



**OTONOM SİSTEMLERİN GİZLİLİK VE KİŞİSEL VERİLERİN
KORUNMASI ÇERÇEVESİNDE İNCELENMESİ**

Naz Nebile KARATAŞ

**YÜKSEK LİSANS TEZİ
ADLI BİLİŞİM ANA BİLİM DALI**

**GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ**

ŞUBAT 2024

Naz Nebile KARATAŞ tarafından hazırlanan OTONOM SİSTEMLERİN GİZLİLİK VE KİŞİSEL VERİLERİN KORUNMASI ÇERÇEVESİNDE İNCELENMESİ” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Adli Bilişim Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç.Dr.Hüseyin ÇAKIR

Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı, Gazi
Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Başkan: Prof.Dr.Aydın ÇETİN

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Üye: Doç.Dr.Recep BENZER

Yazılım Mühendisliği Ana Bilim Dalı, Konya Gıda ve Tarım Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Tez Savunma Tarihi: 16/02/2024

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....
Prof. Dr. Aslıhan TÜFEKÇİ
Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
 - Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
 - Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
 - Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
 - Bu tezde sunduğum çalışmanın özgün olduğunu,
- bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Naz Nebile KARATAŞ

16/02/2024

OTONOM SİSTEMLERİN GİZLİLİK VE KİŞİSEL VERİLERİN KORUNMASI ÇERÇEVESİNDE İNCELENMESİ

(Yüksek Lisans Tezi)

Naz Nebile KARATAŞ

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Şubat 2024

ÖZET

Yapay zekanın gelişmesi, beraberinde otonom sistemler gibi pek çok yeniliğin oluşmasına neden olmuştur. Otonom sistemler, insan müdahalesi olmadan kendi başlarına karar verebilen ve eylemler gerçekleştirebilen sistemlerdir. Bu sistemler, ulaşım, sağlık, üretim, savunma gibi çeşitli alanlarda yaygın olarak kullanılmaya başlamıştır. Otonom sistemlerin kullanımının artması, kişisel verilerin gizliliği ve korunması açısından önemli riskler oluşturmaktadır. Bu çalışmanın odak noktası gizlilik ve kişisel verilerin korunması çerçevesinde otonom sistemlerin oluşturabileceği riskleri ortaya koyarak alınabilecek önlemler hakkında öneride bulunmaktır. Bu çalışmada otomatik ve otonom sistem arasındaki farklara değinilerek otonom sistem tanımlanmaya çalışılacak, gizlilik ve kişisel verilerin korunmasına ilişkin Türkiye ve Avrupa Birliği'ndeki hukuki düzenlemelere, otonom araçlarla ilgili Türkiye ve Avrupa Birliği'ndeki hukuki düzenlemelere değinilecektir. Ayrıca otonom araçlarda gizlilik ve kişisel verilerin korunması çerçevesinde kullanıcıların ve uzmanların görüşlerine yer verilecektir. Toplanan verilerden yola çıkarak otonom araçlarda mahremiyete ilişkin olası problemler açıklanarak bu problemlere ilişkin çözüm önerilerinde bulunulacaktır. Mevcut durumda hukuki düzenlemeler teknolojinin gerisinden gelmektedir. Bu sebeple gelecekte otonom sistemler sebebiyle doğabilecek hukuki uyumsuzlukların çözümünün mevcut düzenlemelerle sağlanamayacağı ve bu amaç için özel düzenlemelere ihtiyaç olduğu muhakkaktır.

Bilim Kodu	: 92401
Anahtar kelimeler	: Otonom sistemler, otonom araç, kişisel veri, gizlilik
Sayfa Adedi	: 87
Danışman	: Doç.Dr.Hüseyin ÇAKIR

THE ASSESSMENT OF PRIVACY AND PERSONAL DATA PROTECTION IN AUTONOMOUS SYSTEMS

(M. Sc. Thesis)

Naz Nebile KARATAŞ
GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

February 2024

ABSTRACT

The development of artificial intelligence (AI) has led to the emergence of many new innovations, such as autonomous systems. Autonomous systems are capable of making decisions and performing actions without human intervention. These systems have begun to be widely used in various fields, such as transportation, healthcare, manufacturing, and defense. The increasing use of autonomous systems poses significant risks to the privacy and protection of personal data. This study focuses on identifying the risks associated with autonomous systems in the context of privacy and personal data protection and proposes measures that can be taken to address these risks. In this study, the differences between automatic and autonomous systems will be discussed, and autonomous systems will be defined. It will also discuss the legal regulations in Turkey and the European Union regarding the protection of privacy and personal data, and the legal regulations in Turkey and the European Union regarding autonomous vehicles. In addition, the views of users and experts will be included in the context of the protection of privacy and personal data in autonomous vehicles. Based on the collected data, potential problems related to privacy in autonomous vehicles will be explained and solutions to these problems will be proposed. Currently, legal regulations lag behind technology. Therefore, it is evident that existing regulations will not be sufficient to resolve legal disputes that may arise due to autonomous systems in the future. Special regulations will be necessary to address this issue and ensure the resolution of legal conflicts arising from autonomous systems.

