza verme durumu bakımından gerçek zamanlı bilgi sağlaması gerekmektedir. Araç üreticileri veri aktaran veri sorumlusu olarak merkez konumda olup, birçok hizmet sağlayıcının sunacağı hizmetler için alınan rızaların merkezi olarak işlenmesi ile aktarılan veri taleplerini gerçek zamanlı olarak doğrulamaktadır¹⁴¹.

İlgili kişilerin işlenmesine açık rıza verdiği kişisel verilerine ve veri işleme amaçlarına takip eden kullanımlarında kolayca erişmesi gerekmektedir. İlgili kişilere dilerlerse açık rızalarını kolayca ve dilediği zaman geri alma imkanı

¹⁴¹ Otonomo, s.10.

tanınmalı¹⁴² ve güncel tercihleri veri sorumlusu veri kayıt sisteminde sorunsuz şekilde tutulmalıdır. İlgili kişilerden rıza alınması sürecinde kullanılan toplama alanları ve rızanın temini için sağlanan kolaylıklar, aynı şekilde rızanın geri alınması sürecinde de temin edilmelidir. Örneğin, ilgili kişi araç sahibi veya sürücüsü daha önce bir veri işleme süreci için vermiş olduğu açık rızayı bağlanabilir araç ekranları ve bağlanabilir araç mobil uygulaması gibi veri toplama ekranlarından kolaylıkla geri alabilmelidir. Bu bakımdan açık rızanın geri alınmasına ilişkin sürecin yalnızca kişisel veri işleme politikası ve aydınlatma metinleri içerisine gömülen teorik bir bilgi olmanın ötesinde, ilgili kişinin başvurabileceği yasal bir hakkı olarak erişiminin kolaylaştırılması gerekmektedir.

Açıklanan sebeplerle, veri sorumlularının faaliyetleri kapsamında işledikleri kişisel verilerin ilgili kişi haklarına etkisini ve veri işleme hukuki sebeplerini belirlerken KVKK ve GDPR gibi ana veri koruma mevzuatlarının yanı sıra ilgili faaliyete yönelik kişisel verilerin korunması kapsamında hükümler de içeren sektörel düzenlemeleri de göz önünde bulundurması gerekmektedir. Veri sorumlularınca açık rıza hukuki sebebine dayanarak veri işlenmesi halinde ilgili kişilere karşı aydınlatma yükümlülüğünün yerine getirilmesi şeffaflığı arttırarak ilgili kişilerin işlenen kişisel verilerinin nasıl toplandığı, hangi verilerin ne amaçla işlendiği, ilgili kişi olarak haklarının neler olduğu, ilgili kişinin vermiş olduğu açık rızasını geri alma yöntemi ve paylaşıldığı üçüncü kişilerle ilgili tüm bilgilere erişmesi sağlanmalıdır. Açık rızaya dayalı veri işlemede aydınlatma yükümlülüğünün mevzuata uygun şekilde yerine getirilmesi de ilgili kişilerin veri sorumlusuna karşı güven duygusunu artırmaktadır. Bağlanabilir araçlarda işlenen kişisel veriler bakımından bazı senaryolarda araç sürücüsünün ve yolcuların kişisel veri işleme faaliyetinden haberdar olmaması riski bulunmaktadır. Bu bilgi eksikliği de esasen hukuka uygun bir açık rızanın temin edilmesinin önündeki ciddi engellerden biridir. Bu bakımdan, bağlanabilir araçlarda kişisel veri işleme faaliyetlerinden açık rıza hukuki sebebine dayanılacak durumlarda klasik

¹⁴² **Mesut Serdar Çekin**, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, On İki Levha Yayıncılık, İstanbul, 2018, s. 62.

yöntemlerin dışına çıkılarak, hukuka uygun şekilde açık rızanın temin edilebileceği yöntemlerin belirlenmesi oldukça önemlidir. Pratikte ayrıca rıza sürecinin yalnızca araç sahipleri üzerinden yürütülmesi, araç sahibi olmayan araç sürücüsü ve yolcusu gibi ilgili kişilere karşı aydınlatma yükümlülüğünün yerine getirilememesi ve hukuka uygun şekilde rızaların temin edilmemesi riskini barındırmaktadır. Özellikle araç kiralama şirketlerinin ve ikinci el araç satışlarında yeni araç sahiplerine ulaşma noktasında bağlanabilir araç üreticileri ile katma değerli hizmet sunun üçüncü tarafların ilgili kişileri aydınlatarak rızalarını temin etme yükümlülüklerini düzenli olarak gözden geçirmeleri gerekmektedir.

Veri işleme faaliyetinin açık rıza hukuki sebebine dayanılarak gerçekleştiği hallerde, her bir veri işleme faaliyeti için ayrı olarak rızanın temin edilmesi gerekmektedir. Açık rıza hukuki sebebine dayanarak veri işlemenin gerçekleştiği faaliyetin devamında farklı amaçlarla veri işlenmesinin gerekmesi halinde veri sorumlusunun ilgili yeni amaçlar için ayrıca açık rıza temin etmesi gerekmektedir. Bu bakımdan rızanın spesifik ve bilgilendirilmiş olması ve ilgili kişilerin her bir veri işleme amacı için bilgilendirilerek belirli amaçları reddetme hakkına sahip olmaları gerekmektedir¹⁴³. Örneğin, aracın kullanımı sırasında araç bakımı amacıyla işlenen telemetri verileri, sürüş davranışını baz alan sigorta poliçelerinin sunulması için sürücü profilleri oluşturmak amacıyla araç sürücüsünün rızası olmadan sigorta şirketleri ile paylaşılmamalıdır¹⁴⁴.

2.5.2. Veri İşlemenin Sözleşmenin İfası İçin Gerekli Olması

Kişisel verilerin işlenmesi, GDPR ve KVKK gibi düzenlemeler kapsamında belirli hukuki sebeplere dayanmalıdır. Bu hukuki sebeplerden biri, kişisel verilerin sözleşmenin kurulması ve ifası için işlenmesinin zorunlu olmasıdır. Bu durum, bağlanabilir araçlar söz konusu olduğunda, özellikle araç sahibi ile araç üreticisi

¹⁴³ Rıza Rehberi, s.13-17.

¹⁴⁴ Rehber, s.14.

veya hizmet sağlayıcı arasında kurulmuş olan hizmet sözleşmelerine dayanmaktadır.

Bağlanabilir araçlarda araç sahibi ile araç üreticisi arasındaki araç satış sözleşmesi kapsamında araç üreticisi, araç sahibine belirli hizmetleri sunmayı taahhüt etmektedir. Örneğin, aracın yazılım güncellemeleri, güvenlik sistemleri veya acil durum hizmetleri gibi fonksiyonlar, sözleşmenin bir parçası olarak kabul edilebilir. Bu tür hizmetlerin sağlanabilmesi için aracın konum bilgisi, sürüş davranışları ve teknik durumu gibi belirli kişisel verilerinin işlenmesi gerekmektedir.

Bu bağlamda, aracın güvenli ve verimli bir şekilde çalışmasını sağlamak amacıyla gerekli olan kişisel veri işleme faaliyetleri GDPR 6/1-(b) maddesi ve KVKK 5/2-(c) maddesinde düzenlenen "sözleşmenin kurulması ve ifası için zorunlu olma" hukuki sebebine dayanmaktadır. Örneğin, araçta oluşabilecek bir teknik arızanın uzaktan teşhis edilmesi ve çözülmesi için aracın durumu hakkında veri işlenmesi, araç sahibinin hizmet sözleşmesine dayalı olarak beklediği hizmetlerin sağlanabilmesi için gereklidir. Sözleşmenin ifası, esasen GDPR’da yer verilen diğer iki hukuki sebepler olan meşru menfaat ve hukuki yükümlülük kapsamında değerlendirilen bazı özellikli veri işleme faaliyetlerinin dayandırılabilceği bir hukuki sebep olarak ele alınsa da AB veri koruma mevzuatı her bir hukuki yükümlülüğü ayrı ayrı ele alarak GDPR 6. maddeyi bu bakımdan geniş tutmuştur¹⁴⁵. Bu bakımdan, bu tez kapsamında temel inceleme konusunun bağlanabilir araç sahibi / sürücüsü ilgili kişilerin araç üreticisi ve katma değerli hizmet sağlayıcısı gibi veri sorumluları ile ürün / hizmet alımı kapsamında işlenen kişisel verileri olduğundan, GDPR’da düzenlenen diğer rıza dışındaki hukuki sebepler ana hukuki sebep olarak ele alınmayarak ilgili hizmetler bütünüyle “sözleşmenin ifası” altında incelenmektedir.

¹⁴⁵ **Kuner**, s. 330-331.

Sözleşmenin kurulması ve ifası için zorunlu olan veri işleme faaliyetleri bakımından bağlanabilir araçlar kapsamında işlenen veriler ve işleme süreçleri aşağıda ele alınmaktadır:

- Araç konum bilgisi: Bağlanabilir araçlarda en yaygın kullanılan fonksiyonlardan biri navigasyon hizmetleridir. Navigasyon hizmeti sunulabilmesi için aracın anlık konum bilgisinin navigasyon aktif olduğu müddetçe sürekli olarak izlenmesi ve işlenmesi gerekmektedir. Bu işlem, araç sürücüsüne doğru ve güncel yönlendirmelerin sağlanabilmesi için zorunludur. Ayrıca, konum verisi acil durum yardım hizmetleri için de kullanılmaktadır. Örneğin, bir kaza durumunda aracın yerini belirlemek ve acil servislerin yönlendirilmesi için konum verisi işlenmektedir. Navigasyon hizmeti ve acil durum yardımı, genellikle araç üreticisi ile araç sahibi arasında yapılan sözleşmenin bir parçası olarak sunulan hizmetlerdir. Bu nedenle, konum bilgisinin işlenmesi, sözleşmenin ifası için zorunlu bir veri işleme faaliyeti olarak kabul edilmektedir.

- Araç motor durumu, yakıt tüketimi, hız, fren kullanımı, lastik basıncı, batarya durumu gibi araç performans ve teknik durum bilgileri: Araç performans ve teknik durum bilgileri, aracın güvenli ve verimli bir şekilde çalışmasını sağlamak için sürekli olarak izlenmektedir. Bu tür veriler, aracın bakım ihtiyacının belirlenmesi, olası arızaların önceden tespiti ve uzaktan teşhis için işlenmektedir. Örneğin, bataryanın durumu hakkında bilgi toplamak, elektrikli araçların enerji yönetimi için kritiktir ve bu verilerin işlenmesi, kullanıcının araçla ilgili sözleşmeye dayalı haklarını ve beklentilerini karşılamak için zorunludur. Araç sahibi / sürücüsünün araçtan beklediği güvenli ve sorunsuz kullanım, üretici ile yapılan satış ve hizmet sözleşmesinin temel bir parçasıdır. Bu nedenle, teknik verilerin işlenmesi, sözleşmenin ifası için zorunludur.

- Hızlanma, ani frenleme, direksiyon hareketleri, ortalama hız, yolculuk süresi gibi sürüş davranışlarına ilişkin veriler: Sürüş davranışlarına dair veriler, araç içi güvenlik sistemlerinin etkinleştirilmesi, sürücü asistan sistemlerinin

doğru çalışması ve sigorta hizmetlerinin özelleştirilmesi gibi çeşitli amaçlar için işlenmektedir. Örneğin, bir sürüş güvenliği sistemi, ani frenleme durumlarını analiz ederek kaza öncesi uyarılar sağlamaktadır. Araç sahibi ile yapılan ürün / hizmet sözleşmeleri kapsamında, özellikle sigorta poliçelerinin kişiselleştirilmesi ve sürüş güvenliğinin artırılması gibi amaçlarla bu verilerin işlenmesi zorunlu olmaktadır. Bu durum, sigorta şirketleri ve araç üreticileri ile yapılan sözleşmelerin ifası için gerekli bir veri işleme faaliyeti olarak değerlendirilmektedir.

- Kullanıcının medya tercihleri, sesli komutlar, bağlantılı cihaz bilgileri (örneğin, telefon veya tablet bağlantısı), uygulama kullanım alışkanlıkları: Araç içi eğlence ve bilgilendirme sistemleri, kullanıcının tercihlerine dayalı olarak kişiselleştirilmiş içerikler sunmaktadır. Bu sistemler, kullanıcının medya tercihlerini, örneğin, sık dinlenen radyo istasyonları veya müzik listeleri, kaydederek, kullanım deneyimini optimize eder. Ayrıca, sesli komut sistemleri aracılığıyla araçla etkileşim sağlanır ve bu verilerin işlenmesi, bu tür hizmetlerin sağlanması için zorunludur. Bu tür veri işleme faaliyetleri, kullanıcı ile yapılan hizmet sözleşmelerinin bir parçası olduğunda, örneğin, bir müzik hizmet sağlayıcısı ile yapılan sözleşme, kullanıcının medya alışkanlıklarının işlenmesini gerektirmektedir. Bu nedenle, bu verilerin işlenmesi, sözleşmenin ifası için zorunludur.

- Acil durum yardımı ve çağrı hizmetleri kapsamında konum bilgisi, sürücü ve yolcu bilgileri, araç durumu, çarpışma sensör verileri: Acil durum yardım hizmetleri, bir kaza veya acil durumda kullanıcılara yardım sağlamak amacıyla hayati önem taşır. Bu hizmetlerin sağlanabilmesi için aracın konum bilgisi, araç durumu ve içindeki kişilerin bilgileri gibi veriler işlenmektedir. Örneğin, bir çarpışma durumunda, acil servislerin bilgilendirilmesi ve doğru yere yönlendirilmesi için bu verilerin anında işlenmesi zorunludur. Bu hizmetler genellikle araç üreticisi ile yapılan sözleşmelerin bir parçası olarak sunulur. Araç sahibi, araç satın alırken veya hizmet sözleşmesini imzalarken bu tür

hizmetlerden yararlanmayı kabul eder. Dolayısıyla, acil durum yardımı için veri işleme faaliyetleri, sözleşmenin ifası için zorunludur.

Araç üreticilerinin yanı sıra, üçüncü taraf katma değerli hizmet sağlayıcıları da bağlanabilir araçlardan toplanan verileri işlemektedir. Bu hizmet sağlayıcılar, örneğin araç sigortası, eğlence içerikleri veya araç bakım hizmetleri gibi çeşitli ek hizmetler sunmakta ve araç sahipleri / sürücüleri bu tür hizmetlerden faydalanmak için ilgili hizmet sağlayıcı ile ayrı bir sözleşme ilişkisine girmektedir. Katma değerli hizmet sağlayıcılarının sunduğu hizmetlerin ifası için belirli kişisel verilerin işlenmesi gerekmektedir. Örneğin, sigorta hizmeti sunan bir şirketin, aracın sürüş davranışları hakkında veri toplaması, hizmetin özelleştirilmesi ve fiyatlandırmanın yapılabilmesi için zorunlu olmaktadır. Rehber'de¹⁴⁶ de benzer şekilde, "sürüş başına öde" veya iyi sürüş davranışını teşvik eden "nasıl sürersen öyle öde" (pay-as-you-drive/pay-how-you-drive) sigorta hizmetleri, park yeri kiralama ve rezervasyonu ve araç hırsızlığıyla mücadele gibi durumlarda, hizmet sağlayıcının veri işleme faaliyetleri, "sözleşmenin kurulması ve ifası için zorunluluk" hukuki sebebine dayandırılmaktadır. Örneğin, bir kullanıcının sürüş alışkanlıklarına dayalı olarak sigorta primi belirlenmesi veya bir park yerinin rezerve edilmesi gibi durumlar, hizmetin sağlanması için veri işlemeyi zorunlu kılmaktadır.

Kişisel verilerin "sözleşmenin kurulması ve ifası" için işlenmesinin zorunlu sayılabilmesi için işlenen kişisel verilerin, sözleşmede belirtilen hizmetin sağlanması için gerekli olup olmadığı değerlendirilmelidir. Örneğin, bir navigasyon hizmeti sağlanacaksa, aracın konum bilgilerinin işlenmesi zorunludur. Ancak sağlanacak navigasyon hizmetinin sözleşmede tespit edilen amaç dışında bir kullanımının da planlanması halinde burada yeni bir hukuki sebep analizi yapılması gerekmektedir.

Bir üst bölümde her ne kadar 2002/58/EC sayılı Direktif kapsamında rıza alınması gerekli haller ele alınsa da E-Gizlilik Yönetmeliği'nin Avrupa Konsey

¹⁴⁶ Rehber, s. 26, 29 ve 35.

taslağının 21. gerekçesi¹⁴⁷, bu yönetmelik kapsamında onayın gerekli olmadığını öne sürmektedir. Bu gerekçede, "IoT hizmetlerinin bağlı cihazlara dayandığı durumlarda, bu cihazların işleme ve depolama kapasitelerinin kullanımı ve orada depolanan bilgilere erişim, kullanıcının talep ettiği hizmetin sağlanması için gerekli olduğu ölçüde onay gerektirmemelidir" denilmektedir. Bağlanabilir araçlar gibi bağlı cihazlara dayanan IoT hizmetleri alanında bu cihazların işleme ve depolama kapasitelerinin kullanımı ve orada depolanan bilgilere erişim, son kullanıcının talep ettiği hizmetin sağlanması için gerekli olduğu ölçüde rıza gerektirmemelidir. Örneğin, güvenlikle ilgili yazılım güncellemeleri için bağlanabilir araçlardan bilgi depolama, işleme veya bu bilgilere erişim için sözleşmesel ilişki geçerlidir.

AB yeni mevzuat düzenlemelerinin verinin işlenmesi adına salt ilgili kişi rızasına bağlı süreçleri işletmeden diğer hukuki sebeplere yer vermesi oldukça yerinde ve olumludur. Bunun en temel sebebi ise, rıza ve sözleşmenin ifasının bir arada kullanılmasının uygulamada sorunlara yol açmasıdır. Örneğin, araç sahibi / sürücüsünün rızasını geri çekmesi, taraflar arasındaki hizmet / ürün sözleşmesi hala yürürlükteyken dahi veri işlemenin durdurulmasına sebep olabilmektedir. Ancak, Avrupa Konsey taslağı, kullanıcının açıkça talep ettiği bir hizmeti sağlamak için verilerin depolanması veya erişim sağlanmasına olanak tanıdığı için yeni E-Gizlilik Yönetmeliği gibi mevzuat düzenlemelerinin yürürlüğe girmesi bu tarz sorunları ortadan kaldıracaktır¹⁴⁸.

Bağlanabilir araçlarda siber güvenlik ve ürün güvenliği gibi düzenleyici gereklilikler, üreticilerin belirli verileri işlemelerini zorunlu kılmaktadır. Örneğin, bir aracın güvenliğini sağlamak için siber güvenlik önlemlerinin uygulanması sırasında kişisel verilerin işlenmesi gerekebilir ve ürün güvenliği ve yasal

¹⁴⁷[https://www.european-eprivacy-regulation.com/ePrivacy_Regulation_Preamble_21_to_30_\(Council_Proposal_10.02.2021\).html](https://www.european-eprivacy-regulation.com/ePrivacy_Regulation_Preamble_21_to_30_(Council_Proposal_10.02.2021).html) (e.t. 30.08.2024).

¹⁴⁸ **European Automobile Manufacturers Association**, ACEA comments EDPB guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, Nisan, 2020. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: https://www.acea.auto/files/ACEA_comments_EDPB_guidelines_1-2020.pdf (e.t. 23.08.2024).

uyumluluk açısından kritik olduğundan, sözleşmeye dayalı veri işleme, bu tür yasal yükümlülüklerin yerine getirilmesini sağlamaktadır.

Bağlanabilir araçlarda veri işlemenin kullanıcı memnuniyeti ve güvenliğinin temini gibi amaçlardan kaynaklanarak kesintisiz sürmesi önemlidir. Bu bakımdan hukuki sebebin sözleşmenin ifasına dayandırılması, rızanın aksine veri işlemenin kesintisiz devam etmesini sağlamaktadır¹⁴⁹. Rızaya dayalı veri işlemlerde, kullanıcının rızasını geri çekmesi durumunda veri işleme durdurulmak zorundadır, bu da hizmetin sağlanmasını engelleyen bir haldir. Örneğin, bir sürücü, sigorta sözleşmesi kapsamında veri işlenmesine onay verdikten sonra bu onayı geri çekerse, sigorta priminin doğru hesaplanması mümkün olmayacaktır ve veri işleme yarıda kesilecektir. Ancak, sözleşmenin ifası dayanağı ile veri işlemeye devam edilmesi, hizmetin kesintisiz ve sorunsuz bir şekilde sunulmasını sağlamaktadır. Benzer şekilde sözleşmeye dayalı veri işleme, kullanıcı deneyimini ve araç işlevselliğini önemli ölçüde iyileştirmektedir. Sürekli onay talep edilmesi veya kullanıcı etkileşimi gerektiren durumlar, sürücü dikkatinin dağılmasına ve araç işlevlerinin kesintiye uğramasına neden olmaktadır. Örneğin, her seferinde bir veri işleme özelliği etkinleştirildiğinde rıza talep edilmesi, sürüş sırasında tehlikeli olabilir ve kullanıcıların araçtaki bazı özellikleri etkili bir şekilde kullanmasını engelleyebilmektedir. Bu nedenle, sözleşmenin ifası dayanağı, ölçülü ve amaca uygun olarak işlenen verilerin daha akıcı ve kullanıcı dostu bir şekilde işlenmesini sağlayarak hem güvenliği artırmakta hem de işlevselliği korumaktadır.

Bununla birlikte, sözleşmenin ifası kapsamında veri işleme hallerinde de diğer mevzuatlardan kaynaklı yükümlülüklerin gözetilmesi oldukça kritiktir. Örneğin, araç üreticisi ve araç sahibi arasındaki sözleşmesel ilişki kapsamında işlenen veriler bakımından AB Veri Yasası ile akıllı ürün üreticilerine ve tasarımcılarına, kullanıcılarla ve kullanıcıların belirlediği üçüncü şahıslarla veri paylaşma yükümlülüğü getirilmiştir. Bağlanabilir araçlar gibi ürünlerde bu yükümlülük, kullanım sırasında üretilen geniş çapta veri nedeniyle önemli etkiler doğurmaktadır.

¹⁴⁹ Kuner, s. 331.

AB Veri Yasası, AB içinde IoT çapında veri paylaşımını sağlamak için temel bir çerçeve oluşturmakla beraber bağlanabilir araçlar için "araç içinde üretilen verilere" erişim ve kullanım koşullarını belirlemeye yönelik özel düzenlemeler¹⁵⁰ de gündeme alınmıştır. Bu düzenlemelere uyum sağlamak, üreticilerin ve tasarımcıların yasal yükümlülüklerini yerine getirmesi açısından kritik öneme sahiptir.

Veri paylaşma yükümlülüğü kapsamındaki veriler arasında aşağıda sayılanlar yer almaktadır¹⁵¹:

- Bağlanabilir aracın performansı, kullanımı ve çevresi hakkında veriler ve kullanıcı tarafından ortak kullanım sırasında üretilen ilgili hizmetler, yerleşik uygulamalar, örneğin, GPS konumu veya sensörler tarafından yakalanan görüntüler, donanım durumu ve arızaları gösteren özellikler.
- Araç sürücüsünün ve aracın hareketsiz olduğu zamanlarda, bekleme modunda veya kapalı durumdayken üretilen veriler (örneğin, pillerin durumu).
- "Ham veriler" ve ayrıca meta verilerle zenginleştirilmiş veriler dahil verilerin kullanılabilir hale getirilmesi için temel bağlam ve zaman damgası içeren, yaygın olarak kullanılan bir formata uygun yeniden düzenlenmiş veriler olarak "ön işlenmiş veriler".