Science Code : 92401
Keywords : Autonomous systems, autonomous vehicle, personal data, privacy
Page Number : 87
Supervisor : Assoc. Prof. Dr. Hüseyin ÇAKIR

TEŞEKKÜR

Bu tez çalışmasının tamamlanmasında emeği geçen ve katkıda bulunan herkese en içten teşekkürlerimi sunarım.

Öncelikle, değerli danışman hocam Doç. Dr. Hüseyin Çakır'a, tezimin her aşamasında verdiği değerli destek ve rehberlik için şükranlarımı sunarım. Hocam, tezimin her aşamasında yaptığı kapsamlı ve yapıcı eleştirileri ile tezimin kalitesini arttırmama büyük katkıda bulunmuştur.

Ayrıca aileme, her zaman yanımda oldukları ve bana verdikleri koşulsuz sevgi ve destek için teşekkür ederim. Ailemin desteği olmadan bu çalışmayı tamamlamam mümkün olmazdı.

Tez çalışmamın çeşitli aşamalarında bana yardımcı olan Dr. Ali Ufuk Peker, Batuhan Özcan, Selen Zengin ve Ali Akkaya'ya da en içten teşekkürlerimi sunarım. Tezime değerli bilgi, deneyim ve önerileri ile önemli katkı sağlamışlardır.

Bu çalışmanın tamamlanmasında emeği geçen herkese tekrar teşekkür ederim.

Saygılarımla,

Naz Nebile KARATAŞ

İÇİNDEKİLER

	Sayfa
ÖZET.....	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
ÇİZELGELERİN LİSTESİ.....	x
ŞEKİLLERİN LİSTESİ.....	xii
1.GİRİŞ.....	1
2.KURAMSAL ÇERÇEVE VE İLGİLİ ARAŞTIRMALAR.....	7
2.1. Kuramsal Çerçeve.....	7
2.1.1.Mahremiyet.....	7
2.1.2.Kişisel veri.....	8
2.1.3.Otomatik sistemler ve otonom sistemler.....	8
2.1.4.Makine etiği.....	9
2.1.5.Otonom araç seviyeleri.....	10
2.1.6.Otonom araçların veriye yönelik mimarisi.....	14
2.1.6.1.Otonom araçlarda sensör teknolojisi.....	15
2.1.6.1.1.Harici sensörler (Dışsal duyuşal sensörler) (Exteroceptive sensors).....	15
2.1.6.1.1.1.LiDAR (Işık algılama ve mesafe ölçme).....	15
2.1.6.1.1.2.Kamera.....	16
2.1.6.1.1.3.Radar.....	16
2.1.6.1.1.4.Ultrasonik.....	17
2.1.6.1.2.Dahili sensörler (Kendinden duyuşal sensörler) (Proprioceptive sensors).....	17
2.1.6.1.2.1.GPS (Küresel konumlandırma sistemi).....	17
2.1.6.1.2.2.IMU (Atalet Ölçüm Birimi).....	18
2.1.6.1.2.3.Kodlayıcılar.....	19
2.1.6.2.V2X (Araçtan- Her Şeye).....	19
2.1.7.Otonom araçlarda toplanan veri türleri.....	20
2.1.8.Otonom araçlarda mahremiyet türleri.....	22
2.1.9.Otonom araçlarda mahremiyete yönelik kullanılan yöntemler.....	23
2.1.9.1.128D (128-Dimensional face embedding).....	23

2.1.9.2.MMFE (Morphable model-based facial exchange).....	25
2.1.9.3."De-Identification" (Anonimleştirme) "Release-And-Forget" (Yayınlama ve unutmama) Modeli.....	25
2.2.İlgili Araştırmalar.....	26
2.2.1.Gizlilik ve kişisel veriler ile ilgili yapılan araştırmalar.....	27
2.2.2.Otonom sistem ve araçlar ile ilgili yapılan araştırmalar.....	27
2.2.3.Otonom sistemlerde ve araçlarda gizlilik ve kişisel veri ile ilgili yapılan araştırmalar.....	28
3.YÖNTEM.....	31
3.1.Araştırmanın Modeli.....	31
3.2.Çalışma Grubu.....	32
3.3.Veritoplama Aracı.....	32
3.4.Verilerin Analizi.....	33
4.BULGULAR VE YORUM.....	35
4.1.Gizlilik ve Kişisel Verilerin Korunmasına İlişkin Türkiye'deki Hukuki Düzenlemelerin İncelenmesi.....	35
4.1.1. Kişisel verilerin korunması kanunu (KVKK).....	36
4.2.Gizlilik ve kişisel verilerin korunmasına ilişkin Avrupa Birliği'ndeki hukuki düzenlemelerin incelenmesi.....	36
4.2.1.Avrupa Birliği genel veri koruma tüzüğü (General data protection regulation-GDPR).....	38
4.2.2.Avrupa veri koruma kurulu- kişisel verilerin video cihazları aracılığıyla işlenmesine ilişkin 3/2019 sayılı yönerge.....	40
4.3.Otonom Araçlarla İlgili Türkiye'deki Hukuki Düzenlemelerin İncelenmesi.....	44
4.3.1.Motorlu araçlar ve römorkları ile bunlar için tasarlanan aksam, sistem ve ayrı teknik ünitelerin genel güvenliği ve korunmasız karayolu kullanıcılarının ve yolcuların korunması ile ilgili tip onayı yönetmeliği (AB/2019/2144).....	44
4.3.2.112 Acil çağrı servisi tabanlı araç içi acil çağrı sistemine ilişkin motorlu araçların tip onayına yönelik idari hükümlerin hazırlanması ve bu sistem kullanıcıları için gizlilik ve veri korumasına ilişkin yönetmelik (2017/78/AB).....	45

4.4.Otonom Araçlarla İlgili Avrupa Birliği'ndeki Hukuki Düzenlemelerin İncelenmesi.....	47
4.4.1.Avrupa veri koruma kurulu- bağlı araçlar ve mobilite ile ilgili uygulamalar bağlamında kişisel verilerin işlenmesine ilişkin 01/2020 sayılı yönerge (Kılavuz ilkeler).....	47
4.4.2.Motorlu araçlar ve römorkları ile bunlar için tasarlanan aksam, sistem ve ayrı teknik ünitelerin genel güvenliği ve korunmasız karayolu kullanıcılarının ve yolcuların korunması ile ilgili tip onayı yönetmeliği (27 Kasım 2019 tarihli AB/2019/2144 sayılı).....	50
4.4.3.Avrupa Birliği yapay zeka yasası.....	51
4.5. Otonom Araçlarda Gizlilik ve Kişisel Verilerin Korunması Çerçevesinde Kullanıcıların Görüşlerinin İncelenmesi.....	56
4.6.Otonom Araçlarda Gizlilik ve Kişisel Verilerin Korunması Çerçevesinde Uzmanların Görüşlerinin İncelenmesi.....	65
4.7.Otonom Araçlarda Mahremiyete İlişkin Olası Problemlerin İncelenmesi.....	69
5.SONUÇ ve ÖNERİLER.....	71
KAYNAKLAR.....	75
EKLER.....	81
EK-1.Katılımcı Anket Formu.....	82
EK-2.Uzman Görüşme Formu Soruları.....	85
EK-3.Etik Kurul Onayı.....	86
ÖZGEÇMİŞ.....	88

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 2.1. Otomatik ve Otonom Sistem Karşılaştırması.....	9
Çizelge 2.2. Otonom Araç Seviyeleri Sınıflandırmalarının Karşılaştırması.....	14
Çizelge 2.3. Araç Modellerine Göre Kaydedilen Veriler.....	21
Çizelge 4.1. Biyometrik Verinin İşlendiğinin Kabul Edilebilmesi İçin Dikkate Alınan Kriterler.....	43
Çizelge 4.2. Anket formuna katılan otonom araç kullanıcılarının kişisel özellikleri...	56
Çizelge 4.3. Otonom araç kullanıcılarının tercih sebebi.....	57
Çizelge 4.4. “Bağlı araç” teriminin ne demek olduğunu bilinmesi.....	57
Çizelge 4.5. Otonom araç satın alırken yapılan bilgilendirme.....	58
Çizelge 4.6. Otonom aracın kaydettiği verilerin kişisel veri olup olmadığına ilişkin görüşler.....	58
Çizelge 4.7. Otonom araçta kaydedilen verilerin güvenli şekilde saklanıp saklanmadığına ilişkin görüşler.....	59
Çizelge 4.8. Otonom aracın veri kaydı özelliği devre dışı bırakılabiliyor olsaydı bu özelliğin kapatılmak istenip istenmeyeceği.....	59
Çizelge 4.9. Otonom aracın kaydettiği verilerin kimlerle paylaşıldığı konusunda izin verilip verilmediği.....	60
Çizelge 4.10. Otonom aracın kaydettiği verilerin üçüncü taraflar ile paylaşılmadan önce kullanıcılardan onay alınması.....	60
Çizelge 4.11. Otonom araçta kaydedilen verilerden hangilerinin kontrol edilmek istendiği.....	60
Çizelge 4.12. Otonom araçta kaydedilen veriler ile ilgili kullanıcıları endişelendiren konular.....	61
Çizelge 4.13. Otonom aracın kaydettiği hangi verileri paylaşırken kullanıcılar rahat hisseder.....	62
Çizelge 4.14. Otonom aracın kaydettiği verilerin kullanıcılar hangi durumlarda paylaşılmasını kabul eder.....	63
Çizelge 4.15. Otonom araç bozulduğunda kullanıcıların bir tuş ile yardım çağırma ve arıza hakkında bilgi gönderebilme durumunda verilerini paylaşmak isteyip istemedikleri.....	64