Veri paylaşma yükümlülüğü kapsamına girmeyen veriler arasında aşağıda sayılanlar yer almaktadır:

- Ham verilerden türetilen bilgiler, ek analizler ve yatırımların sonuçları.

¹⁵⁰ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources_en (e.t. 30.08.2024).

¹⁵¹ **Hogal Lovells**, EU Data Act (part 5): smart cars and data sharing obligations – Q&A, Eylül, 2023. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://www.engage.hoganlovells.com/knowledgeservices/news/eu-data-act-part-5-smart-cars-and-data-sharing-obligations-qa> (e.t. 30.08.2024).

- Araç sahibi / sürücüsünün içerik kaydettiği, ilettiği, görüntülediği veya oynattığı sırada bağlanabilir araç tarafından üretilen veriler ve ayrıca bu içeriklerin kendisi.
- Araç üreticisi tarafından tasarlanan ve geri alınamayacak şekilde oluşturulan ürünlerin kullanımı sırasında üretilen veriler (örneğin, elektronik iletişim hizmeti, fiziksel bağlantı veya cihaz üzerinde erişim yoluyla temin edilemeyen veriler)

Veri paylaşımı talep etme hakkına sahip olanlar esas olarak veri kullanıcılarıdır. Veri kullanıcıları dediğimiz kişiler ise bir bağlanabilir aracı satın alan veya kiralayan gerçek kişi ve bir filo kullanan şirket gibi tüzel bir kişidir. Ancak, bazı durumlarda veri kullanıcısının kim olduğu konusunda belirsizlikler söz konusudur. Örneğin, kiralık araç hizmetlerinde veri kullanıcısının ve dolayısıyla veri paylaşımı talep etme hakkına sahip kişinin kiralık araç şirketi mi yoksa aracı kiralayan kişi mi olduğu tartışmalıdır. Burada esasen bağlanabilir araçtan doğan verinin kullanım ve paylaşım menfaatinin hangi tarafta baskın olduğuna ilişkin analiz yaparak paylaşım taleplerini değerlendirmek isabetli olacaktır.

Veri paylaşımı, kullanıcı veri alıcısı olduğu durumda, teknik olarak mümkünse, verilerin doğrudan cihaz üzerinde depolama alanından veya uzak bir sunucudan erişilebilir hale getirilmesi suretiyle gerçekleştirilmelidir. Doğrudan erişim sağlanamıyorsa, üretici, verileri (ve ilgili meta verileri) derhal, ücretsiz, kolayca erişilebilir, güvenli, yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta ve mümkünse aynı kalitede temin etmekle yükümlüdür. Sözleşmeye dayalı kısıtlamalar, yasal güvenlik gerekliliklerini zayıflatabilecekse, verilerin erişimi, kullanımı veya paylaşımı kısıtlanabilir veya yasaklanabilmektedir. Bu durum, özellikle bağlanabilir araçlar bağlamında, verilerin paylaşılmasının kişisel güvenliği tehlikeye atabileceği durumlarda önem arz etmektedir. Bu bakımdan kullanıcının elde ettiği verileri, verilerin kaynaklandığı ürünle rekabet edecek bir ürün üretmek amacıyla kullanımı yasaklanmaktadır.

Veri paylaşımı üçüncü bir tarafla gerçekleştirildiğinde, üretici, verileri aynı şekilde derhal, ücretsiz, güvenli, yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta ve varsa aynı kalitede sağlamakla mükelleftir. Veriler ticari sır yasalarıyla korunuyorsa, veri sahibi ve üçüncü taraf arasında, gizliliğin korunması amacıyla gerekli teknik ve idari tedbirleri belirlemek üzere bir anlaşma yapılmalıdır. Üçüncü taraflar, bu verileri, verilerin kaynaklandığı ürünle rekabet edecek bir ürün üretmek amacıyla kullanamaz ve sadece kullanıcının talep ettiği hizmeti sağlamak için gerekli olduğu durumlarda diğer taraflara sunabilmektedir. Ayrıca, tüketici olan bir kullanıcının verileri başka taraflara sunmasını engellemek de yasaktır.

Bağlanabilir araçlarda veri işleme dayanağının sözleşmenin ifası olması gerektiği, hem kullanıcı deneyimi ve güvenliği açısından hem de yasal ve düzenleyici uyumluluk açısından önemlidir. Bu yaklaşım, veri işlemenin etkin ve kesintisiz bir şekilde devam etmesini sağlarken, aynı zamanda kullanıcıların hizmetlerden tam anlamıyla yararlanabilmesini sağlamaktadır. Bu nedenle, EDPB'nin Rehber'deki yaklaşımının aksine, veri koruma mevzuatlarında yer alan hukuki sebeplerin, otomotiv sektörü özelinde hazırlanan mevzuat ve rehberler ile uyumlandırılması ve rızaya gereğinden fazla odaklanmak yerine, sözleşmenin ifası gibi diğer yasal dayanakların da veri işleme faaliyetleri bakımından temel alınması gerekmektedir.

2.6. İLGİLİ KİŞİ HAKLARI

Bağlanabilir araçlar, araç sahipleri, sürücüler, araç yolcuları gibi ilgili kişilere ait kimlik ve iletişim verileri, araç kimlik numarası veya araca ait diğer bilgiler, konum verileri, araç sürücüsünün biyometrik verileri, araç sürücüsü ve yolcuları hakkında aracın kullanımından kaynaklı verileri ve araca ilişkin teknik verileri işleyerek ilgili kişiler hakkında önemli miktarda veri toplanmasını sağlayarak otomobil sektöründe esaslı bir değişim yaratmıştır. İşlenen bu veriler her ne kadar araç üreticilerine ve hizmet sağlayıcılara yeni hizmetler sunma ve kullanıcı deneyimini geliştirme imkanı sunsa da, ilgili kişilerin haklarının korunması veri sorumluları için kritik bir

öneme sahiptir. Bu bakımdan, bağlanabilir araçlarda işlenen kişisel verilere ilişkin olarak KVKK ve GDPR’da ilgili kişilere kapsamlı haklar tanımaktadır.

Araç üreticileri ve katma değerli hizmet sağlayıcılar gibi veri sorumluları, ilgili kişilerin; kendileri ile ilgili kişisel verilerin işlenip işlenmediğini öğrenme ve işlenmesine dair bilgi talep etme, verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, verilerin içeriği eksik veya hatalı ise bu verilerin düzeltilmesini talep etme, hukuka aykırı veri işleme yapılması halinde verilerin silinmesini, yok edilmesini, anonim hale getirilmesini ve buna göre yapılan işlemlerin ilgili kişinin verilerinin paylaşıldığı üçüncü taraflara bildirilmesini talep etme, otomatik sistemler vasıtasıyla analiz sonucu kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, maruz kaldığı zararın giderilmesini talep etme gibi haklarını¹⁵² kullanmaları için etkili bir yol sağlayan belirli araçların uygulanması yoluyla, ilgili kişilerin tüm veri işleme faaliyetleri süresince kişisel verileri üzerindeki kontrolünü kolaylaştırmalıdır. “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik”¹⁵³ kapsamında kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi konusundaki esaslar düzenlenmektedir. KVKK’nın 11. maddesinde ilgili kişilere kişisel verilerinin içeriği eksik veya hatalı ise bu verilerin düzeltilmesini talep etme hakkı tanınmıştır. Düzeltme hakkı, kişisel verilerin doğru ve gerektiğinde güncel olma ilkesine dayanan bir sonuçtur. İlgili kişiler, işlenen kişisel verilerinin doğruluğunu periyodik olarak kontrol etme hakkına sahiptir¹⁵⁴. Unutulma hakkı kavramını hukuk dünyasına sokan Avrupa Birliği Adalet Divanı’nın (“ABAD”), Google Spain kararında¹⁵⁵ kişisel verilerin işleme amacı bakımından yetersiz, amaçla bağlantısız olması veya işleme amacını aşması, işlenen

¹⁵² **Kişisel Verileri Koruma Kurumu**, İlgili Kişinin Hak Arama Yöntemleri, Ankara, Nisan, 2018, s.2. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/353d85d5-87df-4c91-b08e-b4f0991a80f4.pdf> (e.t. 21.05.2024).

¹⁵³ RG T. 28.10.2017, S. 30224.

¹⁵⁴ **Buse Doğan**, Kişisel Verilerin İşlenme Şartları Bağlamında Açık Rıza, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, İstanbul, 2019 (Yayımlanmamış Yüksek Lisans Tezi).

¹⁵⁵ AAD kararları için bkz. <https://curia.europa.eu>. 13.05.2014 tarihli ve C-131/12 sayılı kararı.

verilerin güncellenmemesi ve veri işleme faaliyeti için gerekli olan saklama süresini aşarak gereğinden uzun tutulması gibi nedenlerle ilgili kişinin veri silme talebinde bulunabileceği vurgulanmıştır¹⁵⁶.

İlgili kişi tercihlerinin yansıtılması adına veri sorumluları, veri kayıt sistemlerine ayar değişikliklerini kolaylaştırmak ve araç sahibi / sürücülerin tercihlerini saklamak ve gizlilik ayarlarını istedikleri zaman kolayca değiştirmelerine yardımcı olmak amacıyla bir profil yönetim sistemi kurmalıdır. Profil yönetim sistemi, özellikle ilgili kişinin talebi üzerine kişisel verilerin bağlanabilir araç sistemlerinden erişimini, silinmesini ve kaldırılmasını kolaylaştırmak adına her veri işleme için tercihlerin yansıtılmasına imkan tanımalıdır. Araç sahibi / sürücülerin, veri sorumlusunun kişisel verilerini toplamaya devam etmek için dayanabileceği hukuki sebebi olmadığı sürece, belirli kişisel veri kategorilerinin toplanmasını geçici veya kalıcı olarak herhangi bir anda durdurabilmeleri mümkün olmalıdır. İlgili kişiler tarafından rızanın geri alınmasına ilişkin tercihler öncelikli olarak bağlanabilir araç ekranları üzerinden veya bağlanabilir araç mobil uygulaması gibi araçlar vasıtasıyla yansıtılabilmelidir. EDBP de ilgili kişilerin bağlanabilir araç ekranlarında saklanabilen GPS navigasyon geçmişi, web geçmişi gibi kişisel verilerinin hızlı ve kolay bir şekilde silmelerine olanak tanımak için araç üreticilerinin silme düğmesi gibi basit bir mekanizma sunmasını önermektedir¹⁵⁷.

Açık rıza hukuki sebebi ile sürüş davranışına dayalı olarak kişiselleştirilmiş tekliflerin sunulduğu hizmetlerde, ilgili kişinin rızasını geri almasını takiben verilerin veri sorumlusu tarafından profillemeye amacıyla işlenmesinin durdurulması halinde araç sahibi / sürücüsünün standart hizmet sözleşmesi kapsamında hizmet almaya devamı temin edilmelidir.

¹⁵⁶ **Kişisel Verileri Koruma Kurumu**, Unutulma Hakkı (Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi), Ankara, Ekim, 2021, s.10. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/11b6fd99-d42a-45b1-a009-21f2d36ded21.pdf> (e.t. 21.05.2024).

¹⁵⁷ Rehber, s. 23.

Bağlanabilir aracın satışı ve araç sahiplik değişikliği durumunda, ilgili kişinin daha önce belirtilen amaçlar için artık gerekli olmayan kişisel verilerinin silinmesini talep etme hakkını kullanabilmesi sağlanmalıdır. Bu kapsamda veri sorumluları, araç sahiplik değişimi sırasında ilgili kişilerin veri silme hakkını kullanmalarına yardımcı olarak, taleplerini iletmeyi kolaylaştıran prosedürler oluşturmaktadır. KVKK'da yer almamakla birlikte GDPR'ın 20. maddesinde düzenlenen veri taşınabilirliği hakkı, Rehber'de ilgili kişiler için tanınan haklar arasında sayılmaktadır¹⁵⁸. GDPR ile yasal olarak güvence altına alınan veri taşınabilirliği hakkı, bireylerin kendi verileri üzerindeki kontrolünü güçlendirmeyi amaçlamaktadır. Bu hak sayesinde ilgili kişiler, kişisel verilerini bir veri sorumlusundan diğerine kolayca aktarabilmektedir. Veri taşınabilirliği hakkının ilgili kişilere dört ana fayda sağlayabileceği öngörülmektedir: (i) Kişisel veri transferleri üzerinde kontrol sağlanması, (ii) kişisel verilerin yeniden kullanılmasına veya başka amaçlarla kullanılmasına imkân tanınması, (iii) veri akışlarının daha iyi anlaşılması ve (iv) kişilerin çevrimiçi kimlikleri üzerinde daha fazla kontrol sahibi olması ile eşitliğin sağlanması. Bu dört fayda sayesinde veri taşınabilirliği hakkı, veri işleme süreçlerinin şeffaflığını artırmakta ve ilgili kişilerin çevrimiçi kimliklerini daha iyi yönetmelerine yardımcı olmaktadır¹⁵⁹. Veri taşınabilirliği hakkının KVKK kapsamında gelecekte nasıl şekilleneceği henüz tam olarak netlik kazanmamış olsa da ilgili kişi dijital kimliklerinin veri sorumluları tarafından nasıl işleneceği hususunda önemli bir uygulama olacaktır.

Dijital kimlikler, farklı platformlarda kullandığı verilerin birer birikimi olarak ilgili kişi varlığı ve kimliğini dijital ortamda temsil eden bilgiler olarak tanımlanmaktadır. İlgili kişi, verilerini işleyen platformu değiştirmek istediğinde dijital kimliklerinin kaybolma riski, ilgili kişinin mevcut platformlara bağlı kalmasına sebep olmaktadır. Veri taşınabilirliği hakkı bu noktada devreye girerek,

¹⁵⁸ Rehber, s. 23.

¹⁵⁹ **Helena Ursic**, *Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control*, SCRIPTed: Journal of Law, Technology and Society, Sayı. 15, 2018, s. 44, 45. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://script-ed.org/wp-content/uploads/2018/08/ursic.pdf?d=05232024> (e.t. 21.05.2024).

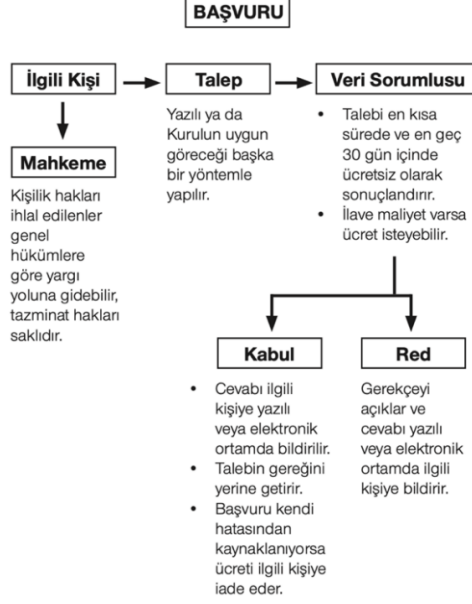
dijital kimliklerin taşınabilirliğini sağlayarak ilgili kişilerin platform tercihlerinin özgürleşmesi ve verileri üzerindeki kontrolün artmasını amaçlamaktadır. Bu sayede, kişisel veri güvenliğinin temin edilmesinin yanında veri sorumluları arasındaki adil rekabetin korunması da mümkün olacaktır. İlgili kişilerin kişisel verilerini tercih ettikleri platformlarda kullanma özgürlüğüne imkân tanıyan veri taşınabilirliği hakkı, veri transferleri üzerinde kontrol sahibi olunmasını ve verilerin yeniden kullanılmasını sağlayarak, dijital dünyada eşitliğin sağlanması bakımından önemli olmaktadır¹⁶⁰.

KVKK'nın 11. maddesinde sayılan haklarını kullanmak isteyen ilgili kişiler için KVKK'da veri sorumlusuna başvuru usulleri iki temel kategoriye ayrılmıştır; yazılı başvuru ve elektronik başvuru. Yazılı başvuru, ıslak imza içeren belge ile yapılan başvuruyu ifade ederken, güvenli elektronik imza ile imzalanan belgeler de yazılı başvuru kapsamında değerlendirilmektedir. Elektronik başvuru ise veri sorumlusunun belirlediği mobil imza, güvenli elektronik imza, KEP, kurumsal mail adresi gibi elektronik ortamlar üzerinden gerçekleştirilmektedir. Veri sorumluları, ilgili kişilerin başvurularını en kısa sürede ve en geç 30 gün içinde ücretsiz olarak sonuçlandırmak zorundadır. Başvurunun kabul edilmesi halinde, veri sorumlusu talebin gereklerini doğrudan ve derhal yerine getirmek zorundadır. Veri sorumlusu için gerekçeli olarak ret kararı verme imkânı da mevcut olup bu durumda veri sorumlusu, red kararının gerekçesini açıklamakla yükümlüdür. Veri sorumlusu, kendisine yapılan başvurulara dair kararını, ilgili kişinin başvurduğu yöntem aracılığıyla bildirmelidir¹⁶¹.

¹⁶⁰ **Beste Yılmaz**, Kişisel Verilerin Korunması ve Rekabet Hukuku Bağlamında Veri Taşınabilirliği Hakkı, On İki Levha Yayıncılık, İstanbul, 2023, s. 12, 13. (e.t. 06.04.2024).

¹⁶¹ İlgili Kişinin Hak Arama Yöntemleri, s. 4, 5. (e.t. 21.05.2024).

Şekil 2. 3. Veri Sorumlusuna Başvuru Usulü¹⁶²



2.7. KİŞİSEL VERİ AKTARIMI

Bağlanabilir araçlar, araç sürücüleri ve yolcuları hakkında önemli miktarda veri toplayarak veri işleme faaliyeti yürütmektedir. Fakat bu veri akışı, kişisel veri gizliliği ve güvenliği açısından önemli riskleri de beraberinde getirmektedir. Araç sahibi, sürücüleri ve yolcularının, araç içinde veya araç vasıtasıyla toplanan verilerin işlenmesi ve üçüncü taraflara aktarımı hakkında bilgilendirilmesi gerekmektedir. Bu bilgilerin sadece araç sahibine iletilmesi ve araç sürücüsü ve yolcuların aydınlatılmaması veya zamanında bilgilendirilmemeleri söz konusu riskler arasındadır. Verisi işlenen ilgili kişilerin zamanında ve uygun şekilde bilgilendirilmemeleri, haklarını kullanma konusunda engel teşkil etmektedir. Aracın sahipliğinin değiştiği hallerde, örneğin, aracın satılması veya kiralanması ile birden fazla kişiye ait olduğu durumlarda yeni araç sahibi veya kiralayanın, bağlanabilir araçtaki veri işleme faaliyetleri hakkında bilgi sahibi olması

¹⁶² Kaynak: İlgili Kişinin Hak Arama Yöntemleri, s. 12. (e.t. 21.05.2024).

gerekmektedir. Bir diğer risk ise veri aktarımının yeni araç sahibi / sürücüsü ilgili kişinin rızası veya bilgisi olmadan otomatik ve varsayılan olarak devam etmesidir.

2.7.1. Üçüncü Taraflara Veri Aktarımı Yapılması

Kişisel veri gizliliği ve güvenliğinin sağlanması adına prensip olarak, bağlanabilir araç vasıtasıyla üretilen kişisel verilere yalnızca araç üreticisi ve hizmet sağlayıcılar gibi veri sorumlularının ve verisi işlenen ilgili kişilerin erişmesi gerekmektedir. Ancak veri sorumlusu, kişisel verileri veri minimizasyonu ilkesini gözeterek ve gerekli teknik ve idari tedbirleri sağlayarak belirli amaçlarla KVKK'nın 8. maddesinde sayılan açık rızanın varlığı veya açık rıza aranmaksızın KVKK'nın 5/2. maddesinde ve yeterli önlemler alınmak kaydıyla, KVKK'nın 6/3 maddesinde belirtilen hukuki sebeplerden birine dayandığı ölçüde üçüncü taraflara aktarmaktadır. Bağlanabilir araçta işlenen kimliği belirleyici bilgiler, iletişim bilgileri, ödeme bilgileri gibi araç sahibi / sürücüsü işlem verileri ile araç tarafından üretilen kişisel veriler, sürüş alışkanlıkları, konum verileri vb. araç kullanım verilerinin veri sorumluları tarafından üçüncü taraflara aktarımından önce, aktarıma dayanılan hukuki sebebin tespit edilmesi ve özellikle ek hizmetlerin sunulduğu hallerde ilgili kişinin açık rızasının alınması gerekmektedir. EDPB, kişisel verileri veri sorumlusu olarak hareket eden üçüncü bir tarafa aktarmadan önce ilgili kişinin rızasının sistematik olarak, örneğin, önceden işaretlenmemiş bir onay kutucuğunu işaretleyerek veya teknik olarak mümkün olduğunda, ilgili kişinin araçtan erişebileceği fiziksel bir cihaz kullanılarak alınmasını önermektedir¹⁶³. Kişisel verilerin aktarıldığı üçüncü taraf, kişisel verilerin işlenmesine ilişkin kararları almaya, kişisel verilerin işlenme amacını ve yöntemini belirlemeye başladığında ve verileri kendi elektronik veya fiziki veri kayıt sistemine kaydettiğinde ayrı bir veri sorumlusu olarak KVKK kapsamında yükümlü olacaktır¹⁶⁴.

¹⁶³ Rehber, s. 25.

¹⁶⁴ **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Ankara, Aralık, 2018, s.57. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF> (e.t. 22.05.2024).

Bağlanabilir araçlarda mümkün oldukça verilerin araçta muhafaza edilmesi ve yerel veri işlemenin olması teknik tedbiri ile araç üreticisi ve hizmet sağlayıcılar gibi veri sorumlularının kişisel verileri araç dışına aktarmadan işlemeye yönelik süreçleri geliştirmesi gerekmektedir. Bu şekilde ilgili kişilerin kişisel verilerinin tek yerden kontrolü mümkün olmaktadır. Araç üreticileri ve hizmet sağlayıcılar gibi veri sorumlularının, verileri bulutta depolamaması, “tasarım gereği” ilgili kişinin verilerini bilgisi dışında üçüncü taraflara aktarmaması daha az gizlilik ve siber güvenlik riski barındıracaktır. Bağlanabilir araç dışına çıkmasının gerektiği hallerde, veri aktarımından önce kişisel verilerin anonim hale getirilmesi alınabilecek teknik tedbirlerden biridir. EDPB görüşüne göre¹⁶⁵, veri koruma mevzuat ilkeleri kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyen veya ilgili kişinin kimliğinin belirlenmesi veya tekrar tanımlanması mümkün olmayan anonim bilgiler için geçerli değildir. Bu nedenle, anonimleştirme veri sorumluları tarafından belirli durumlarda bağlanabilir araçlardaki veri aktarım risklerini azaltmak amacıyla başvurulacak bir yöntem olarak değerlendirilmelidir¹⁶⁶.