Çizelge 4.16. Otonom araç bozulduğunda kullanıcıların yardım çağırma ve arıza hakkında bilgi gönderebilme durumunda verilerini paylaşacağı yol yardım servisini seçmek isteyip istemeyecekleri.....	65
Çizelge 4.17. Otonom araç kullanıcılarının kaydedilen veriler ile alakalı hukuki bir düzenleme gerekip gerekmediği ile alakalı düşünceleri.....	65
Çizelge 4.18.Otonom araç alanında çalışan uzmanların gizlilik ve kişisel verilerin korunması çerçevesinde görüşleri.....	66



ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 2.1. LiDAR (Işık Algılama ve Mesafe Ölçme) Sensörü.....	15
Şekil 2.2.Kamera Sensörü.....	16
Şekil 2.3. Radar Sensörü.....	16
Şekil 2.4. Ultrasonik sensörler.....	17
Şekil 2.5. GPS (Küresel Konumlandırma Sistemi) Sensörü.....	18
Şekil 2.6. IMU (Atalet Ölçüm Birimi).....	18
Şekil 2.7. Otonom Araçlarda Veriye Yönelik Kullanılan Teknoloji.....	19
Şekil 2.8. Kabin İçi İzleme Sonucu Elde Edilen Görsel Verilerin İşlenmesinde İzlenebilecek Yollar.....	23
Şekil 4.1. Risk temelli yaklaşıma göre yapay zeka sistemleri risk kategorileri.....	53

1.GİRİŞ

Otonom sistemlerin yaygınlaşmasıyla birlikte, bu sistemler tarafından toplanan ve işlenen kişisel verilerin güvenliği de önemli bir konu haline gelmiştir. Bu tezde, otonom sistemlerin gizlilik ve kişisel verilerin korunması açısından incelenmesi amaçlanmaktadır. Otonom sistemler, kişisel verileri çeşitli şekillerde toplayabilirler. Örneğin, otonom araçlar, konum, hız, rota ve diğer sürüş verilerini toplarlar. Akıllı evler, kullanıcıların hareketlerini, tüketim alışkanlıklarını ve diğer kişisel bilgilerini toplarlar. Sağlık hizmetleri alanında kullanılan otonom sistemler, hastaların sağlık bilgilerini toplarlar. Üretim alanında kullanılan otonom sistemler ise çalışanlarının performans verilerini toplarlar.

Otonom sistemler tarafından toplanan kişisel veriler, farklı amaçlarla kullanılabilir. Örneğin, otonom araçların verileri, trafik güvenliğini sağlamak için kullanılabilir. Akıllı evler tarafından toplanan veriler, enerji verimliliğini artırmak için kullanılabilir. Sağlık hizmetleri alanında kullanılan otonom sistemler tarafından toplanan veriler, hastalıkların teşhis ve tedavisi için kullanılabilir. Üretim alanında kullanılan otonom sistemler tarafından toplanan veriler, verimliliği artırmak ve maliyetleri düşürmek için kullanılabilir.

Otonom sistemler tarafından toplanan kişisel verilerin yetkisiz kişiler tarafından ele geçirilmesi, bireylerin mahremiyetlerine ve güvenliklerine zarar verebilir. Örneğin, otonom araçların verileri, kullanıcıların hareketlerini izlemek ve takip etmek için kullanılabilir. Akıllı evler tarafından toplanan veriler, kullanıcıların alışkanlıklarını öğrenmek ve onları hedefli reklamlarla bombardıman etmek için kullanılabilir. Sağlık hizmetleri alanında kullanılan otonom sistemler tarafından toplanan veriler, hastaların sağlık bilgilerinin çalınması ve kullanılması için kullanılabilir. Üretim alanında kullanılan otonom sistemler tarafından toplanan veriler, çalışanların performansını izlemek ve onları baskı altına almak için kullanılabilir.

Bu çalışmada otonom sistemler gizlilik ve kişisel verilerin korunması çerçevesinde ele alınarak, diğer otonom sistemlere göre gündelik hayatta daha sık kullanılan otonom araçların topladıkları veri türleri ve bu araçlardaki mahremiyet türleri açıklanacaktır. Ayrıca otonom araçların veriye yönelik mimarisi izah edilerek bu araçlarda mahremiyete yönelik kullanılan yöntemler açığa kavuşturulacaktır.

Problem durumu

Otonom sistemler, insan müdahalesi olmadan kendi başlarına karar verebilen ve hareket edebilen sistemlerdir. Otonom araçlar, otonom sistemlerin en yaygın uygulamalarından biridir. Otonom araçlar, genellikle sensörler, yapay zeka ve kontrol sistemleri kullanarak çevresel koşulları değerlendirir ve bu bilgileri temel alarak hareket eder. Bu otonom fonksiyonlar, sürücüsüz araçlar gibi ulaşım sistemlerinde ve endüstriyel otomasyon uygulamalarında kullanılmaktadır.

Yapay zekanın gelişmesiyle birlikte robotlar ve otonom sistemler hayatımıza dahil olmuştur. Yakın gelecekte hayatlarımızın ayrılmaz birer parçası olacakları tahmin edilmektedir. Otonom sistemler hayatımızı kolaylaştırır da beraberinde bazı problemleri de getirmektedir. Çalışmamızda otonom sistemlerin gizlilik ve kişisel veriler açısından insan hayatında yaratabileceği problemler ele alınarak, bu alanda çalışmakta olan uzmanların görüşlerinden ve kullanıcıların düşüncelerinden faydalanılmıştır.

Otonom sistemler, büyük miktarda veri üretme, toplama ve işleme yeteneği ile bilinir. Otonom araçlar, trafik koşullarını algılamak, yolları takip etmek ve diğer araçlarla güvenli bir şekilde etkileşim kurmak için çeşitli sensörlere ve yazılımlara sahiptir. Bu sensörler ve yazılımlar, otonom araçların çevresini ve yolcularını izlemek için iç ve dış ortamlardan sürekli olarak veri toplar. Bu durum, bireylerin özel hayatlarının gizliliğini tehlikeye atabilir. Kişisel veri ise bireylerle ilgili her türlü bilgiyi ifade eder. Bu kavramlar, hukuki ve etik açıdan korunmalıdır, çünkü bireylerin özel hayatlarının gizliliği temel bir insan hakkıdır. Sürücü ve yolcu davranışlarından, çevresel koşullara kadar bir dizi veri, araç tarafından sürekli olarak analiz edilir. Bu durum, bireylerin kişisel verilerinin nasıl kullanılacağı konusunda endişelere yol açmaktadır.

Otonom sistemlerin özel hayatın gizliliği ve kişisel verilerin korunması açısından oluşturduğu başlıca problemler; veri toplama, veri depolama ve veri kullanımı çevresinde yoğunlaşmaktadır. Otonom sistemler, çevreyi ve yolcuları izlemek için çeşitli sensörlere sahiptir. Bu sensörler, konum, hız, yön, yüz tanıma, ses tanıma gibi kişisel verileri toplayabilir. Bu veriler, otonom sistemlerin çalışması için gerekli olsa da, üçüncü kişiler tarafından kötüye kullanılabilir. Ayrıca otonom sistemler tarafından toplanan veriler, genellikle bulut tabanlı depolama sistemlerinde saklanır. Bu verilere üçüncü kişilerin

erişimi, özel hayatın gizliliği açısından bir tehdit oluşturabilir. Toplanan veriler, trafik koşullarını analiz etmek, otonom araçları geliştirmek veya reklam hedeflemek için kullanılabilir. Bu kullanımlar, özel hayatın gizliliğine müdahale edebilir.

Otonom sistemlerin kullanımıyla ilgili hukuki çerçeve, genellikle mevcut veri koruma ve gizlilik düzenlemelerine dayanır. Çalışmamızda Türkiye’de ve Avrupa Birliği’nde bu alandaki hukuki çalışmalara yer verilmiştir. Ancak, otonom araçlar gibi yeni teknolojiler ortaya çıktıkça, mevcut düzenlemelerin yetersiz kaldığı ve bu teknolojilere özgü yeni düzenlemelere ihtiyaç duyulduğu görülmektedir.