Bağlanabilir araçlarda kişisel veri aktarım tarafları ve amaçları aşağıdaki şekilde sıralanmaktadır:

- Yol yardım hizmetleri, şikâyet ve taleplerin takibi amaçlarıyla çağrı merkezi hizmeti sağlayıcıları gibi üçüncü taraf hizmet sağlayıcılara aktarım yapılmaktadır.
- Araç teşhisi, bakım ve onarımı, yol yardım süreçleri, bayi/servis randevusu alma amaçlarıyla yetkili servisler ve bayilere aktarım yapılmaktadır.
- Saklama faaliyetleri, teknik altyapı hizmetinin sunulması amaçlarıyla veri merkezleri, bulut bilişim platformları gibi bulut tabanlı hizmet sağlayıcılara

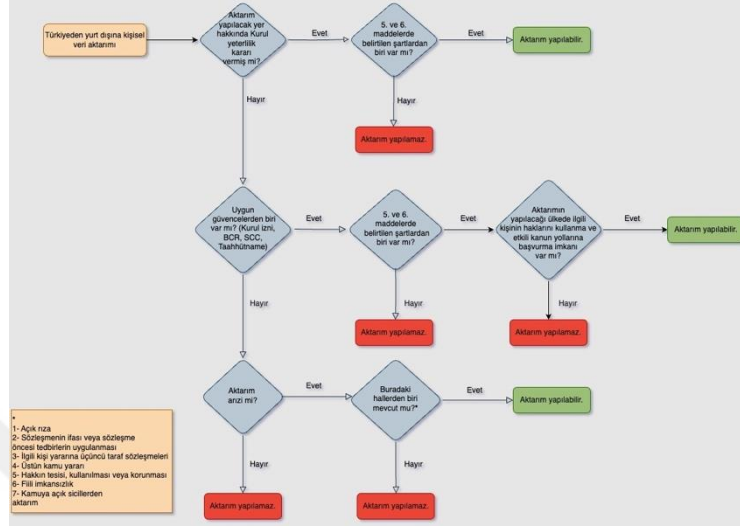
¹⁶⁵ Rehber, s. 20.

¹⁶⁶ Çuhadaroglu, s. 81.

aktarım yapılmaktadır.

- Ürün ve hizmet geliştirme, yatırım kararları, ürün planlama amaçlarıyla veri sorumlusunun danışmanları, hissedarları, iş ortakları, iştirakleri ve bağlı ortaklıklarına aktarım yapılmaktadır.
- Araç sigorta süreçlerinin yürütülmesi kapsamında sigorta işlemlerinin yapılması amacıyla sigorta şirketlerine aktarım yapılmaktadır.
- Bağlanabilir araç faaliyetlerinin yürütülmesi, ağ gereksinimlerinin kontrolü amaçlarıyla telekomünikasyon firmalarına aktarım yapılmaktadır.
- Faaliyetlerin yürürlükteki mevzuata uygun yürütülmesi, hukuk işlerinin takibi ve savunma hakkının kullanılması ile yetkili kurum ve kuruluşlara bilgi temini amaçlarıyla bakanlıklar, mahkemeler, icra daireleri, avukatlar gibi yetkili kamu kurumları ve özel kişilere aktarım yapılmaktadır.
- Sunulan müşteri hizmeti ve kullanıcı deneyiminin iyileştirilmesi amacıyla satış ve pazarlama ortakları, müşteri hizmetleri sağlayıcıları gibi yetkili iş ortaklarına aktarım yapılmaktadır.
- Ürün ve hizmetlerin optimizasyonu ve geliştirilmesi, daha iyi ve daha çeşitli hizmetler sunmak amaçlarıyla yazılım geliştirme firmaları, veri analizi şirketleri gibi tedarikçiler veya hizmet sağlayıcılara aktarım yapılmaktadır.
- Ürün veya hizmetlerin işlevselliğini ve sabitliğini sağlamak, daha fazla hizmet ve fonksiyona erişim imkânı sunmak amaçlarıyla haritalama hizmeti sağlayıcıları, ödeme işlemcileri gibi üçüncü taraflara aktarım yapılmaktadır.
- Hizmet şartlarını ihlal araştırması, dolandırıcılık ve diğer güvenlik risklerini tespit ve önleme amaçlarıyla avukatlar, siber güvenlik firmaları gibi üçüncü taraflara aktarım yapılmaktadır.

Şekil 2. 4. KVKK m.9 Yurt Dışına Veri Aktarım Yöntemleri



2.7.2. Yurt Dışına Veri Aktarımı Yapılması

Kişisel verilerin sayılan amaçlarla yurt dışındaki üçüncü taraflara aktarımının uygun olduğu haller KVKK'nın 9. maddesinde ayrıca düzenlenmektedir. KVKK'nın yürürlüğe giren ilk hali ile 9. maddenin GDPR ile uyumlu olmaması ve AB ile kurulan yakın ilişkiler dikkate alındığında, ilgili maddede değişiklik yapılması gerekliliği doğmuştur. Nitekim, AB Adli İş birliği Teşkilatı ("EUROJUST") ve AB Polis Teşkilatı ("EUROPOL") kurumları ile kurulacak ortaklıklarda ve AB Vize Muafiyeti Yol Haritası'nda Türkiye'de AB standartlarında bir kişisel verileri koruma mevzuatının geliştirilmesine yönelik beklenti yer almaktadır¹⁶⁷. Bu bakımdan 2021 yılında yayımlanan "İnsan Hakları Eylem Planı"¹⁶⁸, "Ekonomi Reformları Eylem Planı"¹⁶⁹ ile "2024-2026 Orta Vadeli

¹⁶⁷ **Berna Akçalı Gür**, "Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 25/2 (Aralık 2019), s.869. İlgili makaleye internet üzerinden şu link ile ulaşılabilir: <https://dergipark.org.tr/tr/download/article-file/902576> (e.t. 23.05.2024).

¹⁶⁸ İnsan Hakları Eylem Planı, 6.7.a. numaralı faaliyet planı. İnternet üzerinden şu link ile ulaşılabilir:

https://insanhaklarieylemplani.adalet.gov.tr/resimler/%C4%B0nsan_Haklar%C4%B1_Eylem_Plan%C4%B1_ve_Uygulama_Takvimi.pdf (e.t. 23.05.2024).

¹⁶⁹ Ekonomi Reformları Eylem Planı, 7.3.g. numaralı eylem planı. İnternet üzerinden şu link ile ulaşılabilir: <https://ms.hmb.gov.tr/uploads/2021/03/Ekonomi-Reform-Takvimi.pdf> (e.t. 23.05.2024).

Program”’da¹⁷⁰ KVKK’nın GDPR uyarınca güncellenmesine yönelik hedefe yer verilmiştir¹⁷¹.

Açıklanan gereklilikler neticesinde, KVKK’nın 9. maddesinde de değişiklik hükmü içeren Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun¹⁷² Resmî Gazete’de yayımlanmıştır. Yapılan değişiklik ile kişisel verilerin yurt dışına aktarımında kademeli ve alternatifli bir aktarım rejimi¹⁷³ getirilmiştir. Yeni haliyle kişisel verilerin yurt dışına aktarılması için; (i) yeterlilik kararına dayalı aktarım, (ii) uygun güvencelere dayalı aktarım ve (iii) arızı durumlara dayalı aktarım olarak üç farklı alternatif bulunmaktadır.

Bağlanabilir araçlarda işlenen kişisel verilerin sayılan üçüncü taraflara aktarımında kişisel verinin yurt dışına çıkması halinde yaşanabilecek gizlilik ve güvenlik sorunlarının göz önünde bulundurulması gerekmektedir. Bu bakımdan Bilgi Teknolojileri ve İletişim Kurumu’nun (“BTK”) 22.01.2018 tarih ve 2018/DK-YED/27 sayılı kararı¹⁷⁴ önemlidir. İlgili kararda BTK güvenlik gerekçeleri nedeniyle bağlanabilir araçlarda katma değerli servislerin kullanılmasının uygun olmadığını karara bağlamış olup ilgili kararda gerekçe olarak araçlarda katma değerli hizmetlerin sunulması için haberleşme sistemlerinde kullanılan SIM kartlarının Türkiye’de mobil elektronik haberleşme hizmeti sunmak üzere yetkilendirilmiş işletmecilerden temini, ilgili işletmecilerce kontrol edilebilir olarak programlanması ve verilerin Türkiye’deki sunucularda tutulması gerekliliği yer almaktadır. BTK ilgili kararını 2022 yılında gözden geçirerek bağlanabilir araçlarda katma değerli hizmetlerin kullanımına imkân tanıyan yeni bir düzenlemeye imza atmıştır. İlgili düzenleme ile bağlanabilir araç üreticilerinin katma değerli

¹⁷⁰ Orta Vadeli Program, “Uluslararası Normlara Uygun, Şeffaf ve Öngörülebilir Düzenlemeler” başlıklı eylem planı. İnternet üzerinden şu link ile ulaşılabilir: https://www.sbb.gov.tr/wp-content/uploads/2023/09/Orta-Vadeli-Program_2024-2026.pdf (e.t. 23.05.2024).

¹⁷¹ **Kaya**, KVKK Reformu, s. 99.

¹⁷² RG T. 12.03.2024, S. 32487.

¹⁷³ **Kaya**, KVKK Reformu, s. 30.

¹⁷⁴ 22.01.2018 tarih ve 2018/DK-YED/27 karar numaralı Bilgi Teknolojileri ve İletişim Kurulu Kararı, 112 Tabanlı Araç İçi Acil Çağrı Sistemi (E-Call). İlgili karara internet üzerinden şu link ile ulaşılabilir: <https://www.btk.gov.tr/uploads/boarddecisions/112-tabanlı-arac-ici-acil-cagri-sistemi-e-call/027-05-112-tabanlı-arac-ici-acil-cagri-sistemi-e-call-22-01-2018.pdf> (e.t. 17.03.2024).

hizmetleri sunması için BTK'ya başvuruda bulunması gerekmektedir. Yapılan başvuruları takiben BTK'nın araç üreticilerinin sistemlerini test ederek uygun bulunan araç üreticilerinin bağlanabilir araca bağlı hizmetleri sunmasına onay vereceği düzenlenmektedir. Düzenlemeye göre bağlanabilir araçlarda ilgili katma değerli hizmetleri sunmak isteyen araç üreticilerinin Türkiye'de faaliyet gösteren bir internet servis sağlayıcıdan hizmet alması ve BTK'nın sunucuların erişimini açma ve kapatma kontrolüne sahip olması gerekmektedir. Ayrıca BTK'nın bağlanabilir araçlarda ve araç iletişim sistemlerinde kullanımının yaygın olacağı eSIM sistemlerine ilişkin "Uzaktan Programlanabilir SIM Teknolojileri ("eSIM") Kurul Kararı"¹⁷⁵ ile eSIM sistemlerindeki veriyi içeren sunucuların Türkiye'de barındırılmasına ve uluslararası dolaşım hizmetlerinin amaca uygun kullanımına yönelik hükümler belirlenmiştir¹⁷⁶.

¹⁷⁵ BTK'nın 12.02.2019 tarihli ve 2019/DK-TED/053 sayılı ilgili kararına internet üzerinden şu link ile ulaşılabilir: <https://www.btk.gov.tr/uploads/boarddecisions/uzaktan-programlanabilir-sim-teknolojileri-esim/053-2019-web.pdf> (e.t. 17.03.2024).

¹⁷⁶ Çuhadaroğlu, s. 121.

ÜÇÜNCÜ BÖLÜM

BAĞLANABİLİR ARAÇLARDA KİŞİSEL VERİ GÜVENLİĞİ

3.1. BAĞLANABİLİR ARAÇ TEKNOLOJİLERİNİN KULLANILMASINDAKİ RİSKLER

Bağlanabilir araçlar, araç kullanım ve sürüş deneyimini iyileştiren hizmetleri araç sürücülerine sunarken internete ve diğer araçlara bağlanarak başta araç sürücülerini olmak üzere araçta yolculuk eden diğer kişilere ilişkin kişisel verileri işlemektedir. Bu veri işleme faaliyeti ise veri gizliliği ve güvenliği açısından bazı riskler barındırdığından bu alanda çeşitli yasal düzenlemelerin getirilmesine ve mevcut mevzuat düzenlemelerinin de bağlanabilir araç teknolojilerini regüle etmesine zemin oluşturmaktadır.

Gelinen noktada bağlanabilir araçların kullanımında giderek artan miktarda veri işlenmesi ile artık bir araç kullanmanın da ötesinde bir bilgisayar kullanıldığı kabul edilmektedir¹⁷⁷. İşlenen verilerin niteliği incelendiğinde ise araç bilgilerinin yanı sıra özellikle araç sürücüsünü belirleyen veya belirlenebilir kılan verilerin mevcut olması nedeniyle ilgili veriler gerek KVKK gerek GDPR kapsamında kişisel veri olarak değerlendirilmektedir.

Bağlanabilir araçlarda yoğun olarak kişisel veri işlenmesi sebebi ile veri koruma otoriteleri bu alanı ve veri işleme faaliyetlerini düzenleyici incelemeler yapmaya ve görüşlerini paylaşmaya başlamıştır. EDPB tarafından 28 Ocak 2020 tarihinde taslak olarak görüşe açılan Bağlanabilir Araçlar Kapsamında Kişisel Verilerin İşlenmesine İlişkin Rehber¹⁷⁸ bu alanda yayımlanan en önemli kaynaklar arasındadır. Uzun süre beklenen Rehber, görüşe sunulan taslak versiyona gelen çok sayıda yoruma rağmen taslak hali ile neredeyse aynı olarak 9 Mart 2021 tarihinde yayımlanmıştır. Rehber’de bağlanabilir araçlarda kişisel verilerin işlenmesi

¹⁷⁷<https://www.dataguidance.com/opinion/eu-edpb-issues-guidelines-connected-vehicles> (e.t. 05.03.2024).

¹⁷⁸ Rehber. İlgili rehber internet üzerinden şu link ile ulaşılabilir: https://www.edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf (e.t. 10.03.2024).

kapsamındaki devam eden bölümlerde detaylı şekilde bahsedilen potansiyel riskler de ele alınmaktadır.¹⁷⁹

3.1.1. IoT Sistemlerinin Uygun Kullanılmaması

Nesnelerin interneti (“IoT”) sistemleri hakkında bağlanabilir araç teknolojisinde de geçerli olacak uygulamada karşılaşılan veri güvenliği ve kontrolü konuları hakkında Madde 29 Çalışma Grubu¹⁸⁰ tarafından sakıncalar dile getirilmiştir. Madde 29 Çalışma Grubu tarafından yayımlanan görüşte¹⁸¹ cihaz üreticilerinin IoT teknolojisi kullanımında gizlilik, bütünlük ve kullanılabilirlik önlemlerinin uygulanmasının, nesneler ve sensörler tarafından kullanılacak ve veri işlemeye dayanan hesaplamaların en iyi hale getirilme ihtiyacı ile nasıl dengelenecekleri hususu netleşmesi gereken bir konu olarak ele alınmaktadır. IoT’nin uygulama alanı ve ekonomik etkisi hızla büyürken 2025 yılında internete bağlı cihazların sayısının 50 milyara ulaşması beklenmektedir¹⁸². Bu nedenle, IoT ile gündelik bir nesnenin, potansiyel bir gizlilik ve bilgi güvenliği ihlaline sebebiyet verebilecek bir uygulamaya dönüşmesi ve bu kullanımın internetin doğrudan kullanıldığı versiyondan çok daha geniş bir alana veri yayma riski bulunduğu vurgulanmaktadır. Bağlantılı cihazlarda gözetleme faaliyetlerinin kolaylaşması, kişisel verilerin çalınması veya tehlikeye atılmasıyla sonuçlanan veri ihlalleri de dahil olmak üzere olası güvenlik sorunları, ilgili kişilerin IoT’nin güvenliğine ilişkin algısı üzerinde olumsuz etkileri olabilecek potansiyel olarak etkili yeni saldırı yollarına da kapı

¹⁷⁹ Rehber’de bağlanabilir araçlarda kişisel verilerin işlenmesi kapsamındaki potansiyel risklerle ilgili olarak s. 13-15 arasında ayrıntılı analizlere yer verilmiştir. İlgili rehber internet üzerinden şu link ile ulaşılabilir: [edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en](https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en) (e.t. 10.03.2024).

¹⁸⁰ Madde 29 Çalışma Grubu (the Article 29 Working Party), 95/46 sayılı Direktifin 29. maddesine göre kurulan ve 25 Mayıs 2018 tarihine kadar (GDPR’in uygulamaya girmesi) gizlilik ve kişisel verilerin korunmasına ilişkin konularla ilgilenen bağımsız bir danışma kuruludur. İlgili tanıma internet üzerinden şu link ile ulaşılabilir: https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en (e.t. 10.03.2024).

¹⁸¹ **Madde 29 Çalışma Grubu**, Opinion 8/2014 on the on Recent Developments on the Internet of Things, Eylül, 2014, s. 9. İlgili görüş internet üzerinden şu link ile ulaşılabilir: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (e.t. 10.03.2024).

¹⁸² **Acarer.**

aralamaktadır. Ayrıca, IoT cihazlarının ve platformlarının veri alışverişi yapması ve bunları hizmet sağlayıcıların altyapılarında depolaması halinde IoT'deki güvenlik uygulamaları, sadece cihazların değil, tüm ekosistemin iletişim bağlantıları ve depolama altyapısı gibi tüm bileşenlerinin de güvenliği göz önünde tutularak tasarlanmalıdır. IoT bağlamında değinilen çekinceler esasen bağlanabilir araçlar söz konusu olduğunda çok daha önemli bir hal almaktadır. Bunun esas nedeni, geleneksel olarak dış kontrollerden uzak ve korumalı olarak algılanan bir ortamda IoT uygulamalarının kullanılmasının sürüş güvenliği ve hatta araç sürücüsünün fiziksel bütünlüğünün dahi etkilenmesi endişesine yol açmasıdır.

3.1.2. Konum Verisinin Mevzuat Düzenlemelerine Uygun İşlenmemesi

Bağlanabilir araçların konum verisini işlemesi de önemli veri koruma ve gizlilik sorunlarını tartışmaya açmaktadır. Özellikle konum verisinin kullanımının araç sürücülerinin ve yolcuların takibi ve gözetlenmesi ile kötüye kullanımına yol açma potansiyeli yüksek olduğundan EDPB de Rehber'de konum verisine ilişkin veri gizliliği ve güvenliği için özel tedbirlerin uygulanması gerekliliği vurgulanmakta ve bu konuda farkındalık yaratmanın önemine değinmektedir.¹⁸³ Bağlanabilir araç verilerinin büyük bir kısmının konum tabanlı olması sebebiyle araçlardan sağlanan verilerin anonim olarak işlenmesi ve ilgili kişinin kimliğini belirli kılmasının önüne geçilmesi oldukça zordur. Araç kimlik numaraları ("VIN"), konum verileri, seyahat yönü veya yolculuğun başlangıç ve bitiş noktası gibi veriler birbirleriyle ve diğer veriler ile birleştğinde araç sürücüsü ve yolcuların belirlenebilir kılınmasına ve özel hayatlarına ilişkin çeşitli bilgilerin edinilmesine olanak sağlamaktadır.¹⁸⁴ Örneğin, araç sürücüsünün uzun süre durakladığı lokasyonlardan nerede yaşadığı, nerede çalıştığı, düzenli olarak bir sağlık kuruluşunu ziyaret edip etmediği, ilgi alanlarının neler olduğu gibi pek çok bilgiye ulaşılmaktadır. Bu bakımdan konum verileri de özellikle ilgili kişilerin alışkanlıklarını ortaya koymaktadır. Bağlanabilir

¹⁸³ Rehber, s.13.

¹⁸⁴ **Otonomo**, A Privacy Playbook for Connected Car Data, Ekim, 2019, s.15. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: https://iapp.org/media/pdf/resource_center/privacy_playbook_for_connected_car_data.pdf (e.t. 16.03.2024).

araçlarda konum verisinin işlenmesi kapsamında ülke otoritelerinin güvenlik kaygısı da olmaktadır. BTK 2018 yılından 2022 Nisan ayına kadar bağlanabilir araçlarda katma değerli hizmetlerin kullanılmasına güvenlik gerekçesi ile izin vermemekteydi. BTK ilgili kararında¹⁸⁵, telematik sistemler tarafından işlenen konum verilerinin güvenliğini ve mahremiyetini korumaya yönelik düzenlemeler getirmiştir. Bu düzenlemeler ile konum verilerinin yetkisiz erişime karşı korunmasının, sadece yetkili kişiler tarafından kullanılmasının ve yasalara uygun şekilde işlenmesinin temini hedeflenmiştir. BTK'ya göre bu sayede, milli güvenliği tehlikeye atabilecek casusluk faaliyetleri ve veri sızıntıları önlenabilmektedir.

Açıklanan sebeplerle konum verilerinin işlenmesinde uyulması gereken temel hususlar şu şekilde sıralanmaktadır¹⁸⁶:

- Konum verisinin işlenmesine ilişkin olarak araç sürücüsü, konuya özel ve ayrı olarak aydınlatılmalı ve gerekirse, örneğin yol bilgisayarı üzerinden açık rızası alınmalıdır.
- Konum verisinin işlenme amacına uygun, sınırlı ve ölçülü şekilde işlenmesi adına gerekli tedbir ve kontroller sağlanmalıdır. Bu bakımdan konum verisinin işlenmesine gerek duyulan katma değerli hizmetlerin kullanım amaçlarının da analiz edilmesi gerekmektedir. Örneğin, bir hava durumu uygulamasının ilgili kişinin rızası olsa dahi aracın konumuna her saniye erişememesi için kontrollerin sağlanması bu analizlerdendir.
- Araç sürücüsünün bağlanabilir araç konum paylaşımını herhangi bir zamanda devre dışı bırakabilmesi sağlanmalıdır.
- Konum verisi varsayılan olarak ve araç çalıştırıldığında sürekli olarak değil, yalnızca araç sürücüsü aracın konumunun bilinmesini gerektiren bir katma

¹⁸⁵ İlgili karara internet üzerinden şu link ile ulaşılabilir: <https://www.btk.gov.tr/uploads/boarddecisions/112-tabanlı-arac-ici-acil-cagri-sistemi-e-call/027-05-112-tabanlı-arac-ici-acil-cagri-sistemi-e-call-22-01-2018.pdf> (e.t. 17.03.2024).

¹⁸⁶ CNIL Rehberi, s. 25.

değerli hizmeti başlattığında etkinleştirilmelidir.

- Araç sürücüsü ekranda hareket eden bir ok gibi simgeler kullanılarak konumun etkinleştirildiği konusunda bilgilendirilmelidir.
- Konum verisinin işlenme amacı ve işlenme süresi hakkında araç sürücüsü ilgili kişi bilgilendirilmelidir.
- Konum verisinin saklanması için sınırlı bir saklama süresi belirlenmelidir.

3.1.3. İlgili Kişinin Uygun ve Eksiksiz Şekilde Aydınlatılmaması

Veri koruma mevzuatları kapsamında, ilgili kişilerin veri işleme faaliyetleri bakımından hukuk kurallarına uygun olarak bilgilendirilmeleri çok büyük öneme sahiptir¹⁸⁷. Bu bakımdan faaliyetleri kapsamında kişisel veri işleyen gerçek ve tüzel kişi veri sorumluları aydınlatma yükümlülüklerini yerine getirmelidir. Bu yükümlülüğün yerine getirildiğine dair ispat da veri sorumlusuna aittir. Tüm kişisel verilerin işlenmesinde olduğu gibi, bağlanabilir araç içinde veya aracılığıyla gerçekleşen veri işleme faaliyetleri hakkında veri sorumluları tarafından araç sürücüleri ve yolcularının yeterli şekilde bilgilendirilmesi için sunulacak aydınlatma metninde KVKK'nın 10. maddesinde sayılan aşağıdaki bilgiler yer almalıdır:

- Veri sorumlusu ve varsa temsilcisine ait kimlik bilgisi.
- Kişisel verilerin işlenme amaçları.
- Kişisel verilerin hangi taraflara ve ne amaçla aktarılabilceği.
- Kişisel verilerin toplanma yöntemi ve veri işlemenin hukuki sebebi.
- KVKK'nın 11. maddesinde yer alan ilgili kişi hakları.