Araştırmanın amacı

Bu tez, otonom sistemlerin kullanımıyla birlikte ortaya çıkan gizlilik risklerini ve kişisel verilerin korunması ihtiyaçlarını ele almayı amaçlamaktadır. Bu inceleme, uzman görüşleri, kullanıcı deneyimleri ve hukuki çerçevenin incelenmesi yoluyla gerçekleştirilecek çoklu perspektiflerin sentezini hedefler. Otonom sistemlerin yaygınlaşmasıyla birlikte, bu sistemlerin toplumda ve bireylerde potansiyel etkilerini, özellikle de kişisel mahremiyetin korunması bağlamında, detaylı bir şekilde anlamayı amaçlamaktadır. Bu bağlamda, veri güvenliğinin, kullanıcı haklarının ve özel yaşamın korunmasını sağlayacak yöntemlerin ve politikaların geliştirilmesine yönelik öneriler sunulması planlanmaktadır. Tez, mevcut mevzuatın otonom sistemlerin sunduğu zorluklarla nasıl uyumlu hale getirilebileceğini ve bu alandaki boşlukların nasıl doldurulabileceğini araştırarak, ileriye dönük politika önerileri geliştirmeyi amaçlamaktadır.

Bu genel amaca ulaşabilmek için belirlenen alt amaçlar ise şunlardır:

1. Gizlilik ve kişisel verilerin korunmasına ilişkin hukuki düzenlemeler;

1.1. Türkiye’de gizlilik ve kişisel verilerin korunmasına ilişkin hukuki düzenlemeler nelerdir?

1.2. Avrupa Birliği’nde gizlilik ve kişisel verilerin korunmasına ilişkin hukuki düzenlemeler nelerdir?

2. Otonom araçlarla ilgili hukuki düzenlemeler;

2.1. Türkiye’de otonom araçlarla ilgili hukuki düzenlemeler nelerdir?

2.2. Avrupa Birliği’nde otonom araçlarla ilgili hukuki düzenlemeler nelerdir?

3. Otonom araçlarda gizlilik ve kişisel verilerin korunması çerçevesinde kullanıcıların görüşleri nelerdir?
4. Otonom araçlarda gizlilik ve kişisel verilerin korunması çerçevesinde uzmanların görüşleri nelerdir?
5. Otonom araçlarda mahremiyete ilişkin olası problemler nelerdir?

Araştırmanın önemi

Otonom sistemler, kullanıcıların konumları, hareketleri, sağlık durumları gibi kişisel verileri toplayabilmektedir. Bu veriler, otonom sistemlerin performansını iyileştirmek, kullanıcılara daha iyi hizmet sunmak için kullanılabilir. Ancak, bu verilerin kötü niyetli kişiler tarafından ele geçirilmesi halinde, kullanıcıların mahremiyetinin ihlali, kimlik hırsızlığı, dolandırıcılık gibi ciddi sorunlara yol açabilmektedir.

Bu nedenle, otonom sistemlerin gizlilik ve kişisel verilerin korunması konusunda uygun bir şekilde tasarlanması ve kullanılması gerekmektedir. Çalışmada, günlük hayatta en yaygın olarak gördüğümüz otonom sistemlerden olan otonom araçların topladığı veri türleri ile mahremiyet türleri açıklanarak, bu verilerin gizliliğinin korunması için alınabilecek önlemler ele alınacaktır.

Tez çalışmasının amacı, otonom sistemlerin gizlilik ve kişisel verilerin korunması konusunda farkındalık yaratmak ve bu alandaki çalışmalara katkı sağlamaktır. Çalışmanın sonucunda, otonom sistemlerin gizliliğinin korunması için alınabilecek önlemler konusunda önerilerde bulunulacaktır.

Bu tez çalışması, otonom sistemlerin gizlilik ve kişisel verilerin korunması konusunda önemli bir katkı sağlayacaktır. Çalışma, otonom sistemlerin geliştirilmesinde ve kullanılmasında dikkat edilmesi gereken hususları ortaya koyacaktır. Çalışma, otonom sistemlerin güvenilir ve güvenli bir şekilde kullanılması amacıyla yapılacak çalışmalara katkı sağlayacaktır.

Varsayımlar

Bu tez çalışmasında, aşağıdaki varsayımlara dayanılmıştır:

- Otonom sistemler, kullanıcıların konumları, hareketleri, sağlık durumları gibi kişisel verileri toplamaktadır.
- Bu veriler, otonom sistemlerin performansını iyileştirmek, kullanıcılara daha iyi hizmet sunmak için kullanılmaktadır.
- Bu verilerin kötü niyetli kişiler tarafından ele geçirilmesi halinde, kullanıcıların mahremiyetinin ihlali, kimlik hırsızlığı, dolandırıcılık gibi ciddi sorunlara yol açabilmektedir.
- Otonom sistemlerin gizlilik ve kişisel verilerin korunması konusunda uygun bir şekilde tasarlanması ve kullanılması gerekmektedir.

Bu varsayımların geçerliliği, tez çalışmasının bulguları ile test edilecektir.

Sınırlılıklar

Bu tez çalışması, otonom sistemleri gizlilik ve kişisel verilerin korunması açısından incelemektedir. Çalışma, otonom sistemlerin detaylı teknik özellikleri, güvenlik özellikleri gibi konuları kapsamamaktadır. Ayrıca otonom araç alanındaki çalışmalar daha gelişmiş ve yaygın iken, diğer otonom sistemler alanındaki çalışmalar ise henüz başlangıç aşamasındadır. Bu sebeple, çalışma;

1. Otonom araç sektöründe çalışmakta olan ulaşılabilen uzman görüşleri ile,
2. Ulaşılabilen seviye 3 otonom araç kullanıcılarının görüşleri ile sınırlıdır.

Çalışmada, otonom araç sistemlerinin ürettiği kişisel veriler arasında, kullanıcıların konumları, hareketleri, araç içi kamera görüntüleri gibi veriler yer almaktadır. Otonom sistemlerin diğer alanlarında üretilen kişisel veriler, çalışmanın kapsamı dışında kalmıştır. Örneğin, sağlık alanında kullanılan otonom sistemler, kullanıcıların sağlık verilerini toplayabilmektedir. Üretim alanında kullanılan otonom sistemler, çalışanların kişisel verilerini toplayabilmektedir. Bu tür veriler, çalışmanın kapsamına dahil edilmemiştir. Ayrıca çalışmada, otonom araç sistemlerinde kişisel verilerin gizliliğinin korunması için alınabilecek önlemler genel olarak incelenmiştir. Ancak, bu önlemlerin teknik boyutuyla da ayrıntılı olarak incelenmesi gerekmektedir. Örneğin, otonom araç sistemlerinde kullanılan

şifreleme teknolojileri, kullanıcıların verilerini nasıl korumakta ve bu önlemlerin etkinliği nasıl test edilmektedir gibi sorular, çalışmanın kapsamı dışında kalmıştır.

Bu sınırlamalar, çalışmanın gelecekteki çalışmalar için bir yol haritası oluşturmaya olanak sağlamaktadır. Gelecekteki çalışmalarda, otonom sistemlerin diğer alanlarında çalışan uzmanlara ve kullanıcılara da ulaşılması, çalışmanın kapsamının genişletilmesi ve daha kapsamlı sonuçlar elde edilmesi sağlanabilir.

Tanımlar

-Otonom Sistemler; kendi kararlarını verebilen ve eylemlerini gerçekleştirebilen, insan müdahalesi olmadan çalışabilen sistemlerdir. Otonom araçlar, akıllı evler, sağlık hizmetleri ve üretim gibi birçok farklı alanda kullanılmaktadır.

-Kişisel Veri; bireylerin kimliklerini, konumlarını, hareketlerini ve tercihlerini ortaya çıkaran bilgilerdir. Ad, soyad, doğum tarihi, adres, telefon numarası, e-posta adresi, fotoğraf, sağlık bilgileri, finansal bilgiler vb. kişisel verilere örnek olarak verilebilir.

-Gizlilik; bireyin mahremiyetinin korunmasıdır. Bireylerin kişisel ve duygusal alanlarının korunması anlamına gelir. Bireyin kişisel verilerinin yetkisiz kişiler tarafından erişilmesinden, kullanılmasından veya paylaşılmasından korunmasıdır.

-Kişisel Verilerin Korunması; kişisel verilerin yetkisiz kişiler tarafından erişilmesinden, kullanılmasından veya paylaşılmasından korunmasıdır. Kişisel verilerin toplanması, işlenmesi, saklanması ve paylaşılması gibi süreçlerin, ilgili kanun ve düzenlemelere uygun olarak yürütülmesidir.

2.KURAMSAL ÇERÇEVE VE İLGİLİ ARAŞTIRMALAR

Bu bölümde araştırmanın problemini açıklamaya yönelik kuramsal bilgiler verilerek, araştırma konusu ile ilgili Türkiye’de diğer ülkelerde yapılmış araştırmalara yer verilmiştir.

2.1. Kuramsal Çerçeve

Bu bölümde, araştırmanın problemi ile doğrudan ilgili konulara ilişkin kuramsal bilgiler verilmeye çalışılmıştır. Bu amaçla kuramsal çerçeve mahremiyet, kişisel veri, otomatik sistem, otonom sistem, makine etiği alt başlıklarında incelenmiştir.