¹⁸⁷ Elif Küzeci, Kişisel Verilerin Korunması, 3. Baskı, Ankara, 2019, s.218.

Aydınlatma yükümlülüğünün yerine getirilmesi adına ilgili kişi ile paylaşılması gereken bilgiler, ilgili kişiden doğrudan elde edilmesi veya edilememesi ayrımı ile GDPR’ın 13. ve 14. maddesinde düzenlenmekte olup veri sorumlularının GDPR kapsamında sayılan veri işleme faaliyetlerinde ilgili maddelerde yer alan yükümlülükleri yerine getirmesi gerekmektedir. Birden fazla veri sorumlusunun bulunduğu durumlarda ve bağlanabilir araçlarda katma değerli hizmetlerle birlikte veri işleyen yeni veri sorumluları da ilgili kişilere gerekli bilgileri sağlamalıdır. Örneğin, bağlanabilir araç ekranı vasıtasıyla araç ve araç sürücüsü verilerini işleyen araç üreticisi dışında, kullanılan katma değerli uygulama sağlayıcılar da söz konusu uygulamalarla verilerin elde edilme amaç ve vasıtalarını belirlediği takdirde veri sorumlusu olarak ilgili kişileri aydınlatma yükümlülüğü altında olacaktır.

İlgili kişileri aydınlatma yükümlülüğü yerine getirilirken söz konusu olacak bir diğer risk ise aydınlatmanın süreç özelinde doğru kişilere yapılamaması veya verisi işlenen tüm ilgili kişilerin aydınlatılmamasıdır. Örneğin, kişisel veri işlenen süreç özelinde verisi işlenen araç sürücüsüne veya yolculara karşı yapılması gereken aydınlatmanın hatalı olarak yalnızca o süreçte verisi dahi işlenmeyen araç sahibine yapılması veya aydınlatma yükümlülüğünün ilgili kişilerin kişisel verisi işlenmeden önce veya en geç ilgili kişilerle ilk temas kurulan zamanda yapılması yükümlülüğüne¹⁸⁸ aykırı şekilde ve zamanında yerine getirilememesi gibi kişisel verilerin korunması mevzuat düzenlemelerine aykırı veri işleme faaliyeti yürütülmesi riski mevcuttur. Aydınlatma yükümlülüğü yerine getirilirken ilgili kişilere detaylı aydınlatma metninin ilk aşamada sunulamayacağı durumlarda katmanlı aydınlatma yapılması da değerlendirilmektedir. Bu bakımdan ilk katmanlı aydınlatmada ilgili kişiye kişisel verilerinin elde edildiği konusunda ön bilgilendirme yapılarak ilgili kişi, KVKK’nın 10. maddesine uygun şekilde yapılacak ikinci katman aydınlatmaya yönlendirilmelidir. Aydınlatma Rehberi’nde, katmanlı aydınlatma yapılmasına yönelik örnekler arasında elektronik ortamda web

¹⁸⁸ **Kişisel Verileri Koruma Kurumu**, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi (“Aydınlatma Rehberi”), Ankara, Nisan, 2019, s.17. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/Icerik/5394/Aydinlatma-Yukumlulugunun-Yerine-Getirilmesi-Rehberi> (e.t. 17.03.2024).

sayfasında yer alan bir belgede katmanlı aydınlatma yapılması, açılan pencere [pop-up pencere] çıkması yer almaktadır¹⁸⁹. Bu bakımdan Madde 29 Çalışma Grubu tarafından da vurgulanan husus, aydınlatma metninin sözleşme hükümleri ya da genel işlem koşulları gibi hukuki belgelerden bağımsız olarak sunulması gerekliliğidir¹⁹⁰.

GDPR'ın 12. maddesi kapsamında aydınlatma yükümlülüğü, özellikle yapay zeka sistemlerinin kullanıldığı hallerde veri sorumluları açısından zorlu bir görev olmaktadır. Yapay zeka, kişisel veriler üzerinde bilinmeyen veya açıklanması zor değişkenlerle çalıştığında, işleme amaçlarını önceden belirlemek, doğrulamak veya net bilgi sağlamak her zaman mümkün olmamaktadır¹⁹¹. Kara kutu problemi olarak bilinen, yapay zeka modellerinin nasıl karar verdiğinin veya iç işleyişinin anlaşılamaması ve bu sistemlerin girdilerden nasıl bir çıktıya ulaştığının bilinmemesi durumu da bu şeffaflığı sağlama çabalarını zorlaştırmakta ve yazılım süreçlerinin izlenebilirliğini sınırlamaktadır¹⁹².

Bu bakımdan otonom ve kendi kendine öğrenen yapay zeka sistemlerinde şeffaflık ve açıklık gibi ilkelere uyum gösterilmesi, yapay zeka teknolojilerinin uygulanmasında, milyonlarca verinin işlenmesinin karmaşıklığı nedeniyle şeffaflık ilkesinin yerine getirilmesi zor olabilmektedir. Bu durum, bazı temel haklar ve GDPR hükümleri açısından riskler yaratmaktadır¹⁹³.

GDPR ve KVKK gibi veri koruma mevzuatları çerçevesinde ise şeffaflık ilkesi, özellikle veri işleme faaliyetlerinin temelinde ilgili kişinin rızasının bulunduğu durumlar için hayati öneme sahiptir. Verilerin işlenme gerekçeleri göz önüne alındığında, ilgili kişinin rızasına dayanılarak gerçekleştirilen işlemlerde veri

¹⁸⁹ Sembol kullanım yolu ile katmanlı aydınlatma yükümlülüğünün yerine getirilmesi bakımından Aydınlatma Rehberi, s.21.

¹⁹⁰ **Madde 29 Çalışma Grubu ("WP 29")**, Guidelines on transparency under Regulation 2016/679, Nisan, 2018, s.7. İlgili belgeye internet üzerinden şu link ile ulaşılabilir: <https://ec.europa.eu/newsroom/article29/items/622227> (e.t. 17.03.2024).

¹⁹¹ **Paal**, s. 292, 293.

¹⁹² Turgut Bilgiç, s. 262.

¹⁹³ **Aleksandr Kesa, Tanel Kerikmaa**, "Artificial Intelligence and the GDPR Inevitableness?", Taltech Journal of European Studies, 2020, Sayı: 10, s. 75.

sorumlusu tarafından ilgili kişinin şeffaf şekilde bilgilendirilmesi yükümlülüğü devreye girmektedir¹⁹⁴.

Bağlanabilir araçlarda işlenen kişisel verilere ilişkin olarak da araç sürücülerinin veri sorumlusunun kimliği, veri işleme faaliyetinin amacı ve işlenen veriler, varsa verilerin aktarıldığı üçüncü taraflar ve ilgili kişinin sahip olduğu haklar konularında aydınlatılması gerekmektedir. Bu bakımdan araç ekranları üzerinden veri işleme süreçleri özelinde ilgili kişi araç sürücülerinin bilgilendirilmesi sağlanmalıdır. Bunun yanı sıra konum verisi gibi işlenen verilere ilişkin araç ekranında ayrıca semboller vasıtasıyla katmanlı aydınlatma ile¹⁹⁵ işleme faaliyetinin devam ettiğine yönelik de araç sürücülerinin bilgilendirilmesi sağlanmalıdır. GDPR da şeffaflık ilkesi gereği ilgili kişiye yönelik her türlü bilginin kısa, kolay erişilebilir ve kolay anlaşılır olmasını, açık ve sade bir dil kullanılmasını ve uygun olan hallerde sembol gibi görselleştirme araçlarının kullanımını düzenlemektedir¹⁹⁶. Aynı şekilde GDPR kapsamında veri sorumlusu tarafından ilgili kişiye sunulacak bilgilerin, amaçlanan işleme faaliyetine ilişkin anlamlı bir genel bakışı kolayca görülebilir, anlaşılabilir ve açıkça okunabilir bir şekilde sunmak amacıyla standartlaştırılmış sembollerle birlikte sunulmasına işaret edilmektedir¹⁹⁷. Ancak, sembollerin kullanımının ilgili kişinin aydınlatılması için gerekli ve detaylı bilgilerin sağlanması yükümlülüğünün yerine geçmeksizin, veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmesi temin edilmelidir. Bu kapsamda GDPR'ın 12/7 maddesinde¹⁹⁸ de, GDPR 13 ve 14. maddeleri uyarınca ilgili kişilere sağlanacak bilgilerin, amaçlanan işleme faaliyetine ilişkin anlamlı bir genel bakışın kolayca görülebilir, anlaşılabilir ve açıkça okunabilir bir şekilde verilmesi amacıyla standartlaştırılmış simgelerle birlikte sağlanabileceği hükmü yer almaktadır.

¹⁹⁴ Paal, s. 293.

¹⁹⁵ Aydınlatma Rehberi, s.14.

¹⁹⁶ GDPR, Giriş, Recital 58.

¹⁹⁷ GDPR, Giriş, Recital 60.

¹⁹⁸ GDPR Art. 12/7: The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing.

Açıkça görüldüğü üzere, sembollerin kullanılmasının amacı, ilgili kişiye sunulacak detaylı yazılı bilgi ihtiyacını potansiyel olarak azaltarak ilgili kişiler için şeffaflığı artırmaktır. Bununla birlikte, sembollerin GDPR’ın 13. ve 14. maddeleri kapsamında gerekli olan bilgilerin ilgili kişilere etkili bir şekilde iletilmesindeki faydası, bu bilgiler için evrensel olarak kullanılacak ve tanınacak sembollerin / resimlerin standartlaştırılmasına¹⁹⁹ da bağlı olacaktır. Böylelikle hem araç sürücüleri hem de yolcular bağlanabilir araç kullanımı esnasında işlenen kişisel verilerine ilişkin kolaylıkla bilgi sahibi olabileceklerdir.

Bağlanabilir araçlarda veri işlenmesinin hem otomatik olarak hem de varsayılan olarak, araç sürücüsü farkında olmadan tetiklenmesi de oldukça kolaydır. Bu bakımdan araç sürücüsünün, bağlanabilir araçlar ve sunulan katma değerli hizmetler vasıtasıyla sağlanan hizmetleri ve dolayısıyla veri akışını etkili bir şekilde kontrol edememesi halinde istenmeyen yeni özelliklerin eklenmesi ile potansiyel kişisel veri işleme süreçlerinin önüne geçilmesi oldukça zor olacaktır. Şekil-3.1’de de görüleceği üzere otomotiv sektöründeki veri sorumluları bağlanabilir araçlar ile işlenen kişisel verilere ilişkin olarak sundukları detaylı aydınlatma metinlerinin yanı sıra bağlanabilir araç ekranlarında sembol gösterimi ile de araç sürücüsü ve yolcuların veri işleme faaliyetinden haberdar olmasını temin etmektedir.

¹⁹⁹ Guidelines on transparency under Regulation 2016/679, Madde 29 Çalışma Grubu, Nisan, 2018, s.25-26.

Şekil 3. 1. Bağlanabilir Araç Ekranlarında Sunulan Semboller²⁰⁰



Modemin etkinleştirildiğini ve konum haric bağli araç verilerinin iletildiğini gösterir.



Araçın konumunun iletildiğini gösterir.



Modemin etkinleştirildiğini ve hem bağli araç verilerinin hem de araçın konumunun iletildiğini gösterir.

3.2. KİŞİSEL VERİ GÜVENLİĞİ TEMEL İLKELERİ

3.2.1. Veri Minimizasyonu

Veri minimizasyonu ilkesi²⁰¹, kişisel verilerin sadece amaca uygun, sınırlı ve ölçülü olarak işlenmesini gerektirir. Bu ilke, özellikle GDPR’ın 25. maddesinde belirtilen “tasarımla veri koruma ve varsayılan ayarlarla veri koruma” (privacy by design ve privacy by default) ilkeleriyle uygulanır. Ancak, yapay zeka teknolojileri büyük miktarda veri gerektirdiğinden, bu ilke ile yapay zekanın veri talepleri arasında bir çelişki ortaya çıkmaktadır. Kişisel verilerin amaca ulaştıktan sonra silinmesi veya kısıtlanması, yapay zekanın gelişimini ve kullanımını olumsuz etkileyebilmektedir²⁰².

Avrupa Parlamentosu’nun “GDPR’ın Yapay Zeka Üzerindeki Etkileri” adlı raporu, geleneksel veri koruma ilkeleri ile yapay zeka arasındaki gerilimi kabul etmekte ve bu ilkelerin yapay zeka ve büyük veri kullanımına uyarlanması gerektiğini vurgulamaktadır. Raporda, veri minimizasyonu konusunda veri

²⁰⁰ Kaynak: Ford Otomotiv Sanayi Anonim Şirketi Kişisel Verilerin Bağlantılı Araçlar Kapsamında İşlenmesine İlişkin Aydınlatma Metni. İlgili aydınlatma metnine internet üzerinden şu link ile ulaşılabilir: <https://www.ford.com.tr/sartlar-ve-kisisel-verilerin-korunmasi/baglantili-araclar-aydinlatma-metni> (e.t. 17.03.2024).

²⁰¹ GDPR’ın 5/1-c maddesinde veri minimizasyonu; “işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlı” olarak ifade edilmektedir.

²⁰² **Boris Paal**, “Artificial Intelligence as a Challenge for Data Protection Law: And Vice Versa” The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives, Cambridge Law Handbooks, 2022, s. 295, 296.

sorumlularının, veri işleme amaçlarına göre ek amaçlardan daha önemli bir fayda sağlaması durumunda verilerin saklanması haklı gösterebileceği belirtilmektedir²⁰³.

AB'nin sıkı veri koruma mevzuatının, ABD ve Çin gibi bilgiye dayalı ekonomiler karşısında rekabeti kaybettirebileceği endişesine karşı, yapay zeka ile bireylerin sosyal ilişkilerini dengelemek, anonim veri üretmek ve profil oluşturma gibi kişisel verilere dayalı işlemlere ancak belirli koşullarda izin vermek gerektiği önerilmektedir. Ancak, “meşru menfaat” gibi belirsiz amaçların öne çıkarılması, bu konudaki dengelemelerin yeterince etkili olmayabileceğini göstermektedir²⁰⁴.

Veri minimizasyonu ilkesine uymak için, araç üreticileri, katma değerli hizmet sağlayıcılar gibi veri sorumluları, yalnızca işleme süreci ve amacıyla ilgili ve gerekli olan kişisel verileri toplayacaklarından, bağlanabilir araç üzerinden işledikleri kişisel veri kategorilerini mevzuata uygun olarak belirlemeli ve gerekli teknik ve idari tedbirleri alarak veri işleme faaliyetlerini sürdürmelidir. Örneğin, 2.3.1. başlığı altında detaylı ele alındığı üzere bağlanabilir araçta konum verilerinin işlenmesi, ilgili kişinin yaşam alışkanlıklarını ortaya koyabildiğinden özellikle sınırlı hallerde söz konusu olmalıdır. Buna göre, araç üreticileri ve katma değerli hizmet sağlayıcı gibi veri sorumlularının veri işleme amacı için kesinlikle gerekli olmadığı sürece konum verilerini toplamama konusunda süreçlerini kontrol etmeleri gerekmektedir.

Veri minimizasyonu ilkesi doğrultusunda veri sorumluları, belirlenen veri işleme faaliyeti kapsamındaki amaca ulaşabilmek için gereken asgari kişisel veri olarak tanımlanabilecek kapsamı dikkate alarak veriyi işlemekle yükümlüdür. Bu bakımdan veri sorumluları yalnızca amaçla bağlı, sınırlı ve ölçülü olan kişisel verileri işlemeli, aşkın veriyi ise zira gelecekte faydalı olabileceği gerekçesiyle veri

²⁰³ Paal, s. 47.

²⁰⁴ **European Commission**, “What does grounds of legitimate interest mean?”. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en (Erişim Tarihi: 02.08.2024).

kayıt sisteminde tutmamalıdır. Örneğin, yalnızca teknik bakım veya model optimizasyonu ile ilgili bir amaç için bağlanabilir araçların düzenli olarak ve kesintisiz şekilde ayrıntılı konum verilerinin işlenmesi veri minimizasyonu ilkesine aykırılık olarak değerlendirilmektedir²⁰⁵.

Bağlanabilir araçlarda kullanılan araç içi ve dışında yer alan sensör miktarının artması, sağlanan hizmetlere yönelik ihtiyaçların ötesinde aşırı veri toplanması riskini artırmaktadır. Örneğin, bir sigorta firmasının sunacağı araç sigortalama hizmeti için gereken araç kullanım verilerinin yanı sıra çeşitli araç sürücüsü davranış verilerini de işlemesi ve araç sahibi / sürücüsü gibi ilgili kişileri bilgilendirdiği asıl amaç dışında ikincil amaçlar için de bu verileri kullanması veri minimizasyonu ilkesine aykırılık doğuracaktır. Veri sorumlusu şirketlerin, aşırı veri toplaması, tahmin modellerini oluşturmak için makine öğrenimi ve yapay zeka ile desteklenen uygulamalarda genellikle uzun bir süre boyunca toplanan büyük veri kümelerine yol açmaktadır. Daha fazla kişisel veri toplamanın insanların davranışlarını daha doğru tahmin etmeyi sağlayacağı varsayımı, örneklem boyutunu genişletmek için veri sorumlularının büyük miktarlarda veri işlemeye yönelik sürekli bir motivasyonu olması sorununa sebep olmaktadır²⁰⁶. İlgili sorunun çözümü adına GDPR’da yer alan veri minimizasyonu ilkesinin genel veri koruma yaklaşımına uygulanması ve bu ilkenin benimsenmesi önemlidir. Bu bakımdan her ne kadar GDPR’da yer alan veri minimizasyonu tanımını KVKK’da doğrudan yer almasa da Kurul vermiş olduğu kararlarda KVKK’nın 4/1-c hükmü uyarınca kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık teşkil ettiğinde veri minimizasyonu ilkesine aykırılığın söz konusu olacağını²⁰⁷ ve kişisel

²⁰⁵ CNIL Rehberi, s. 10.

²⁰⁶ **Ayça Atabey**, “Is Google At Odds With The GDPR? Evaluation of Google’s Personal Data Collection on Mobile Operating Systems in Light of The Principles of Data Minimisation, Purpose Limitation, and Accountability”, İstanbul Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, Yüksek Lisans Tezi, İstanbul, 2019, (“Atabey”) s. 158. İlgili teze internet üzerinden şu link ile ulaşılabilir: https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=9MiDp3x86xrwjpi5-14w-Tiw6MEvWpcRXBA25_FzBfidxLYsxN3J5ZaHUG833qLb (e.t. 25.05.2024).

²⁰⁷ İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık). İlgili karara internet üzerinden şu link ile ulaşılabilir:

verilerin tasarımı mahremiyet, veri minimizasyonu ve kişisel verilerin amaca uygun ve ölçülü işlenmesi ilkelerine uygun olarak işlenmesinin önemini²⁰⁸ vurgulamaktadır.

3.2.2. Tasarımla Veri Koruma ve Varsayılan Ayarlarla Veri Koruma

Bağlanabilir araçlar ile artan kişisel veri işleme faaliyetleri, araçlar ve araçlar vasıtasıyla sunulan hizmetler ile işlenen kişisel verilerin korunması konusunu otomotiv sektörü için önemli başlıklardan biri haline getirmektedir. Bu bağlamda Tasarımla Veri Koruma (“Privacy by Design”) ve Varsayılan Ayarlarla Veri Koruma (“Privacy by Default”) ilkeleri²⁰⁹, kişisel verilerin güvenliğini ve mahremiyetini korumak için iki temel ilke olarak ele alınmalıdır.

Tasarımla veri koruma, kişisel verilerin korunmasına yönelik tedbirlerin, veri işleme faaliyetlerinin planlama ve tasarım aşamasında entegre edilmesi anlamına gelmektedir. Bu ilke, olası risklerin önceden belirlenerek proaktif bir şekilde önlemler alınmasını sağlayarak daha sağlam bir veri koruma temin etmektedir. Varsayılan ayarlarla veri koruma ise, veri işleme faaliyetlerinin yalnızca önceden belirlenmiş ve ilgili kişiye bildirilen amaçlarla sınırlı kalmasını sağlayan teknik mekanizmaların oluşturulmasını ifade etmektedir. Bu ilke, veri minimizasyonu ve amaç ile sınırlı veri işleme gibi temel ilkelerle doğrudan bağlantılı olarak, ilgili kişinin kişisel verileri üzerinde daha fazla kontrol sahibi olmasını temin etmektedir²¹⁰.

<https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik-> (e.t. 24.05.2024).

²⁰⁸ Kişisel Verileri Koruma Kurulu, “Yemek kartı hizmeti sunan veri sorumlusuna ait mobil uygulamada T.C. kimlik numarasının işlenmesi” hakkında kararı, T: 17/08/2023, K: 2023/1430. İlgili karara internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/Icerik/7782/2023-1430> (e.t. 24.05.2024).

²⁰⁹ **Nilgün Başalp**, “Avrupa Birliği Veri Koruma Genel Regülasyonu’nun Temel Yenilikleri”, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi (MÜHF HAD), 2015, Cilt.21, Sayı.1, s.92. İlgili makaleye internet üzerinden şu link ile ulaşılabilir: <https://dergipark.org.tr/tr/download/article-file/271091> (e.t. 24.05.2024).

²¹⁰ **İpek Çimen Bulut**, Avrupa Dijital Tek Pazarında Kişisel Verilerin Korunması, T.C. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Avrupa Birliği Anabilim Dalı Avrupa Çalışmaları Programı Doktora Tezi, İstanbul 2023, s. 152 (yayımlanmamış yüksek lisans tezi).

EDPB Rehber’de bağlanabilir araçlar tarafından üretilen kişisel verilerin hacmini ve çeşitliliğini dikkate alarak GDPR’ın 25. maddesi uyarınca veri sorumlusu, teknolojinin geldiği noktayı, uygulama maliyetini ve veri işleme faaliyetinin kapsamı ve amaçlarıyla beraber veri işleme faaliyetinin ilgili kişinin hak ve özgürlüklerine yönelik olarak ortaya çıkardığı farklı olasılık ve ciddiyetteki riskleri dikkate almalıdır. Veri sorumluları hem işleme faaliyetine yönelik araçların belirlenmesi sırasında hem de işleme faaliyetinin kendisi sırasında veri minimizasyonu gibi veri koruma ilkelerini etkili bir şekilde uygulamak, GDPR’ın gerekliliklerini karşılamak ve ilgili kişi haklarının temini adına gerekli güvenceleri işleme faaliyetine entegre etmek üzere tasarlanmış olan takma ad kullanımı gibi uygun teknik ve kurumsal tedbirleri uygulamalıdır.

Bu bakımdan veri sorumlusunun, tasarımla veri koruma ve varsayılan ayarlarla veri koruma yükümlülüklerini uygulayarak, bireylerin gizliliğine saygı göstermek, kişisel veri güvenliğini temin etmek ve yalnızca işleme faaliyetinin her bir özel amacı için gerekli olan kişisel verilerin işlenmesini sağlamak üzere uygun teknik ve idari tedbirleri alacak şekilde bağlanabilir araçlar bağlamında kullanılan teknolojileri yapılandırması gerektiğini belirtilmektedir. Bağlanabilir araç teknolojileri, toplanan kişisel verilerin miktarı, işlenmelerinin kapsamı, saklanma süreleri ve erişilebilirliklerini en aza indirecek, veri gizliliğini koruyan varsayılan ayarlar sağlayacak şekilde ve ilgili kişilerin aydınlatılmasını ve kişisel verileriyle ilişkili tercihlerini kolayca değiştirme seçeneğine sahip olmasını sağlayacak şekilde tasarlanmalıdır.

Tasarımla veri koruma ilkesinin faydaları arasında ilgili kişilerin haklarının ve özgürlüklerinin daha iyi korunması, kişisel veri ihlalleri risklerinin azaltılması, veri sorumlularına duyulan itibar ve güvenin artırılması ile tasarım aşamasında veri güvenliğini sağlayan yöntemlerin uygulanması ile kişisel veri işleme maliyetlerinin

düşürülmesi yer almaktadır. Tasarımla veri koruma ilkesinin uygulama adımları aşağıdaki şekilde sıralanacaktır²¹¹:

- Kişisel veri işleme faaliyetinin amacının ve kapsamının belirlenmesi.
- Potansiyel risklerin ve tehditlerin belirlenmesi.
- Uygun teknik ve idari tedbirlerin seçilmesi ve uygulanması.
- Tedbirlerin etkinliğinin düzenli olarak gözden geçirilmesi ve gerektiğinde güncellenmesi.

Varsayılan ayarlarla veri koruma ilkesi, kişisel verilerin işlenmesinde sadece gerekli olan asgari miktarın işlenmesini sağlamayı amaçlamaktadır. Bu ilke, veri işleme sürecinin tasarım aşamasında kişisel verilerin işlenmesi için gerekli olan minimum miktarın ötesine geçilmemesini sağlayan önceden tanımlanmış ayarların gerekliliklere göre belirlenmesi ile uygulanmaktadır. İşlenen kişisel veri miktarı, kişisel verilerin kapsamı, saklanma süresi ve verilere erişim yetkilerinin tespiti ilkenin uygulama alanını oluşturmaktadır. Varsayılan ayarlarla veri koruma ilkesinin uygulama adımları aşağıdaki şekilde sıralanmaktadır²¹²:

- İşleme amacının ve kapsamının net bir şekilde belirlenmesi.
- Toplanacak kişisel verilerin her birinin işleme amacı için gerekli olduğunun doğrulanması.
- Verilerin işleme süresinin ve saklanma süresinin ihtiyaç duyulan asgari düzeyde olması.

²¹¹ **Avrupa Veri Koruma Kurulu**, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Ekim, 2020, (Version 2.0). İlgili rehber internet üzerinden şu link ile ulaşılabilir: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (e.t. 25.05.2024).

²¹² Guidelines 4/2019, EDPB.

- Verilere erişim yetkilerinin sadece gerekli kişilere ve gerekli düzeyde verilmesi.
- Üçüncü taraf yazılımların kullanımda veri koruma ilkelerine uyumlu olup olmadıklarının kontrol edilmesi.

Tasarımla veri koruma ve varsayılan ayarlarla veri koruma ilkeleri tanımı KVKK'da doğrudan yer almasa da Kurul vermiş olduğu kararlarda²¹³ tasarım aşamasında yapılacak kontroller doğrultusunda, örneğin, bir web sayfasının veya mobil uygulamanın tasarım aşamasında test edilmesi ile kişisel veri gizliliği ve güvenliğinin temin edilmesinin önemini karara bağlamıştır. Bu bakımdan bağlanabilir araç ekranları ve bağlanabilir araç mobil uygulaması vasıtasıyla işlenen kişisel verilerin güvenliğinin temini adına ilgili ekranların ve arka planda sürdürülen veri işlemenin en baştan incelenmesi, ilgili kişilere ait işlenen kişisel verilerin amaçla bağlı, sınırlı ve ölçülü olduğunun temin edilmesi, gerekli alanlarda ilgili kişinin aydınlatılması ve rızasının alınması sağlanmalıdır. Araç üreticisi ve katma değerli hizmet sağlayıcı veri sorumluları, bağlanabilir aracın yaşam döngüsü boyunca veri işlerken uygun teknik ve idari tedbirleri almalıdır.

3.2.3. Anonimleştirme ve Takma Adlı Hale Getirme

Kişisel verilerin anonimleştirilmesi (“anonymization”), kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi, veri sorumlusu ve üçüncü taraflarca verilerin gizliliğini ve bütünlüğünü korumak için uygun tekniklerin kullanılması halinde bile geri döndürülemeyecek veya başka verilerle ilişkilendirilemeyecek şekilde dönüştürülmesi işlemidir²¹⁴. Kişisel verilerin takma adlı hale getirilmesi

²¹³ Kişisel Verileri Koruma Kurulu, “Bir perakende giyim firmasının veri ihlal bildirimi” hakkında kararı, T: 20/01/2020, K: 2020/50. İlgili karara internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/Icerik/7782/2023-1430> (e.t. 24.05.2024).

²¹⁴ **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi, Ankara, Mart, 2018, s.5. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/582ad48e-0a69-417f-ad9c-30cc08b7b5aa.pdf> (e.t. 25.05.2024).

(“pseudonymization”)²¹⁵ de gerçek kişiler ile ilişkilendirilemez bir veri setine dönüşmesi için başvurulmuş bir yöntemdir. Bu bakımdan veri sorumlularının kişisel verilerin anonimleştirilmesi veya takma adlı hale getirilmesi için gerekli tüm teknik ve idari tedbirleri alması gerekmektedir.

Kişisel verilerin bağlanabilir araç dışına aktarılması söz konusu olduğunda, verilerin aktarılmadan önce anonim hale getirilmesi veri sorumluları tarafından değerlendirilmelidir. Veri sorunluları anonimleştirme yolu ile imhada, yerel veri kayıt sisteminde anonim hale getirilmiş verilerin üçüncü taraflara iletilmesi halinde verilerin yeniden tanımlanmasına yol açabilecek tüm işlemleri de dikkate almalıdır. EDPB, kişisel veri koruma ilkelerinin anonimleştirilmiş verilere, yani ilgili kişinin kimliği belirli veya belirlenebilir olmayacak şekilde anonim hale getirilmiş kişisel veriler için geçerli olmayacağını yayımladığı Rehber’de²¹⁶²¹⁷ ifade etmektedir. Bir veri kümesi tamamen anonimleştirildiğinde ve ilgili kişiler artık belirli veya belirlenemez hale geldiğinde, kişisel veri koruma mevzuatında yer alan verilerin imha edilmesine²¹⁸ ilişkin veri sorumlusu yükümlülüğü yerine getirilmiş olacaktır.

Anonimleştirme ile bağlanabilir araçta işlenen verilerin özellikle üçüncü taraflara aktarımında, örneğin, bir sigorta şirketi ile yalnızca araç güvenliğine yönelik ve ilgili kişiyi belirlenebilir kılmayan araç sürüş verisi toplu şekilde istatistik amaçlı paylaşılacak istendiğinde verilerin anonimleştirilerek paylaşılması, kişisel veri güvenliği risklerini azaltmak için bir tedbir olmaktadır.

²¹⁵ **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi, Ankara, Temmuz, 2022, s.5. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/12236bad-8de1-4c94-aad6-bb93f53271fb.pdf> (e.t. 25.05.2024).

²¹⁶ GDPR’ın 26. resitali.

²¹⁷ Rehber, s. 20.

²¹⁸ Anonim Hale Getirilmesi Hakkında Yönetmelik’in “Tanımlar” başlıklı 4/1(c) maddesi kapsamında imha; “kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi” şeklinde tanımlanmaktadır.

Kurul tarafından yayımlanan rehberde anonimleştirme yöntemleri aşağıdaki şekilde sayılmaktadır²¹⁹.

- Değer düzensizliği sağlamayan anonim hale getirme yöntemleri; değişkenleri çıkartma, kayıtları çıkartma, bölgesel gizleme, genelleştirme, alt ve üst sınır kodlama, global kodlama ve örnekleme.
- Değer düzensizliği sağlayan anonim hale getirme yöntemleri; Mikro birleştirme, veri değiş tokuşu, gürültü ekleme.
- Anonim hale getirmeyi kuvvetlendirici İstatistiksel yöntemler; K-çeşitlilik, L-çeşitlilik, T-yakınlık.

Anonimleştirme yöntemleri incelendiğinde, örneğin, tüm bağlanabilir araçlardan toplanan araç kullanım verilerinin araç fonksiyonlarının iyileştirilmesi adına üçüncü taraflara aktarılacağı durumlarda veri sorumlusu araç üreticisi, VIN ve parça numaraları gibi bilgileri değişkenleri çıkartma yöntemi kullanılarak anonimleştirilmesi ile kimliği belirli veya belirlenebilir gerçek bir kişiye ait veri aktarımına neden olacak yüksek dereceli bir tanımlayıcı olmaksızın veri işleme faaliyetinin amacına ulaşacaktır. Madde 29 Çalışma Grubu da yukarıda sayılan tekniklerin de örnek alındığı anonimleştirme tekniklerine ilişkin görüşünde ayrıntılı olarak veri anonimleştirmek için başvurulması gereken çeşitli yöntemlere ve en uygun tekniğin seçilmesinin etkisine ilişkin analizlerine yer vermektedir²²⁰.

Takma adlı hale getirme, kişisel verilerin tekil olarak tanımlanmasını zorlaştırmak için kullanılan bir tekniktir. Bu işlem, verilerdeki benzersiz tanımlayıcıyı, örneğin kimlik numarası farklı bir değerle, takma ad, değiştirerek yapılmaktadır. Takma adlı hale getirilen veriler tamamen anonim hale gelmese de

²¹⁹ **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, Ankara, Mart, 2018, s.17. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf> (e.t. 25.05.2024).

²²⁰ **Madde 29 Çalışma Grubu**, Opinion 05/2014 on Anonymisation Techniques, Nisan, 2014. İlgili görüş internet üzerinden şu link ile ulaşılabilir: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (e.t. 26.05.2024).

ilgili kişilerin belirlenebilir kılınması zorlaşmaktadır. Takma adlı hale getirmede veri sorumluları, kişisel verilerdeki bir tanımlayıcıyı rastgele oluşturulan bir sayı veya ilgili kişi tarafından seçilen bir takma ad ile değiştirmekte ve şifreleme ve karmaşıklıklaştırma (“hashing”) gibi yöntemler kullanmaktadır.

Takma adlı hale getirme, kişisel verilerin anonim hale getirilmesine kıyasla daha hızlı ve kolay uygulanabilen bir yöntem olarak kişisel verilerin güvenliğini artırmaktadır. Bununla beraber, verilerin anonimleşmesini sağlamaması ilgili kişilerin hala dolaylı olarak tanımlanabilmesine yol açmaktadır. Ek olarak, farklı veri setlerinde aynı takma ad kullanıldığında ilgili kişilerin belirlenebilir kılınması gibi hatalı uygulamaların veri gizliliğini ve güvenliğini azaltma riski mevcuttur. Örneğin, saldırganın doğrudan tanımlayıcılar yerine kullanılan kodların veya takma adların kodlamasını değiştirmesi halinde ilgili kişinin kimliğini tamamen açığa çıkması söz konusu olacaktır. Bu durumda ilgili kişinin doğrudan tanımlayıcılarına ulaşılarak kimliği tamamen saptanabilir hale gelmektedir²²¹.

Açıklanan sebeplerle farklı veri setlerinde aynı takma adın kullanılmaması, takma adın tahmin edilebilir olmaması ve takma adın oluşturulma ve saklanma sürecinin güvenli olması dikkat edilmesi gereken noktalardır. Takma adlı hale getirme, güvenlik önlemleri ile desteklendiği takdirde, kötüye kullanım risklerini azaltarak kişisel verilerin korunmasını sağlamaktadır. Özetle, takma adlı hale getirme, kişisel verilerin korunması için faydalı bir teknik olmakla beraber bu yöntemin verilerin tamamen anonimleştirilmesini sağlamadığı ve dikkatli uygulanması gerektiği unutulmamalıdır. Anonimleştirmenin aksine takma adlı hale getirme yönteminde veriler geri döndürülebilir ve takma adlı kullanılan veriler kişisel verilerin korunması mevzuatı kapsamında kişisel veriler olarak kabul edilmektedir²²². Kurul da yayımlandığı veri ihlal bildirimlerinde, veri ihlaline uğrayan veri sorumlusu şirketin veri kayıt sisteminde yer alan takma adlı hale

²²¹ Bankacılık Sektörü İyi Uygulamalar Rehberi, s. 36.

²²² **Madde 29 Çalışma Grubu**, Anonymisation Techniques, s. 20.

getirilmiş kimlik verilerini, ihlale uğrayan kişisel veriler arasında sayarak ilgili veriler için de KVKK kapsamında inceleme yapılmasına karar vermiştir²²³.

3.2.4. Lokal Veri İşleme

Kişisel veri gizliliği ve güvenliği tehditlerinin önüne geçilmesi adına kişisel verilerin araç dışına çıkarılmadan işlenmesi gibi tedbirler değerlendirilmelidir. Kişisel verilerin korunması adına en güvenli yaklaşım, mümkün olduğunca verilerin araç dışında aktarılmasını veya işlenmesini gerektirmeyen yöntemlerin kullanılmasıdır. Bu sayede araç sahibinin / sürücülerinin kişisel verileri üzerinde tam kontrol sağlaması ve verilere yetkisiz tarafların erişiminin engellenmesi mümkün olmaktadır. Verilerin araç dışına çıkarılmadan işlenmesine imkân veren lokal veri işleme süreçlerine aşağıdaki örnekler verilecektir²²⁴:

- Araç içi eko-sürüş uygulamaları gibi, yalnızca araç içinde işlenen ve sürücüye gerçek zamanlı tavsiye veren uygulamalar ile lokal olarak veri işlenebilir. Bu sayede veriler araç dışına çıkmadan işlenmektedir.
- Bluetooth veya Wi-Fi aracılığıyla akıllı telefon ile bağlantı kuran uygulamalarda lokal veri işleme yapılması mümkündür. Bu gibi durumlarda, araç verileri katma değerli hizmet sağlayıcılarına veya araç üreticilerine iletmeksizin işlenmektedir. Örneğin, telefon görüşmeleri için aracın ekranını, multimedya sistemini ve mikrofonunu kullanmak gibi akıllı telefon ile entegrasyon işlemleri lokal olarak işlenebilmektedir.
- Araç sürücüsü kullanım esnasında şerit dışına taşığında sesli uyarı veren veya direksiyon üzerinden titreşimle uyarı veren araç içi güvenlik sistemleri lokal

²²³ Kişisel Verileri Koruma Kurulu, “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Alexion İlaç Ticaret Limited Şirketi”. İlgili duyuruya internet üzerinden şu link ile ulaşılabilir: <https://www.kvkk.gov.tr/Icerik/7904/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Alexion-Ilac-Ticaret-Limited-Sirketi> (e.t. 25.05.2024).

²²⁴ Rehber, s. 18, 19.

veri işleme ile çalışabilmektedir. Bu sistemler araç sürücüsünün ve yolcuların daha güvenli bir sürüş deneyimi yaşamasına yardımcı olmaktadır.

- Araç sahibinin / sürücüsünün yüz tanıma, ses tanıma veya parmak izi ile aracı kilitleme, çalıştırma veya belirli komutları etkinleştirme gibi uygulamalar aracılığıyla işlenen biyometrik verileri lokal olarak işlenebilmektedir.

Madde 29 Çalışma Grubu²²⁵ tarafından yayımlanan bulut bilişim hakkındaki görüşte de vurgulandığı üzere, bulut işlemenin potansiyel risklerini azaltmak için veri sorumlularının mümkün olduğu ölçüde lokal veri işleme yapması önerilmektedir. Bu bakımdan araç üreticileri ve katma değerli hizmet sağlayıcılar güvenli araç içi uygulamalar geliştirmek ve gizlilik ilkelerine uymakla yükümlüdür. Lokal veri işlemenin her zaman mümkün olmadığı hallerde hibrit veri işleme yöntemlerine başvurulabilir. Örneğin, kullanım bazlı sigorta uygulamalarında araç sürücüsünün fren pedalına basma kuvveti, gidilen mesafe, direksiyon hakimiyeti gibi araç sürüş verileri araç içinde işlenebilir ve sigorta şirketi ile yalnızca skor verisi paylaşılabilir. Bu durumda sigorta şirketi veri minimizasyonu ilkesine de uygun şekilde ham davranışsal verilere erişmeksizin, yalnızca işleme sonucu oluşan skor değerine ulaşmaktadır.

3.2.5. Veri Koruma Etki Analizi

Veri koruma etki analizi, bir veri işleme faaliyetinin kişisel veriler üzerinde yaratabileceği riskleri önceden değerlendirmeye yönelik sistematik bir süreçtir. Bu analiz, veri işleme faaliyetinin kapsamı, bağlamı, amaçları ve mahiyeti dikkate alınarak gerçekleştirilmektedir²²⁶. Veri koruma etki analizi ile kişisel verilerin korunmasına ilişkin zarara yol açacak olaydan önce inceleme yapılabilecek bir

²²⁵ **Madde 29 Çalışma Grubu**, Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, Eylül, 2015. İlgili belgeye internet üzerinden şu link ile ulaşılabilir: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf (e.t. 23.05.2024).

²²⁶ **Öykü Beste Bayram**, “Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi”, Kişisel Verileri Koruma Dergisi, Cilt:4, Sayı:1, İstanbul 2022. İlgili belgeye internet üzerinden şu link ile ulaşılabilir: <https://dergipark.org.tr/tr/download/article-file/2432499> (e.t. 25.05.2024).

yapının kurulması, veri işleme faaliyetinin mevzuata ve etik ilkelere uygunluğunun teyidi, olası riskleri ve veri ihlallerini önceden belirleyerek önleyici tedbirlerin alınması, veri işleme faaliyetinin şeffaflığını ve hesap verebilirliğini artırılması ve veri sorumlularının veri gizliliği olgunluğunun artırılması ile itibarının ve marka değerinin korunması sağlanmaktadır.

Veri koruma etki analizinin uygulama adımları; (i) veri işleme faaliyetinin kapsamını ve içeriğini net bir şekilde tanımlanması, (ii) işlenen kişisel verilerin türüne, işleme yöntemlerine ve veri işleme faaliyetinin bağlamına göre risklerin belirlenmesi ve değerlendirilmesi, (iii) belirlenen risklerin ortadan kaldırılması veya azaltılması için uygun teknik ve idari tedbirlerin geliştirilmesi ve uygulanması, (iv) veri koruma etki analizi sonuçlarının ve alınan önleyici tedbirlerin kapsamlı bir şekilde belgelenmesi ve (v) veri koruma etki analizinin düzenli olarak gözden geçirilmesi ve güncellenmesidir.

Veri koruma etki analizi, veri sorumlusunun ilgili veri işleme faaliyeti için tek seferlik bir yükümlülüğü olmayıp özellikle dinamik ve düzenli değişiklik gösteren veri işleme faaliyetleri bakımından ilgili süreç boyunca süreklilik gösteren bir yükümlülüktür. Veri işleme faaliyeti ve faaliyete bağlı etkilerin değişkenliği sebebiyle daima yeni veri gizliliği ve güvenliği açıklarının ortaya çıkma ihtimaline karşı veri koruma etki analizinin düzenli olarak gözden geçirilmesi, kişisel veri güvenliğinin sağlanabilmesi adına da gerekli olmaktadır²²⁷.

Veri koruma ilkelerinin güçlendirilmesi amacıyla, GDPR'ın 35. maddesinde yer alan veri koruma etki analizinin yapılması ve tasarımla veri koruma gibi uygun teknik ve idari tedbirlerin uygulanması, bağlanabilir araçlardaki yapay zeka sistemlerinin geliştirilme sürecinde güvenlik sağlamak açısından da değerlendirilmelidir. Ancak bu konuda üç ana zorluk vardır: İlki, kişisel verilerin sınıflandırılmamasından kaynaklanan geniş kapsamlılık; ikincisi, ilgili kişilerin

²²⁷ **Madde 29 Çalışma Grubu**, Guidelines on Data Protection Impact Assessment (“DPIA”) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, Ekim, 2017. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://ec.europa.eu/newsroom/article29/items/611236/en> (e.t. 23.05.2024).

bilgi edinme ve kişisel verilere erişim hakları; üçüncüsü ise teknik ve idari tedbirleri hayata geçirme sorumluluğunun, veri sorumlularını veri işleme süreçlerini planlarken ve uygularken etik açıdan düşünmeye zorlamasıdır²²⁸. Bu durumda, genel ilkenin uygulanıp uygulanmaması veri sorumlusunun inisiyatifine bırakılmıştır.

Bağlanabilir araçlar aracılığıyla üretilecek kişisel verilerin ölçeği ve hassasiyeti göz önüne alındığında, özellikle kişisel verilerin araç dışında işlendiği durumlarda, işlemenin genellikle ilgili kişilerin hak ve özgürlükleri açısından yüksek bir riskle sonuçlanması muhtemeldir. Bu durumda, araç üreticisi ve katma değerli hizmet sağlayıcılar gibi veri sorumlularının veri işleme faaliyetleri kapsamındaki riskleri belirlemek ve ilgili riskleri azaltmak için veri koruma etki analizi yapması gerekmektedir. Kişisel veri güvenliğinin sağlanması için KVKK'da bulunmayan veri koruma etki analizi yükümlülüğü GDPR'ın 35. ve 36. maddelerinde düzenlenmekte ve ilgili maddede etki analizinin yapılması gereken haller sıralanmaktadır. İlgili maddede özel nitelikli kişisel verilerin işlendiği hallerde veri koruma etki analizi yapılması gerekliliği²²⁹ düzenlenmekte olup bu bakımdan araç sahibi / sürücüsünün biyometrik verisini işleyen veri sorumlularının, ilgili veri işleme sürecine ilişkin veri koruma etki analizi yapması gerekmektedir. Ancak, bir veri koruma etki analizinin gerekli olmadığı durumlarda bile, veri işleme tasarım sürecinin mümkün oldukça erken bir aşamasında bir veri koruma etki analizi yapılması iyi bir uygulama olacaktır. Bu sayede otomotiv sektöründeki veri sorumlularının ilgili analizin sonuçlarını bağlanabilir araçtaki yeni teknolojiler tanıtılmadan önce tasarım kararlarına dahil etmelerine olanak tanınmaktadır. Veri koruma etki analizinin Türk mevzuatında düzenlenmesi, veri sorumlularının yürüttükleri süreçleri veri koruma kültürüne göre geliştirmesini teşvik edecektir. Veri koruma etki analizinin fayda sağlaması adına risklerin tespit, değerlendirme analiz yöntemleri seçilirken göz önünde bulundurulması gerekenler, analiz çıktısı raporda nelerin bulunacağı ve ilgili raporun yayımlanacağı durumlar gibi

²²⁸ **Ufert**, s. 1094.

²²⁹ GDPR'ın 91. resitali.

hususlarda belirleyici kuralların getirilmesi adına veri koruma otoritelerinin rehberlikleri ve sektörel bazda çıkardıkları rehberler gibi yayımları önemli olacaktır²³⁰.

3.3. BAĞLANABİLİR ARAÇLARDA KİŞİSEL VERİ GÜVENLİĞİ SORUNLARI

Bağlanabilir araçlar sundukları pek çok faydanın yanı sıra, kişisel veri güvenliği açısından da birçok risk oluşturmaktadır. Bağlanabilir araçlar, internete bağlanma özelliği ile diğer araçlarla, altyapıyla ve yayalarla iletişim kurabilmektedir. Bağlanabilir araçlar, araç sürücüsü ve yolcular için konfor, güvenlik, kullanım kolaylığı ve eğlence gibi birçok fayda sunsa da aynı zamanda kişisel veri güvenliğinin sağlanması bakımından birçok risk oluşturmaktadır. Bağlanabilir araçlar tarafından sunulan çeşitli işlevler, katma değerli hizmetler ve arayüzler (örn; Wi-Fi) saldırı imkanını ve dolayısıyla kişisel verilerin tehlikeye atılabileceği potansiyel güvenlik açıklarının sayısını artırmaktadır. Çoğu IoT cihazının aksine, bağlanabilir araçlar, bir güvenlik ihlalinin araç sürücüsünün, yolcuların ve araç dışındaki kişilerin hayatını tehlikeye atabileceği kritik sistemlerdir. Bu nedenle, bağlanabilir araçların güvenlik açıklarından faydalanmak isteyen saldırganlara karşı tedbirlerin alınması çok daha önemlidir. Buna ek olarak, bağlanabilir araçlarda depolanan kişisel veriler yetkisiz erişime karşı yeterince korunmalıdır. Örneğin, araç bakımı sırasında aracın bazı teknik verilerine erişmesi gereken bir teknisyenin araçta depolanan tüm verilere erişmeye çalışması ve bu erişimin kısıtlanmasına yönelik bir teknik tedbirin alınmamış olması kişisel verilere yetkisiz erişilmesine ve dolayısıyla veri ihlaline sebebiyet verecektir²³¹.

Bağlanabilir araçlarda toplanan kişisel veriler, siber saldırılara karşı savunmasızdır. Saldırganların, kişisel verilere erişmek için aracın yazılımındaki güvenlik açıklarını veya zayıflıkları kullanmaları halinde çeşitli riskler söz konusu olacaktır. Örneğin, saldırganların aracın kamera ve sensörlerinden gelen

²³⁰ Bayram, s. 50.

²³¹ Rehber, s.15.

görüntülere erişerek araç sürücüsü ve yolcuların özel hayatlarını ihlal etmesi riskleri doğmaktadır. Saldırganların aracın konum verilerini kullanarak araç sürücüsü ve yolcuları takip etmesi ve gözetlemesi, aracın yazılımına sızarak, örneğin, hız kontrol sistemine erişerek aracın freni ve direksiyonunun kontrolünü ele geçirmesi ile kaza ve diğer güvenlik sorunlarının yaşanması gibi risk seviyesi yüksek olaylar ortaya çıkmaktadır.

Bağlanabilir araçlarda sensör kullanımının çoğalması, saldırganların ilgili kişinin finansal bilgileri, konum verisi gibi kişiyi belirlenebilir kılan bilgilerin çalınma riskini doğurmaktadır. Bazı araç üreticilerinin bağlanabilir araçlarda kablosuz anahtarlıklar ile anahtarsız sistemleri kullanması halinde bu kullanım, araca izinsiz ve kullanıma aykırı girişlerin olması ve bağlanabilir araç ile katma değerli hizmetler arasındaki veya kablosuz sistem ve bağlanabilir araç arasındaki iletişiminin kopması riskini doğurmaktadır. Benzer şekilde, bağlanabilir araçlara yapılacak saldırıların geniş etkileri de olabilmektedir. Örneğin saldırganların, bir araç üreticisi veya bağlanabilir araç modeli için ortak tespit ettiği güvenlik açığından yararlanarak araç filosunun tamamına saldırı gerçekleştirme ve aynı anda binlerce aracın kontrolünü ele geçirme riski bulunmaktadır²³².

Bağlanabilir araçlarda kullanılan yapay zeka sistemleri bakımından değerlendirildiğinde kişisel verilerle eğitilmiş yapay zeka dil modellerinin, kimlik avı veya dolandırıcılık gibi kötü amaçlarla kullanılmasının, bu tür işlemler için herhangi bir programlama bilgisine ihtiyaç duyulmaması sebebiyle oldukça kolay olduğu görülmektedir. Bu dil modellerinin hızla günlük işlerde yardımcı olan dijital asistanlara entegre edilmesi, bazı temel sorunları da beraberinde getirmektedir²³³.

²³² **Fethiye Çuhadaroğlu**, “Otomotiv Sektöründe Bağlantılı Araçların Gelişiminde Mobil Şebekeler: Bilgi Teknolojileri ve İletişim Kurumu İçin Öneriler”, Bilgi Teknolojileri ve İletişim Kurumu, Bilişim Uzmanlığı Tezi, Ankara, Mayıs, 2021, (“Çuhadaroğlu”) s. 87. İlgili teze internet üzerinden şu link ile ulaşılabilir: <https://www.btk.gov.tr/uploads/thesis/fethiye-cuhadaroglu-tez.pdf> (e.t. 06.04.2024).

²³³ **Melissa Heikkilä**, “Artificial Intelligence: Three Ways AI Chatbots Are a Security Disaster”, MIT Technology Review, 2023. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://www.technologyreview.com/2023/04/03/1070893/three-ways-ai-chatbots-are-a-security-disaster/> (Erişim Tarihi: 02.08.2024).

Özellikle yazılımsal sınırlamaların ortadan kaldırılması gibi durumlarda, bu modellerin hırsızlık veya patlayıcı yapımı gibi tehlikeli amaçlar için kullanılabileceği, ayrıca ChatGPT gibi modellerin internette gezinme ve etkileşim kurma yeteneklerinin güvenlik açıkları yaratabileceği ve yapay zeka sistemlerine ilişkin eğitim verilerinin kasıtlı olarak bozulabilmesi gibi risklerin var olduğu vurgulanmaktadır.

3.4. VERİ GÜVENLİĞİ RİSKLERİ VE TEDBİRLER

Veri sorumluları, kişisel verilerin güvenliğini sağlamak adına öncelikle işlenen tüm kişisel verilerin neler olduğunu, ilgili verilerin işlenirken ortaya çıkabilecek veri güvenliği risklerinin gerçekleşme ihtimalini ve gerçekleşmesi halinde sebep olacağı riskleri ve sonuçlarını uygun bir şekilde belirleyerek bunlara uygun tedbirlerin alınmasını sağlamalıdır.

IoT ortamının bir parçası olan bağlanabilir araçlar, yetkisiz üçüncü taraflardan gelen siber saldırılar ve yetkili üçüncü taraflardan kaynaklanan veri ihlalleri gibi güvenlik riskleri ile karşı karşıya kalmaktadır. Bağlanabilir araçlar kullanım şekli ve işlediği veriler gereği, kişisel verilere yetkisiz erişim, bu verilerin kaybı, kötüye kullanımı, değiştirilmesi ve yayılması riskini taşımaktadır. Özellikle de bağlanabilir araç, birçok farklı araç sürücüsü ve yolcunun verilerinin toplanabileceği kiralık araç veya taksi kiralama gibi bir araç paylaşım planının parçası olduğunda, pek çok senaryo mümkün olmaktadır. Bu bakımdan siber saldırıların ve veri ihlallerinin yanı sıra uygun güvenlik önlemleri alınmadığı takdirde, araç paylaşımı gibi hallerde araç sahibi, sürücüsü ve yolcular başkalarının kişisel verilerine uygunsuz bir şekilde erişebilmektedir²³⁴. Bu bakımdan bağlanabilir araçlarda verilere erişim yöntemlerinin veri sorumluları tarafından analizi gerekmektedir. Araç içi veri ve kaynaklara erişim raporuna²³⁵ göre bağlanabilir araç içi veri ve kaynaklara erişim

²³⁴ EDPS Bağlanabilir Araç.

²³⁵ **European Commission**, Access to In-vehicle Data and Resources, Final raporu, 2017, s. 6. İlgili rapora internet üzerinden şu link ile ulaşılabilir: https://transport.ec.europa.eu/document/download/107008c3-eecf-428f-887e-9096abc75ac7_en?filename=2017-05-access-to-in-vehicle-data-and-resources.pdf (e.t. 26.05.2024).

için üç teknik çözüm sunulmuş olup bunlar (i) veri sunucusu platformu, (ii) araç içi arayüz ve (iii) araç içi uygulama platformu olarak sayılmıştır. Veri sunucusu platformu çözümünün temel özellikleri, bağlanabilir araçtan gelen verilerin kullanıma sunulabileceği bir arka uç sunucusuna gönderilmesidir. Dolayısıyla hem araç verileri hem de bu verileri kullanan uygulama araç sisteminin dışındadır. Araç içi arayüz kullanılarak verilere erişim, aracın içindeki yükseltilmiş bir araç içi yerleşik bilgisayarların bir parçası olan araç içi teşhis (“on-board diagnostik”) arayüzü aracılığıyla sağlanarak, verileri kullanan herhangi bir uygulama, harici bir cihazda veya ara yüzün kendisindeki bir katmanda araç sisteminin dışında çalışması ile sağlanacaktır. Son olarak, araç içi uygulama platformu, araç verilerine erişime ve araç ortamındaki uygulamaların yürütülmesine izin vermekte ve yalnızca bu çözüm harici sunuculara veri aktarımını önlemektedir.

Bağlanabilir araçlara yapılacak olası saldırılar sonucunda çeşitli tehditlerle karşılaşılması muhtemel olup aşağıda bağlanabilir araçlara yönelik tehditlerden bazıları incelenmektedir²³⁶:

- Bağlanabilir araçlardaki sensör sayısı arttıkça, saldırganların konum bilgileri, eğlence tercihleri ve hatta finansal bilgiler gibi kişisel verileri ele geçirme çalma riski mevcuttur.
- Geleneksel anahtarların yerini dijital anahtarlar, kablosuz anahtarlıklar ve mobil uygulamalar aldıkça, araç hırsızları araçlara yetkisiz erişim sağlayabilmektedir. Öyle ki, araç sahibi yakındayken dahi saldırganların kablosuz sinyalin menzilini genişleten cihazlar kullanarak iletişimi kesmesi ve aracın kilidini açması mümkün olmaktadır.
- Saldırganlar, cep telefonu şebekeleri, Wi-Fi, fiziksel bağlantılar gibi bağlantı noktalarındaki güvenlik açıklarından faydalanarak bağlanabilir araç

²³⁶ <https://www.eenewseurope.com/en/top-ten-security-challenges-for-connected-cars-2/> (e.t. 26.05.2024).

sistemine zarar vermektedir.

- Saldırganlar, direksiyon ve frenleme gibi kritik güvenlik sistemlerinin kontrolünün ele geçirilmesiyle kazalara sebep olmaktadır.
- Bağlanabilir araçlarda araç üreticileri ve katma değerli hizmet sağlayıcılar tarafından daha fazla mobil uygulama yayımlandıkça, bu uygulamalar saldırganlar için hedef haline gelmektedir. Örneğin, bir uygulamada ısıtmalı direksiyon simidi, koltuklar, fanlar ve klimayı uzaktan kontrol eden yetkisiz erişim sonucunda elektrikli bir araçta bu durum aracın bataryasını boşaltarak ve aracı hareket edemez hale getirebilmektedir.
- Araç üreticileri, araçlar için sistem, yazılım ve donanım bileşenlerini üçüncü taraflardan tedarik ettiği hallerde tedarikçilerine sıkı siber güvenlik şartları getirerek güvenlik açığının önüne geçmelidir. Yeni tehditler ve saldırılar keşfedildikçe, bağlanabilir araçların kullanımdayken bile kolay ve güvenli bir şekilde güncellenebilmesi temin edilmelidir.

Bağlanabilir araç ve ekipman üreticileri, katma değerli hizmet sağlayıcılar gibi veri sorumluları, işlenen kişisel verilerin güvenliğini ve gizliliğini koruyarak verilerin yetkisiz bir kişi tarafından ele geçirilmesini önlemek için gerekli teknik ve idari tedbirleri almalıdır. Sektör katılımcıları özellikle aşağıdaki önlemleri dikkate almalıdır²³⁷:

- İletişim kanallarının en son teknoloji ürünü bir algoritma ile şifrlenmesi.
- Her modele genel bir şifreleme anahtarı koyulmaksızın, her araca özgü bir şifreleme anahtarı yönetim sisteminin uygulamaya konulması.
- Veriler araç dışında depolandığında son teknoloji algoritmalarla şifrlenmesi.

²³⁷ Rehber, s. 24.

- Şifreleme anahtarlarının düzenli olarak yenilenmesi ve ilgili şifreleme anahtarlarına erişimin engellenmesi için uygun tedbirlerin alınması. Şifreleme yöntemleri, kişisel veri güvenliğinin sağlanması için başvurulacak bir tedbirdir. Bu kapsamda şifreleme anahtarı yalnızca veriye erişime yetkili kişilerde bulundurulmalı ve yetkisiz erişim önlenmelidir. Bu sebeple seçilen şifreleme yönteminin kişisel verilerin korunması için uygun olması veri sorumlusunun tedbir yükümlüğü altındadır. Veri işleme tedbiri kapsamında uluslararası kabul gören şifreleme programlarının kullanımı veri sorumluları tarafından tercih edilmelidir.

- Verilerin aktarılacağı cihazların kimliğinin doğrulanması.
- Hashleme gibi yöntemlerle veri bütünlüğünün sağlanması.
- Kişisel verilere erişiminin şifre, elektronik sertifika gibi güvenilir kullanıcı kimlik doğrulama tekniklerine tabi kılınması.

EDPB, bağlanabilir araçlarda veri işlenmesi esnasında araç üreticisi veri sorumluları için aşağıdaki güvenlik önlemlerinin uygulanmasını tavsiye etmekte olup, sayılan genel tavsiyelerin her bir veri işleme faaliyetinin özellikleri ve amacı dikkate alınarak özel tedbirlerle tamamlanması gerekmektedir:

- Bağlanabilir araçta sunulması gerekli temel ve hayati fonksiyonlarının bilgi ve eğlence gibi her zaman internete bağlı olan ek hizmetlerden ayrılması.
- Araç üreticilerinin, aracın tüm kullanım ömrü boyunca güvenlik açıklarını hızlı bir şekilde kapatılmasını sağlayan teknik tedbirleri uygulaması.
- Aracın hayati fonksiyonları için, özellikle taşımacılığa ayrılmış güvenli frekansların kullanılmasına mümkün olduğunca öncelik verilmesi.
- Aracın sistemlerine saldırı olması durumunda, düşürülmüş moda çalışma olasılığı ile birlikte bir alarm sistemi kurulması.

- Herhangi bir potansiyel saldırının kaynağının anlaşılmasını sağlamak ve olası anormallikleri tespit etmek için kaydedilen bilgilerin periyodik olarak gözden geçirilmesini sağlamak amacıyla aracın bilgi sistemine yapılan her türlü erişimin altı ay öncesine kadar giden bir kayıt geçmişinin saklanması.

Konuyu siber güvenlik tedbirleri bakımından değerlendirdiğimizde, veri koruma mevzuatları ve sektöre özgü düzenlemeler, araç üreticileri ve diğer ilgili tarafların uygun siber güvenlik önlemlerini sağlamak ve bir siber güvenlik yönetim sistemi uygulamak zorunda olduklarını düzenlemektedir. İlgili yönetim sistemi, siber güvenliği izlemek, örneğin izinsiz giriş veya diğer müdahale girişimlerini tespit etmek ve müşteri hesaplarını korumak, ayrıca olay müdahale süreçlerini yönetmek için sistemler ve önlemler içermelidir. Tüm bunlar, potansiyel olarak kişisel verilerin işlenmesini gerektireceğinden, yeterli siber güvenlik koruması ve olay müdahale yeteneklerini sağlamak için gerekli olan kişisel verilerin bağlanabilir araç kapsamında işlenmesi, veri güvenliğinin sağlanmasının yanı sıra veri sorumlusunun meşru menfaati hukuki sebebine dayanılarak da gerekli olmaktadır²³⁸.

Bağlanabilir araçlar kapsamında araç üreticileri, sürücü dikkatinin dağılmasını önlemek gibi teknik standartlara ve diğer tasarım gereksinimlerine de tabidir. Sürekli veya aşırı düzeyde araç sürücüsü etkileşimi gerektirmek, örneğin veri koruma amacıyla geniş bilgi mesajları göstermek veya her seferinde aracın çalıştırılması ya da bir veri işleme özelliği etkinleştirildiğinde rızanın yenilenmesi gibi durumlar, sürücü dikkatinin dağılmasına neden olabileceği gibi etkileşimi amacına aykırı hale getirecektir. Bu nedenle veri koruma mevzuatlarının yanı sıra sektörel olarak düzenlenen diğer mevzuat ve rehberlerin, veri koruma unsurlarını bu tür gerekliliklerle daha iyi dengelemeyi hedeflemesi gerekmektedir.

Bağlanabilir araçlar, internet ve diğer ağlarla bağlantı kurarak veri gönderip alarak çeşitli bağlı işlevleri sunmaktadır. Bu sayede araçların daha konforlu ve

²³⁸ **European Automobile Manufacturers Association**, ACEA comments EDPB guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, Nisan, 2020. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: https://www.acea.auto/files/ACEA_comments_EDPB_guidelines_1-2020.pdf (e.t. 23.08.2024).

güvenli hale gelmesi sağlanırken, bağlı işlevler araçları siber saldırılara karşı da açık hale getirmektedir. Bu nedenle, otomotiv sektöründeki paydaşlar ile yetkili kamu kurum ve kuruluşlarının iş birliğiyle bağlanabilir araçların güvenliğini sağlamak için çeşitli tedbirlerin alınması değerlendirilmelidir²³⁹.

- Çalışma grubu oluşturma: Ulaştırma ve Altyapı Bakanlığı (“UAB”) öncülüğünde, Bilgi Teknolojileri ve İletişim Kurumu (“BTK”) ve Ulaştırma Siber Güvenlik Operasyon Merkezi (“USOM”) bünyesinde bir çalışma grubu kurulması önemlidir. Bu çalışma grubu, küresel gelişmeleri ve otomotiv sektör ihtiyaçlarını da gözeterek bağlanabilir araçların uçtan uca güvenliğini sağlamak için olası saldırı yöntemlerini tespit ederek gerekli tedbirleri belirlemelidir.
- Otomotiv sektör paydaşlarının sorumlulukları: Bağlanabilir araçlarda güvenliğin sağlanmasında yalnızca kamu kurum ve kuruluşlarının etkinliği yetersiz kalacaktır. Bu kapsamda, araç üreticileri, katma değerli hizmet sağlayıcıları gibi sektör paydaşlarının etkin rol oynaması ve kendilerine ait sistemlerin güvenli bir şekilde işletilmesi adına alınan tedbirleri düzenli olarak gözden geçirmeleri ve iyileştirme tedbirlerini almaları önemlidir. Bağlanabilir araçlara yönelik siber saldırıların potansiyel etkilerini en aza indirmek, benzer tehditleri önceden tespit etmek, olası saldırıları bertaraf etmek veya etkilerini azaltmak için tüm paydaşlar arasında bilgi paylaşımı ve koordinasyonun sağlanması kritik önem taşımaktadır.
- Siber saldırı bildirimi ve raporlaması: Bağlanabilir araçlara siber saldırı olması halinde ilgili saldırıya ilişkin tüm bilgilerin vakit kaybetmeksizin BTK ve USOM gibi yetkili kurumlarla paylaşılması gerekmektedir. Paylaşım yaparken araçların temel yazılım ve sürüm bilgileri gibi düzenli olarak yetkili kurumlara envanter yönetimi amacıyla sağlanması gereken bilgilere ek olarak araca yapılan saldırının türleri, aracın etkilenen aksamı, zafiyet bilgisi, saldırının sonlandırılması ve etkisinin azaltılması adına alınan tedbirlerin neler olduğu ve

²³⁹ Çuhadaroglu, s. 140, 141.

meydana gelen hasar hakkında araç üreticisi gibi saldırıya maruz kalan paydaşların raporlama yapması gerekmektedir.

- Siber güvenlik farkındalığının sağlanması: Siber güvenlik farkındalığının sağlanması adına UAB ve BTK gibi yetkili kurum ve kuruluşlarla beraber sektör paydaşları tarafından araç sahibi / sürücüleri için siber saldırılara karşı farkındalık yaratan faaliyetlerin yapılması önem olmaktadır. Bu çalışmalara ek olarak ISO VE ENISA gibi kurum ve kuruluşlarca bağlanabilir araçlarda güvenliğin sağlanması için yürütülen çalışmaların ve gelişmeler ışığında gerekli tedbirlerin düzenli takibi önem arz etmektedir.
- Kurum içi tedbirlerin alınması: Bağlanabilir araçların güvenliğini sağlamak için organizasyonel ve yönetsimsel süreçler büyük önem taşımaktadır. Bu bakımdan tedarikçilerle ilişkiler, çalışanların eğitimi, olay yönetimi gibi kurumsal kuralların ve en iyi uygulama örneklerinin ayrıntılı olarak belirlenmesi ve prosedüre dökülmesi gerekmektedir²⁴⁰.
- Kişisel verilerin korunması mevzuat takibi: Bağlanabilir araçlarda tasarımla veri koruma ilkesi de gözetilerek kişisel verilerin korunması amacıyla Kurum öncülüğünde BTK gibi yetkili kurum ve kuruluşlar, araç üreticileri ve hizmet sağlayıcı gibi paydaşların katılımları ile veri gizliliği ve güvenliğini sağlamak adına sektörel olarak çalışmaların yürütülmesi gerekmektedir. Türkiye’de ilgili çalışmalar yürütülürken uluslararası düzenlemelerin de dikkate alınması gerekmektedir. Bu bakımdan, GDPR ve 2002/58/EC sayılı Direktif başta olmak üzere veri koruma mevzuatları, EDPB ve CNIL gibi yetkili veri koruma otoriteleri ile Alman Otomotiv Endüstrisi Birliği gibi kuruluşların çalışmaları örnek olarak incelenmelidir.

Bağlanabilir araçların güvenliğinin sağlanması adına yukarıda belirtilen tedbirlerin alınması ile bağlanabilir araçların siber saldırılara karşı daha güvenli

²⁴⁰ ENISA, s. 29.

hale getirilmesi mümkündür. Bu sayede, can ve mal kayıpları önlenerek ulaşım sistemlerinin güvenliği temin edilmektedir.

CNIL Rehberi'nde, araç üreticilerinin bazen hizmet sağlayıcı, bazen de piyasaya sürdükten sonra bile (ürün güvenliği, ürün sorumluluğu, garanti) yasal sorumlulukları olan bir ürünün üreticisi olarak çeşitli amaçlarla veri işlediği göz önünde tutulduğunda araç üreticilerinin model optimizasyonu ve ürün iyileştirmesi amacıyla veri işleyebileceği hallerde, veri güvenliğinin temin edilmesi adına bu veriyi, işleme amacı ortadan kalkar kalkmaz imha etmesini veya anonim hale getirilerek işlemesini savunmaktadır²⁴¹. Teknik tedbirlere uygun şekilde anonim hale getirilen veri özelinde artık veri koruma mevzuatlarının uygulaması kalkacaktır.

3.5. VERİ GÜVENLİĞİ ÖRNEK SENARYOLARI

3.5.1. Veri Güvenliği Tehditleri ve Yaşanmış Saldırıları

Bağlanabilir araçların yazılım ve elektronik bileşenleri gibi karmaşık yapıları ve çeşitli bileşenleri, bu araçları siber saldırılara karşı savunmasız hale getirmektedir. Araçların telematik sistemleri, motor ve şasi kontrol birimleri gibi kritik bileşenleri, kötü niyetli aktörlerin saldırılarına maruz kalabilmektedir. Bu tür tehditlere karşı alınması gereken önlemler arasında, tüm bileşenlerin siber güvenlik kontrollerine tabi tutulması ve sürekli güncellemelerle güvenliğin sağlanması sayılmaktadır.

Elektrikli araçlar ve yüksek güçlü şarj istasyonları, özellikle güç şebekesine yönelik saldırılar için potansiyel bir tehdit oluşturmaktadır. Çok sayıda elektrikli aracın aynı anda şarj edilmesi sırasında gerçekleşebilecek bir saldırı, güç şebekesinde kesintilere veya elektrik kesintilerine yol açabilmektedir. Bu tür bir tehdit, enerji ve ulaşım sektörleri arasında daha güçlü bir iş birliği ve karşılıklı anlayış gerektirmektedir. Bu tehdidi bertaraf etmek için, elektrikli araçların şarj

²⁴¹ CNIL Rehberi s. 24. İlgili rehber internet üzerinden şu link ile ulaşılabilir: <https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data> (E.t. 17.03.2024).

altyapısına yönelik siber güvenlik standartlarının belirlenmesi ve uygulanması gerekmektedir.

Sayılan tehditler göz önünde tutulduğunda, örneğin, Tesla 2023 yılında yaşanan büyük bir veri ihlali sonucunda 75.000'den fazla kişinin kişisel bilgilerinin açığa çıkmasına neden olmuş, bu da bağlanabilir araç teknolojilerinin taşıdığı risklerin boyutunu gözler önüne sermiştir. Benzer şekilde, Nissan, yaklaşık 18.000 müşteriyi etkileyen bir veri ihlali yaşamış, otomotiv sektöründe veri güvenliğinin ihmal edilemeyecek derecede önemli olduğunu bir kez daha göstermiştir²⁴². Yine, Eylül 2023 öncesi Tesla'nın yapay zeka destekli oto pilotu, 17 ölüm ve 736 kazaya karışmış olup, şu anda birçok hükümet soruşturmasının konusudur²⁴³.

Mobil cihazların, bağlanabilir araçların kilit işlevlerini kontrol etmek için kullanılması, bir diğer önemli tehdit vektörüdür. Mobil cihazlar üzerindeki güvenlik açıkları, kötü niyetli yazılımlar veya zayıf şifreleme yöntemleri, araçların ele geçirilmesine yol açmaktadır. Bu riski azaltmak için, mobil cihazlar ve uygulamalar üzerinde güçlü şifreleme ve kimlik doğrulama önlemleri uygulanmalı, kullanıcılar güvenlik konusunda bilgilendirilmelidir. Bağlanabilir araçlar, temelde "tekerlekli bilgisayarlar" olarak nitelendirilebilir ve bu araçlar, 200'den fazla sensörle saatte 25 gigabayta kadar veri üretebilmektedir. Bu veriler genellikle bulut platformlarına aktarıldığından siber saldırılara karşı savunmasız hale gelmektedir. Örneğin, 2015 yılında bir Jeep Cherokee'nin uzaktan hacklenmesi olayı, saldırganların frenler, direksiyon ve şanzıman gibi kritik fonksiyonları ele geçirmesine neden olmuş ve bu olay, 1,4 milyon aracın geri çağırılmasına yol açmıştır²⁴⁴.

²⁴²**Telecom Review**, "Connected Cars and Data Privacy: Challenges and Solutions in a New Automotive Era", Kasım, 2023. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://www.telecomreview.com/articles/reports-and-coverage/7553-connected-cars-and-data-privacy-challenges-and-solutions-in-a-new-automotive-era> (e.t. 23.08.2024).

²⁴³**Mozilla**, "It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy", Eylül, 2023. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/> (e.t. 23.08.2024).

²⁴⁴**Wired**, "Hackers Remotely Kill a Jeep on the Highway—With Me in It", Temmuz, 2021. İlgili yazıya internet üzerinden şu link ile ulaşılabilir: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> (e.t. 23.08.2024).

2016 yılında, bir araştırmacı grubu, Nissan Leaf araçlarının bir mobil uygulama üzerinden nasıl hacklenebileceğini ortaya koyarak aracın bağlantılı mobil uygulaması üzerinden araç içi sistemlere erişim sağlamıştır. Bu şekilde enerji yönetimi sistemi devre dışı bırakılmıştır. Bu saldırı, Nissan Leaf'in mobil uygulamasındaki güvenlik açığından faydalanarak gerçekleştirilmiştir. Uygulama üzerinden araçtaki enerji yönetim sistemi manipüle edilmiş olup böylece araştırmacılar aracın batarya durumunu ve diğer enerji yönetimi özelliklerini kontrol edebilmiştir. Nissan, bu saldırı sonucunda mobil uygulamasını devre dışı bırakmak zorunda kalmış ve güvenlik önlemlerini artırmak için bir dizi önlem planlamıştır. Ancak bu olay, otomotiv sektöründe mobil uygulamalar üzerinden gerçekleştirilebilecek saldırılara ve bu saldırıların, bağlanabilir araçlardaki mobil uygulamaların ne kadar savunmasız bırakılabileceğine ve bu tür saldırıların araçların temel fonksiyonlarını nasıl etkileyebileceğine karşı farkındalığın artması bakımından oldukça önemlidir²⁴⁵.

İnsan faktörü de bağlanabilir araçlar üzerindeki siber tehditlerde kritik bir rol oynamaktadır. Çalışanların siber güvenlik farkındalığının artırılması ve sürekli eğitimlerle desteklenmesi, bu tür tehditleri azaltmada önemli bir adımdır. Ayrıca, çalışanların iş süreçlerinde güvenliği sağlamak için gereken yeni becerilerle donatılması ve güçlü bir güvenlik kültürünün teşvik edilmesi gereklidir.

Bağlanabilir araçlar üzerinden gerçekleştirilebilecek finansal suçlar da ciddi bir tehdit oluşturmaktadır. Araçlar üzerinden yapılan ödemeler, kötü niyetli aktörler tarafından hedef alınabilmektedir. Bu tür tehditlere karşı, ödeme sistemlerinin güvenliği artırılmalı ve sistemler siber güvenlik standartlarına uygun olarak geliştirilmelidir. Araç üreticileri, uluslararası siber güvenlik standartlarına (örneğin, UNECE WP.29, ISO 24089) uymalı ve bu standartları araç geliştirme süreçlerine entegre etmelidir.

²⁴⁵ <https://www.securityweek.com/api-flaw-exposes-nissan-leaf-cars-remote-attacks/> (e.t. 31.08.2024)

3.5.2. Kazalara Yönelik Raporlama Çalışması

Bağlanabilir araç kazalarını konu alan rapor çalışmalarında, toplanan verilerin düzeltici aksiyonları aldırma etkisinin yanı sıra verilerin güvenliğini sağlamak ve veri ihlallerini önlemek de kritik öneme sahiptir. Bu çalışmalarda veri sorumluları tarafından veri işleme faaliyetlerinin yürütülmesi sırasında dikkat edilmesi gereken hususlar EDBP tarafından Rehber’de²⁴⁶ paylaşılmıştır:

- Çalışmaya katılım gönüllülük esasına dayanmalıdır. Bu bakımdan veri sorumlularının araştırmanın amacı, anlık hız, konum bilgisi gibi işlenen verilerin neler olduğu ve kişisel verilerinin işlenme süreci hakkında ilgili kişileri şeffaf bir şekilde bilgilendirmeleri gerekmektedir. Bu bilgilendirme ilgili kişi ile ilk kontak kurulan zaman, ancak en geç veri işleme faaliyetine başlarken sağlanmalıdır (örneğin bilgilendirmenin, ilgili kişilerin formu imzalayarak araştırmaya dahil oldukları aşamada sağlanması). Veri işleme faaliyeti ilgili kişinin açık rızasına dayandığı takdirde bu rıza, önceden işaretli olmayan bir kutucuk seçmek veya bağlanabilir araç ekranı üzerinden aktivasyon sağlamak gibi yöntemlerle alınmalıdır. Rıza, ilgili kişi ile veri sorumlusu arasındaki bağlanabilir araçla ilgili temel hizmetler bakımından sözleşmenin ayrılmaz bir parçası haline getirilmeksizin herhangi bir zamanda geri alınabilmelidir. Rıza geri çekildiğinde ise, rızaya tabii olan veri işleme faaliyeti durdurulmalı ve farklı bir hukuki yükümlülük olmadıkça veriler silinmeli veya anonim hale getirilmelidir.
- Sadece araştırma amacıyla kesinlikle gerekli olan kişisel veriler toplanmalı ve veri minimizasyonu ilkesi gözetilmelidir. Raporlama çalışması için ilgili kişilere ait kimlik bilgisi, araç verisi ve anlık hız gibi araçlardan elde edilen teknik veriler toplansa da raporlama amacı dışında kişisel veri işlenmemelidir. Toplanan verilerin niteliğine ve miktarına dikkat edilmeli, yalnızca gerekli olanlar kullanılmalıdır.

²⁴⁶ Rehber, s. 33, 34.

- İlgili kişilere ve araçlara ilişkin veriler, çalışma süresince saklanabilecek olup veri sorumluları tarafından işleme amacına bağlı saklama sürelerinin tespiti gerekmektedir. Belirlenen sürenin sonunda veriler silinmeli veya anonim hale getirilmelidir. Verilerin gereğinden fazla süreyle saklanması veri güvenliği risklerini artıracığından saklama süresine uyulması önemlidir.

Veri sorumluları tarafından uygulanacak tedbirler hassas verilere göre uyarlanmalıdır. CNIL de yayımladığı rehberde bu kapsamda veri işleme süreçlerine paralel olarak tedbir alınmasını önermektedir²⁴⁷. Örneğin, bağlanabilir araçlarda meydana gelen kazaların analiz çalışmalarının bir parçası olarak anlık hız bilgisine ek olarak araç sahibi / sürücüsü kimlik bilgisi, aracın konum bilgisi, araç seri numarası gibi bilgiler toplanıyorsa aşağıdaki gibi güçlü güvenlik önlemlerinin alınmasını tavsiye etmektedir:

- Bağlanabilir araç aracılığıyla işlenen kişisel verilerin takma adlı hale getirilmesi tedbirinin uygulanması, örneğin, ilgili kişinin adı / soyadı ve araç seri numarası gibi verilerin gizli anahtarlarla hashlenmesi.
- Anlık hız ve araç konumu ile ilgili verilerin farklı anahtarlar ve onay mekanizmaları ile son teknoloji bir şifreleme mekanizması kullanılarak ayrı veri tabanlarında saklanması veya araç konum verilerinin, referans alınan tercih edilen yol ve seyahatin gece veya gündüz yapılması gibi olay veya zaman aralığı tespitinin yapılmasını takiben silinmesi.
- İlgili kişiye ait belirlenebilir verilerin yalnızca az sayıda ve yetkili kişi tarafından erişilebilen ayrı bir veri tabanında saklanması.

Sayılan yöntemlerle kişisel verilerin yetkisiz erişime, kullanıma, değiştirilmeye veya yok edilmeye karşı korunması için gerekli teknik ve idari önlemlerin alınması, veri sorumlularının yükümlülükleri arasındadır.

²⁴⁷ CNIL Rehberi, s. 30.

3.5.3. Araç Hırsızlığı ile Mücadele

İlgili kişiler, özellikle araç sahipleri, hırsızlık durumunda aracın konum verisini kullanarak araçlarını bulmaya çalışmak isteyebilmektedir. Bu durumda araç konum verilerinin kullanımı, resmi makamların soruşturma kapsamında gerekli görmesi amacı ile sınırlı olmaktadır. Kişisel verilerin işlenmesine ilişkin olarak, konum verilerinin işlenmesinin hukuki sebebi araç sahibinin rızası veya araç sahibinin taraf olduğu sözleşmenin ifası için gerekli veriler bakımından bir sözleşmenin ifası olacaktır. Kişisel verilerin işlenmesinden önce ilgili kişinin KVKK uyarınca şeffaf ve anlaşılabilir bir şekilde bilgilendirilmesi gerekmektedir. Söz konusu bilgilendirmede daha spesifik olarak EDPB, veri sorumlusunun aracın sürekli takibinin söz konusu olmadığı ve konum verilerinin yalnızca hırsızlık beyanından itibaren toplanıp yetkili makamlara iletilebileceğini ilgili kişiye yapacağı aydınlatmada vurgulamasını tavsiye etmektedir²⁴⁸. Ayrıca, veri sorumlusu, ilgili kişilere verilerin aktarılacağı taraflarla ilgili şeffaflık içerisinde bilgi verilerek gerek kendi bünyesinde gerek de aktarım taraflarında alınan tedbirlere ve verilere yalnızca yetkili ve sınırlı kişilerin erişebileceğine ilişkin bilgi sağlamalıdır.

Konum verilerinin yalnızca soruşturma süresince işlenmesi ve geri kalan süre boyunca ve sürekli olarak toplanmaması gerekmektedir. Aynı şekilde konum verileri yalnızca vakanın yetkili yasal makamlar tarafından değerlendirildiği süre boyunca veya aracın çalındığının teyit edilmesiyle sona ermeyen şüpheyi ortadan kaldırmaya yönelik bir prosedürün sonuna kadar saklanmalıdır. İlgili kişilerin haklarına ilişkin olarak, veri işleme rızaya dayalı olduğunda ilgili kişi, ileriye dönük etkili olmak kaydıyla dilediği zaman rızasını geri alma hakkına sahip olduğuna ilişkin özel olarak bilgilendirilmelidir.

²⁴⁸ Rehber, s. 35.

3.5.4. E-Call Sistemi

eCall sistemi²⁴⁹, AB genelinde ciddi bir kaza durumunda otomatik olarak 112 acil durum numarasını arayan bir sistemdir. Bu sistem, kazanın hemen ardından olay yerine hızlı bir şekilde ambulans gönderilmesini sağlamak amacıyla tasarlanmıştır. 29 Nisan 2015 tarihli ve 2015/758 sayılı AB Tüzüğü uyarınca, bu sistemin araçlarda bulunması zorunlu kılınmıştır.

eCall sistemi, kazanın hemen ardından otomatik olarak devreye giren ve aracın konum bilgileri gibi minimum verileri acil durum merkezine ileten bir mekanizmaya sahiptir. Bu verilerin işlenmesi, GDPR ve 2002/58/EC sayılı Direktif gibi çeşitli yasal düzenlemeler tarafından sıkı bir şekilde kontrol edilmektedir. eCall sistemi kapsamında işlenen verilerin yasal dayanağı, GDPR'ın 6/1-(c) maddesi ve KVKK'nın 5/2-(ç) maddesi uyarınca yasal bir yükümlülüğe uyumdur. Bu durum, veri sahibinin rızasının aranmasını gereksiz kılmakta ve sistemin zorunlu bir güvenlik tedbiri olarak kabul edilmesini sağlamaktadır. Bu bağlamda, 2002/58/EC sayılı Direktif'in 5/3 maddesi, araç içinde depolanan verilere erişim sağlanmasına ilişkin olarak ilgili kişi rızası gerektirse de 2015/758 sayılı AB Tüzüğü, bu gerekliliği ortadan kaldıran bir yasal zorunluluk yaratmaktadır.

2015/758 sayılı AB Tüzüğü, eCall sistemi tarafından toplanan verilerin sadece gerekli minimum bilgileri içermesini şart koşmaktadır. Bu bilgiler arasında aracın tanımlama numarası (VIN), aracın konumu, seyahat yönü ve kaza anına ilişkin zaman damgası gibi veriler yer almaktadır. Bu verilerin saklama süresi, yalnızca acil durumların işlenmesi için gerekli olan süre ile sınırlıdır ve bu sürenin sonunda veriler tamamen silinmelidir. Ayrıca ilgili kişilerin, eCall sistemi kullanılarak işlenen veriler hakkında açık ve ayrıntılı bir şekilde bilgilendirilmesi zorunludur. Bu bilgiler, araç sahiplerine / sürücülerine sistem kullanılmadan önce verilmelidir. Üreticiler, veri işlemenin yasal dayanağı, toplanan veri türleri, veri saklama süreleri ve ilgili kişilerin hakları gibi konularda kullanıcıları bilgilendirmekle yükümlüdür.

²⁴⁹ Rehber, s. 32, 33.

eCall sistemi, kişisel verilerin korunmasını sağlamak için gerekli güvenlik önlemlerini de içermelidir. Üreticiler, sistemde kişisel verilerin kötüye kullanımını önlemek için gelişmiş gizlilik teknolojilerini dahil etmelidir. Bu kapsamda, PSAP'ler tarafından işlenen verilerin kötüye kullanımına karşı korunması ve kişisel verilerin saklanması, işlenmesi ve korunmasına ilişkin protokollerin titizlikle uygulanması gerekmektedir.

3.5.5. Verilerin Araçta Otomatik Bir İşlem Tetiklemek İçin Uzaktan Hizmet Sağlayıcısına Aktarılması

Bağlanabilir araçlardan toplanan verilerin, araçta uzaktan bir otomatik işlem tetiklemek amacıyla hizmet sağlayıcısına iletilmesi halinde veri işleme faaliyeti, araçların güvenliği, bakım hizmetleri ve sürücü deneyiminin iyileştirilmesi gibi çeşitli amaçlara dayanarak gerçekleştirilmektedir²⁵⁰. Ancak, bu durum aynı zamanda kişisel verilerin işlenmesi ve gizlilik açısından önemli riskler barındırmaktadır.

Bu işleme faaliyeti kapsamında araç sahipleri, fren aşınma durumu veya teknik inceleme tarihinin hatırlatılması gibi aracın işleyişiyle ilgili mesajlar veya uyarılar almak, araçta uzaktan teknik güncellemeler yapılması için bir hizmet sağlayıcısıyla sözleşme ilişkisine girmektedir. Araç sahipleri, sürüş deneyimlerini iyileştirmek amacıyla dinamik trafik bilgileri, örneğin, yolda bir olay sonrası yeni rota gönderilmesi, erken uyarı mesajları veya eko-sürüş uyarıları gibi hizmetlerden yararlanmak adına da bu sözleşme ilişkisini kurmaktadır.

Söz konusu veri işleme faaliyetinin dayandığı hukuki sebep, genellikle ilgili kişinin imzaladığı sözleşmenin ifası kapsamında gerçekleşmektedir. Sözleşmenin ifası hem uzaktan bakım hem de sürüş deneyiminin iyileştirilmesi amacıyla verilerin işlenmesini kapsamaktadır.

250

Veri minimizasyonu ilkesi kapsamında hizmetin sağlanabilmesi için sadece gerekli olan kişisel veriler toplanmalıdır. Örneğin, uzaktan bakım için hassas ve ayrıntılı konum verilerinin işlenmesi gerekli değildir. Özellikle cezai suçları ortaya çıkarabilecek verilerin işlenmesi, yasal bir dayanak olmaksızın işlenmemeli ve bu veriler, mümkün olduğunca yerel olarak araç içinde işlenmeli ve kullanıcıya bu tür veriler üzerinde tam kontrol sağlanmalıdır. Kullanıma dayalı veriler, yalnızca sözleşme süresi boyunca saklanmalı, sözleşmenin sona ermesini takiben farklı bir hukuki sebep mevcut değil ise imha edilmelidir. Ancak uygun teknik tedbirlerin alınması şartıyla veriler anonimleştirilerek saklama süresi uzatılabilmektedir. Ancak veri sorumluları tarafından verilerin saklama süreleri her bir veri seti ve iş faaliyeti kapsamında değerlendirilmelidir. Örneğin, kullanıma dayalı olabilse de araç üzerindeki müdahalelerle ilgili veriler aracın ömrü boyunca saklanmalıdır.

Veri sorumlusu araç üreticisi veya hizmet sağlayıcı tarafından hizmetin sağlanmasında rol oynayan bir veri işleyene kişisel veriler aktarıldığında veri işleyenin bu verileri kendi amacı için kullanmaması gerekir. Veri işleyenin verileri nasıl işleyeceği konusunda sorumluluk veri sorumlusuna aittir. Ayrıca ilgili kişiler, kişisel verilerin işlenmesinden önce, veri sorumlusunun kimliği, işleme amacı, verilerin saklanacağı süre ve veri koruma hakları konusunda bilgilendirilmelidir. GDPR uyarınca, bu bilgilendirme açık, basit ve kolayca erişilebilir terimlerle yapılmalıdır.

Bağlanabilir araçlardan toplanan verilerin, araçta uzaktan bir otomatik işlem tetiklemek amacıyla hizmet sağlayıcısına iletilmesi halinde araç üreticisi ve katma değerli hizmet sağlayıcı gibi veri sorumluları, verilerin güvenliğini ve gizliliğini sağlamak için gerekli kontrolleri uygulamalı ve yetkisiz kişiler tarafından kontrolün ele geçirilmesini önlemek için gerekli tüm tedbirleri almalıdır. Özellikle şu önlemlerin uygulanması, CNIL tarafından rehberdeki örnek senaryolarda²⁵¹ ele alınmaktadır:

²⁵¹ CNIL Rehberi, s. 32-35.

- İletişim kanallarının, ileri düzey bir algoritma kullanılarak şifrlenmesi.
- Her araca özgü, modele değil, bir şifreleme anahtar yönetim sisteminin kurulması.
- Veri tabanında yer alan verilerin ileri düzey algoritmalarla şifrlenmesi.
- Şifreleme anahtarlarının herhangi bir kazayla ifşa edilmesinden korunması.
- Veri alıcı cihazların kimlik doğrulamasının yapılması.
- Kişisel verilere erişimin güvenilir kullanıcı kimlik doğrulaması (şifre, elektronik sertifika vb.) ile sağlanması.
- Araç üzerinde işlem gerçekleştiren cihazların kimlik doğrulamasının yapılması.
- Araçların hayati işlevlerinin, sürekli olarak internete bağlı olan sistemlerden (örneğin "bilgi-eğlence" sistemleri) ayrılması.
- Güvenlik açıklarının hızla yamalanmasını sağlayan teknik önlemlerin uygulanması.
- Araçların hayati işlevleri için mümkün olduğunca ulaşım amaçlı özel olarak ayrılmış güvenli frekansların kullanılmasına öncelik verilmesi.
- Saldırı durumunda bir alarm sistemi kurulması ve aracın azaltılmış modda çalışabilme olasılığının sağlanması.
- Saldırının kaynağını anlayabilmek için altı aya kadar geri giden bir günlük kayıt tarihçesinin tutulması.

Uygulanan önlemler, verilerin duyarlılık düzeyine ve cihazların kontrol kapasitesine uygun olmalıdır. Araç dışındaki altyapılarda uygulanacak önlemlerle ilgili olarak, hizmet sağlayıcısı, işlemle ilgili riskleri değerlendirmek ve bu riskleri minimize etmek için gerekli önlemleri belirlemek amacıyla bir risk değerlendirmesi

yapmalıdır. Ayrıca veri sorumlusu, ürün ve hizmetleri tasarlarken en baştan kişisel veri sorunlarını göz önünde bulundurmalı ve tasarımla veri koruma prensibi ile ürün veya hizmetin, aracın veri çıkışı sadece hizmetin sağlanması için gerekli olanla sınırlamalı ve mümkün olduğunca verilerin yerel olarak depolanmasını sağlamalıdır. Hizmet sağlayıcısı ayrıca, veri toplama zincirinde mümkün olan en erken aşamada veri anonimleştirmeye öncelik vermelidir. Sonuç olarak veri sorumlularının araçta temel işlevlerin korunması adına gerekli teknik önlemler alması gerekmektedir.



SONUÇ

Dijital dönüşümün otomotiv sektörüne etkisi değerlendirildiğinde, bağlanabilir araçlar ve sürüş deneyimindeki teknolojik gelişmeler mobilitayı yeniden şekillendirmekte ve yeni çevrim içi iş modelleri oluşturmaktadır. Bu durum, giderek artan veri hacimleri ve verinin kullanım ihtiyaçları nedeniyle önem kazanmaktadır. Özellikle bağlanabilir araçlardan veri toplayan ve bu verilere erişimi olan hizmet sağlayıcılar için yeni pazar fırsatları ve araçlarla ilgili yeni geliştirmeler ve sunulan hizmet teklifleri; veri koruma, yeni teknolojiler ile ekonomik ihtiyaçların birlikte değerlendirilmesi ihtiyacı doğurmaktadır.

Bağlanabilir araçlardan araç sahibi, sürücüsü, yolcular gibi kimliği belirli veya belirlenebilir gerçek bir kişiye ait veriler ve ilgili kişileri belirlenebilir kılan araç kullanım verileri işlenmektedir. Bu nedenle araç sahibi ve sürücülerinin; araç ve sürüş verilerinin hangi sınırdan işleneceği, bu verilerin hangi üçüncü taraflarla ve ne şekilde paylaşılacağı, ölçülülük, şeffaflık ve veri minimizasyonu ilkelerinin nasıl uygulanacağı ve veri güvenliğinin temini için gerekli teknik ve idari tedbirler kapsamında aydınlatılması gerekmektedir. Ancak henüz bu alana özel yasal düzenlemenin olmaması pek çok konunun detaylı olarak incelenmesini zorunlu kılmaktadır.

Bağlanabilir araçlar ve bu araçların kullanımından kaynaklı veri işlenmesi kaçınılmaz bir teknolojik gelişmedir ve bu alanda yeni düzenlemelerin yapılması zorunluluğunu doğurmaktadır. Pek çok veri koruma otoritesi, bu alandaki inovatif ekosistemi desteklemenin yanı sıra araç sürücülerine ait kişisel verilerin korunması için çalışmalar yürütmekte ve rehberler yayımlamaktadır.

Bu tezde, bağlanabilir araçlarda veri işlenmenin işlenen kişisel veriler dikkate alınarak kişisel verilerin korunması kapsamında baştan sona detaylı olarak incelenmesi ve uygulamada araç üreticileri ve hizmet sağlayıcılar gibi veri sorumluları tarafından dikkat edilmesi gerekenlerin tespit edilmesi hedeflenmiştir.

Tez kapsamında yapılan inceleme üç ana başlık altında gerçekleştirilmiştir:

Birinci bölümde tezin ana inceleme kapsamını oluşturan kişisel veri koruma kavramı ve AB ve Türkiye'deki güncel kişisel veri koruma mevzuat gelişmeleri incelenmiştir. Bu incelemede KVKK ve GDPR'daki yaklaşımlar ve ilgili düzenlemeler ortaya konulmakla beraber, iki mevzuatta yer alan farklılıklar da tartışılmaktadır. Veri koruma mevzuatının genel hatlarıyla incelenmesinin yanında bağlanabilir araçlar özelinde ortaya çıkmış mevzuat gelişmeleri de incelenmiştir. Ayrıca, Avrupa Birliği'ndeki veri işleme ile ilgili diğer mevzuatlar da incelenmiş ve incelenen tüm mevzuatların bağlanabilir araçlardaki veri işleme süreçlerine etkileri tartışılmıştır. Özellikle AB Veri Yasası ve otomotiv sektörü üzerine etkisi detaylı olarak incelenmiştir.

İkinci bölümde bağlanabilir araçlarda ve buna bağlı gelişen teknolojilerdeki güncel gelişmeler ele alınmıştır. Ayrıca ikinci bölümde kişisel veri kavramı kapsamında işlenen veriler, işleme amaçları, hukuki sebepleri, verilerin aktarım tarafları ve ilgili kişi haklarına ilişkin alt başlıklar, bağlanabilir araçlarda işlenen kişisel veriler özelinde ele alınmıştır.

Üçüncü ve son bölümde ise işlenen kişisel verilerin güvenliğinin sağlanması adına kişisel veri mevzuatında yer alan temel ilkelerin uygulanma alanları aktarılmıştır. Son bölümde ayrıca bağlanabilir araçlarda karşılaşılan veri güvenliği riskleri ve bu risklerin sebepleri üzerinde durularak, çeşitli uygulama senaryoları üzerinden riskleri önleyici tedbirlerin neler olduğu incelenmiştir. Bağlanabilir araçlarda veri güvenliğinin sağlanması adına mevzuat ve uygulama çalışma gruplarının oluşturulması, otomotiv sektör paydaşlarının ve yetkili kurum ve kuruluşların sorumluluklarının belirlenmesi, siber saldırı olayları için bildirim ve raporlama yapılması, araç sahipleri / sürücülerinde güvenlik farkındalığının sağlanması, bağlanabilir araçların güvenliğini sağlamak adına gerekli organizasyonel tedbirlerin alınması bakımından geçerli mevzuat takibinin önemi üzerinde durulmuştur.

Tez içerisindeki incelemeler sonucunda, bağlanabilir araçlarda veri işleme faaliyetlerinin kişisel verilerin korunması ilkelerine uygun olarak

gerçekleştirilmesinin, sektörel düzenlemelerin AB'deki mevzuat ve veri koruma otoritesi rehberleri ışığında düzenli olarak gözden geçirilmesinin ve araç üreticisi gibi otomotiv sektör aktörleri ile yetkili kurum ve kuruluşlar arasında iş birliğinin artırılarak sektörel olarak veri koruma olgunluğunun artırılmasının kapsamı ve önemi değerlendirilmiştir.



KAYNAKÇA

Acarer, Tayfun, Endüstri'deki Gelişmelerin Denizcilik İşletmelerine Ait Gemilerin Yönetiminde Temin Ettiği Yeni Olanaklar ve İnsansız Gemiler, Mersin Üniversitesi Denizcilik ve Lojistik Araştırmaları Dergisi, Cilt:5, Sayı:2, 2023.

Akçalı Gür, Berna, Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 2019.

Anı, Nevzat Ali, Kişisel Verilerin İşlenmesi ve Açık Rıza, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 2018 (Yayımlanmamış Yüksek Lisans Tezi).

Arat, Tugay, Aslan, M. Mert, Sosyal Medyada Veri Güvenliği ve Kişisel Mahremiyet Sorunu, Akdeniz Üniversitesi İletişim Fakültesi Dergisi, S:35, 2021.

Atabey, Ayça, Is Google At Odds With The GDPR? Evaluation of Google's Personal Data Collection on Mobile Operating Systems in Light of The Principles of Data Minimisation, Purpose Limitation, and Accountability, İstanbul Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, Yüksek Lisans Tezi, İstanbul, 2019.

Ayözger, Ayşe Çiğdem, Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, İstanbul, 2016 (Yayımlanmamış Doktora Tezi).

Baker, Pam, What Is the Cyber Resilience Act? Secure EU Compliance Simplified, Information Week, Nisan, 2024.

Başalp, Nilgün, Avrupa Birliği Veri Koruma Genel Regulasyonu'nun Temel Yenilikleri, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi (MÜHF HAD), Cilt.21, Sayı.1, 2015.

Bayram, Öykü Beste, Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi, Kişisel Verileri Koruma Dergisi, Cilt:4, Sayı:1, İstanbul 2022.

Bennett, Colin J., Raab, Charles D., The Governance of Privacy: Policy Instruments in Global Perspective, 2006.

Çekin, Mesut Serdar, 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi, İÜHFM, C. LXXIV, S. 2, 2016.

Çekin, Mesut Serdar, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, On İki Levha Yayıncılık, İstanbul, 2018.

Çelikel, Serdar, Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, T.C. Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Doktora Lisans Tezi, Ankara, 2021.

Çimen Bulut, İpek, Avrupa Dijital Tek Pazarında Kişisel Verilerin Korunması, T.C. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Avrupa Birliği Anabilim Dalı Avrupa Çalışmaları Programı Doktora Tezi, İstanbul, 2023.

Çuhadaroğlu, Fethiye, Otomotiv Sektöründe Bağlantılı Araçların Gelişiminde Mobil Şebekeler: Bilgi Teknolojileri ve İletişim Kurumu İçin Öneriler, Bilgi Teknolojileri ve İletişim Kurumu, Bilişim Uzmanlığı Tezi, Ankara, 2021.

de Manuel, Alicia, Ethical Assessments and Mitigation Strategies for Biases in AI-systems Used During the COVID-19 Pandemic, Big Data & Society, 2023.

Dima, Florin Costinel, Drone technology and human rights, University of Twente, 2017.

Doğan, Buse, Kişisel Verilerin İşlenme Şartları Bağlamında Açık Rıza, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, İstanbul, 2019.

Edwards, Lilian, Data Protection and E-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling, Law, Policy and the Internet, Hart Publishing, 2019.

Gamito, Marta Cantero, Marsden, Christopher T, Artificial intelligence co-regulation? The role of standards in the EU AI Act, International Journal of Law and Information Technology, 2024, Sayı: 32.

Greenleaf, Graham, The influence of European data privacy standards outside Europe: implications for globalization of Convention 108, International Data Privacy Law, Sayı: 2, 2012.

Güçlütürk, Osman Gazi, Yapay Zeka ve Verinin Kullanımı, On İki Levha Yayıncılık, 2022.

Günes Peschke, Seldağ, Peschke, Lutz, Artificial Intelligence and the New Challenges for EU Legislation, Yıldırım Beyazıt Hukuk Dergisi, Ağustos, 2022.

Heikkila, Melissa, Artificial Intelligence: Three Ways AI Chatbots Are a Security Disaster, MIT Technology Review, 2023.

Hyseni, Vlerë, A Comprehensive Guide: Understanding the NIS 2 Directive, PECB, Kasım, 2023.

Kaya, Mehmet Bedii, KVKK Reformu: 2024 Değişiklikleri (Dijital Baskı 1.0), 2024.

Kesa, Aleksandr, Kerikmae, Tanel, Artificial Intelligence and the GDPR Inevitablenesses?, Taltech Journal of European Studies, 2020, Sayı: 10.

Keser Berber, Leyla / Atabey, Ayça, Yapay Zeka Sistemlerinin Çocuk Haklarına Etkilerinin Değerlendirilme Yöntemi: Çocuk Hakları Etki Analizi. Adalet Dergisi Sayı: 66, 2021.

Kuner, Christopher, The Internet and the Global Reach of EU Law, Oxford University Press, 2019.

Kuner, Christopher, A Bygrave Lee, Docksey Christopher, Drechsler Laura, The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, Şubat, 2020.

Küzeci, Elif, Kişisel Verilerin Korunması, 3. Baskı, Ankara, 2019.

Küzeci, Elif, Kişisel Verilerin Korunması, On İki Levha Yayıncılık, 4. Baskı, 2020.

McLachlan, Scott, Kyrimi, Evangelia, Dube, Kudakwashe, Fenton, Norman E., Schafer, Burkhard: The Self-Driving Car: Crossroads at the Bleeding Edge of Artificial Intelligence and Law, Cornell University, Workingpaper, 2022.

Mustata, Clara, Connected Cars: The legislative environment, potential reform and privacy issues, IAPP, Haziran, 2024.

O'Doherty, Michael, Internet Law, Bloomsbury Professional, Croydon, 2020.

Paal, Boris, Artificial Intelligence as a Challenge for Data Protection Law: And Vice Versa, The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives, Cambridge Law Handbooks, 2022.

Paul, David, Greenstein Shane, The Economics Of Compatibility Standards: An Introduction To Recent Research, Economics of Innovation and New Technology, 1990, Sayı: 1.

Özer Deniz, Miray, Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk, T.C. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Doktora Lisans Tezi, Adana, 2022.

Turgut Bilgiç, Ezgi, Genel Veri Koruma İlkelerinin Yapay Zeka Karşısında Uygulanabilirliği Sorunu, Türkiye Adalet Akademisi Dergisi, Ocak, 2024.

Ufert Frederike, AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?, European Papers, 2020.

Ursic, Helena, Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control, SCRIPTed: Journal of Law, Technology and Society, Sayı. 15, 2018.

von Ingersleben-Seip, Nora, Competition and cooperation in artificial intelligence standard setting: Explaining emergent patterns, Review of Policy Research, Sayı: 40.

Yılmaz, Beste, Kişisel Verilerin Korunması ve Rekabet Hukuku Bağlamında Veri Taşınabilirliği Hakkı, On İki Levha Yayıncılık, İstanbul, 2023.

Yılmaz, Oğuz Gökhan, Yargı Uygulamasında Yapay Zeka Kullanımı- Yapay Zeka Hâkim Cübbesini Giyebilecek mi?, Adalet Dergisi, sayı 66, 2021.

Yücedağ, Nafiye, Kişisel verilerin korunması kanunu kapsamında genel ilkeler, Kişisel Verileri Koruma Dergisi, 2019.

Çevrimiçi Kaynaklar

<https://www.enisa.europa.eu/publications/smart-cars>

<https://www.forbes.com/sites/forbestechcouncil/2023/03/27/how-to-make-use-of-the-new-gold-data/>

<https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararası-ve-Ulusal-Düzenlemeler>

https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=RjZwH00oMG4iNa5Sgvlgg8n_7mNZ8NqHZRTxHGB-vGqr6bdxh8Yrdt8mLfnSMkhF

https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=RsTBl6RWK25OBMIktIgYYUrajK5kg0Whjop-mbB3gUBeg-C6SdhUv_1KiSEKK5D8

<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/c6206722-f4dc-484d-9bff-63f99b840158.pdf>

<https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1712410558&id=id&accname=guest&checksum=966017718BF7B781F54D210627D333B9>

<http://nek.istanbul.edu.tr:4444/ekos/TEZ/58103.pdf>

<https://rm.coe.int/1680078b37>

https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=DPTyuy3wRPq_qvCPSqUB6_rFkFwB0ydLk7LMNZmv1qlknrbQfer-dPVmt9yZp1H

<https://www.kvkk.gov.tr/Icerik/7834/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununda-Yapilan-Degisiklikler-Hakkinda-Kamuoyu-Duyurusu>

<https://medium.com/@elfkzc/avrupa-konseyinin-108-say%C4%B1l%C4%B1-ki%C5%9Fisel-verilerin-korunmas%C4%B1-s%C3%B6zle%C5%9Fmesi-yenilendi-bc8daad9decc>

https://itlaw.bilgi.edu.tr/media/2020/3/30/Bilgi_Avrupa_Veri_Koruma_Mevzuat%C4%B1_El_Kitab%C4%B1_2018_TR_v01_16022019.pdf

https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_6385

<https://eur-lex.europa.eu/eli/reg/2016/679/oj>

https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=RYan9_S-Z7Eir3xdWGXBIGDRjcmOMffAR9wKMmwadGB7sOCDHavHBVRiy4uyCtR5

<https://www.dataguidance.com/opinion/eu-edpb-issues-guidelines-connected-vehicles>

https://www.edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf

https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

https://iapp.org/media/pdf/resource_center/privacy_playbook_for_connected_car_data.pdf

<https://www.btk.gov.tr/uploads/boarddecisions/112-tabanli-arac-ici-acil-cagri-sistemi-e-call/027-05-112-tabanli-arac-ici-acil-cagri-sistemi-e-call-22-01-2018.pdf>

<https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data>

<https://www.kvkk.gov.tr/Icerik/5394/Aydinlatma-YukumLugunun-Yerine-Getirilmesi-Rehberi>

<https://www.ford.com.tr/sartlar-ve-kisisel-verilerin-korunmasi/baglantili-araclar-aydinlatma-metni>

<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf>

<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>

<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/9feefe58-9b0f-49c9-a0c7-2b2eb8c012bb.pdf>

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_e_privacydir_gdpr_interplay_en_0.pdf

<https://www.btk.gov.tr/uploads/thesis/fethiye-cuhadaroglu-tez.pdf>

https://edps.europa.eu/data-protection/ourwork/publications/techdispatch/techdispatch-3-connected-cars_en

<https://mbkaya.com/hukuk/kvkk-reformu.pdf>

https://www.edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf

<https://op.europa.eu/en/publication-detail/-/publication/0f3e5c98-66ad-11e7-b2f2-01aa75ed71a1/language-en>

<https://www.volvocars.com.cn/en-cn/legal/privacy/privacy-car2#167ea0396a05a393c0a80065655a9f16>

https://login.bmwusa.com/pm2/pm-document-service/api/v1link/documents/policyName/BMW_CONNECTED_DRIVE_DPP/CA/PDF?language=en&KeyId=dbf0a542-ebd1-4ff0-a9a7-

55172fbfce35#:~:text=We%20may%20use%20the%20information,is%20anonym
ized%20and%20not%20identifiable.&text=•,Partners.,with%20our%20approved
%20BMW%20partners

https://essay.utwente.nl/73105/1/DIMA_BA_EPA.pdf

<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/353d85d5-87df-4c91-b08e-b4f0991a80f4.pdf>

<https://script-ed.org/wp-content/uploads/2018/08/ursic.pdf?d=05232024>

<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF>

<https://dergipark.org.tr/tr/download/article-file/902576>

https://insanhaklarieylemlani.adalet.gov.tr/resimler/%C4%B0nsan_Haklar%C4%B1_Eylem_Plan%C4%B1_ve_Uygulama_Takvimi.pdf

<https://ms.hmb.gov.tr/uploads/2021/03/Ekonomi-Reform-Takvimi.pdf>

https://www.sbb.gov.tr/wp-content/uploads/2023/09/Orta-Vadeli-Program_2024-2026.pdf

<https://www.btk.gov.tr/uploads/boarddecisions/uzaktan-programlanabilir-sim-teknolojileri-esim/053-2019-web.pdf>

https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=9MiDp3x86xrwjpi5-14w-Tiw6MEvWpcRXBA25_FzBfidxLYsxN3J5ZaHUG833qLb

<https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik>

<https://www.kvkk.gov.tr/Icerik/7782/2023-1430>

<https://dergipark.org.tr/tr/download/article-file/271091>

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/582ad48e-0a69-417f-ad9c-30cc08b7b5aa.pdf>

<https://kvkk.gov.tr/SharedFolderServer/CMSFiles/12236bad-8de1-4c94-aad6-bb93f53271fb.pdf>

<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf>

<https://kvkk.gov.tr/SharedFolderServer/CMSFiles/11b6fd99-d42a-45b1-a009-21f2d36ded21.pdf>

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf

<https://ec.europa.eu/newsroom/article29/items/622227>

<https://ec.europa.eu/newsroom/article29/items/611236/en>

https://transport.ec.europa.eu/document/download/107008c3-eeef-428f-887e-9096abc75ac7_en?filename=2017-05-access-to-in-vehicle-data-and-resources.pdf

https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf

<https://www.kvkk.gov.tr/Icerik/7399/2022-662https://www.kvkk.gov.tr/Icerik/7399/2022-662>

<https://www.lexology.com/library/detail.aspx?g=454f1afc-8561-4949-a20c-b7a34548d77b>

<https://www.mayerbrown.com/en/insights/publications/2024/03/eu-data-act-new-rules-on-data-sharing-and-portability-of-cloud-services-now-in-force>

<https://autovista24.autovistagroup.com/news/european-data-act-empowers-users-connected-vehicles/>

[https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en#:~:text=On%201%20August%202024%2C%20the,AI%20Act\)%20enters%20into%20force](https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en#:~:text=On%201%20August%202024%2C%20the,AI%20Act)%20enters%20into%20force)

https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_en

https://www.europarl.europa.eu/doceo/document/TA-9-2022-0383_EN.html

<https://www.mondaq.com/uk/security/1283104/building-cyber-security-resilience-nis-2-enters-into-force>

<https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

<https://www.dlapiper.com/en/insights/topics/cyber-resilience-act>

https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5375

<https://www.gsg hukuk.com/tr/bultenler-yayinlar/duyurular/siber-dayaniklilik-yasasi.html>

<https://iapp.org/resources/article/connected-cars-canada/>

<https://www.theparliamentmagazine.eu/partner/article/europe-on-the-move-access-to-vehicle-data-legislation-is-urgently-needed>

<https://www.theparliamentmagazine.eu/partner/article/europe-on-the-move-access-to-vehicle-data-legislation-is-urgently-needed>

https://fipa.bc.ca/wp-content/uploads/2018/01/CC_report_lite.pdf

<https://digital-strategy.ec.europa.eu/en/library/ecall-do-you-have-any-concerns-your-privacy-you-shouldnt>

<https://www.autoconnectedcar.com/definition-of-connected-car-what-is-the-connected-car-defined/> (

<https://www.autoconnectedcar.com/2015/07/onstar-celebrates-1-billion-requeste-with-free-premium-service-for-loyal-users/>

<https://www.autoconnectedcar.com/definition-of-connected-car-what-is-the-connected-car-defined/>

[https://www.european-eprivacy-regulation.com/ePrivacy_Regulation_Preamble_21_to_30_\(Council_Proposal_10.02.2021\).html](https://www.european-eprivacy-regulation.com/ePrivacy_Regulation_Preamble_21_to_30_(Council_Proposal_10.02.2021).html)

https://www.acea.auto/files/ACEA_comments_EDPB_guidelines_1-2020.pdf

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources_en

<https://www.engage.hoganlovells.com/knowledgeservices/news/eu-data-act-part-5-smart-cars-and-data-sharing-obligations-qa>

https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en

<https://www.telecomreview.com/articles/reports-and-coverage/7553-connected-cars-and-data-privacy-challenges-and-solutions-in-a-new-automotive-era>

<https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>

<https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

<https://www.cnil.fr/fr/tenir-compte-de-la-protection-des-donnees-dans-la-collecte-et-la-gestion-des-donnees>

<https://www.securityweek.com/api-flaw-exposes-nissan-leaf-cars-remote-attacks/>

<https://www.dataguidance.com/opinion/eu-overview-european-digital-strategy>

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020DC0066>

https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_264

<https://www.arthurcox.com/knowledge/what-are-common-european-data-spaces/>

https://transport.ec.europa.eu/transport-themes/smart-mobility_en

<https://digital-strategy.ec.europa.eu/en/activities/cef-digital>

<https://digital-strategy.ec.europa.eu/en/news/cef-digital-operational-digital-platforms>

<https://digital-strategy.ec.europa.eu/en/policies/mobility-data>

<https://deployemds.eu/>

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023DC0751>

<https://digital-strategy.ec.europa.eu/en/activities/digital-programme>

<https://mobility-dataspace.eu/mobility-data-space#:~:text=The%20Mobility%20Data%20Space%20connects,data%20and%20for%20what%20purpose.>

<https://digital-strategy.ec.europa.eu/en/library/second-staff-working-document-data-spaces>