2.1.1.Mahremiyet

Mahremiyet kavramı 1890 yılında; Almanya’da eğitim görmesi nedeniyle, kendisini Almanya’daki şahsiyet haklarıyla ilgili eğiten Brandeis ve Warren tarafından kaleme alınan son derece önemli makaleden türemiştir. Bu makalede mahremiyet; “kişinin tek başına kalabilmesi” olarak dile getirilmiş, yani günümüzde yaygın olarak zikredilen bir hak olarak “yalnız bırakılma hakkı” tanımlanmıştır. (Warren, Brandeis, 1890). Özel yaşamın korunması, bir hak olarak ilk defa bu çalışmada ortaya atılmıştır. (Cate, 2003) En geniş anlamıyla bu anlayışta özel yaşamın gizliliği, kişinin duygu ve düşüncelerini başkalarıyla hangi kapsamda paylaşmak istediğiyle ilgilidir. (Yüksel, 2012)

TDK’ya göre mahremiyetin kelime anlamı “gizlilik”tir. Genellikle mahremiyet (privacy) özel hayat anlamında da kullanılmakta ise de bu teriminin özel hayat kavramının yalnızca bir yönünü oluşturduğu, bundan dolayı bu terimin özel hayat kavramı yerine kullanılmaması gerektiği görüşünü savunanlar da vardır. (Üzeltürk, 2004) Mahremiyet kavramının gelişen teknoloji ve şartlar ile birlikte geniş bir çerçeveye sahip olduğu ve sınırlarının çizilmesinin zorlaştığı bir gerçektir. Bu kavram hukuki düzenlemelerle de koruma altına alınmış, ihlali durumunda cezalar öngörülmüştür. Söz konusu kavramın ceza hukuku ile koruma altına alınması sonucunda, suçta ve cezada kanunilik ilkesi gereğince bu kavramın tanımlanması ve içeriğinin belirlenmesi zorunluluğunu doğmuştur.

Anayasa Mahkemesi’ne göre özel hayat, geniş bir kavram olup kapsayıcı bir tanımının yapılması oldukça zordur. Bununla beraber bu kavram; kişinin maddi ve manevi bütünlüğü,

fiziksel ve sosyal kimliği, bireyin ismi, cinsel yönelimi, cinsel yaşamı gibi unsurları korumaktadır (Ahmet Acartürk, B. No: 2013/2084, 15/10/2015, § 46). Özel hayatın gizliliği hakkı kapsamında korunan hukuksal çıkarlardan biri de bireyin mahremiyet hakkıdır. Ancak mahremiyet hakkı sadece yalnız bırakılma hakkından ibaret olmayıp bu hak, bireyin kendisi hakkındaki bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Bireyin; kendisine ilişkin herhangi bir bilginin kendi rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılamaması; kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır. Bu husus, bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkına işaret etmektedir (AYM, E. 2009/1, K. 2011/82, 18/5/2011; Işıl Yaykır, B. No: 2013/2284, 15/4/2014, § 37).

2.1.2.Kişisel veri

Mahremiyet kavramıyla birlikte kişisel veri kavramı gündeme gelmektedir. Kişisel verilerin korunması anlayışının altında mahremiyet anlayışı yer almaktadır. (Korkmaz, 2020) Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder (Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) m. 4/1; Kişisel Verilerin Korunması Kanunu (KVKK) m. 3/1-d).

Mahremiyet; özel hayatın gizliliği ve kişisel verilere yönelik ulusal ve uluslararası düzenlemelerde yer almıştır.

2.1.3.Otomatik sistemler ve otonom sistemler

Otonom sistemlerin her bir meslek dalı açısından farklı tanımlanabileceği söylenebilir. “Otonom”un tanımını yapmak gerekirse; çalışma sırasında beklenmedik olaylara tepki olarak davranışlarını değiştirebilen sistemler şeklinde tanımlanabilir. (Watson ve Scheidt, 2005) Otonom sistemler, dışarıdan uzun süre boyunca herhangi bir etki olmadan faaliyet gösterebilen sistemler şeklinde tanımlanabilir. (Ersoy, 2020) Bir diğer tanıma göre ise otonom sistemler, kendi başlarına karar verebilen ve bu kararları belirli hedeflere uygun olarak uygulayabilen, çevresel koşullara adapte olabilen ve diğer sistemlerle iletişim kurabilen sistemlerdir ve insan müdahalesine ihtiyaç duymadan görevlerini yaparlar. (Güleç ve Benzer, 2020) Otonom sistemlerin gelişmesine öncülük eden otomatik sistemler ile otonom sistemler birbirlerinden farklıdır. Otomatik sistemler her ne kadar dışarıdan

müdahale olmadan süreçlerine devam edebilmekte iseler de tek başlarına karar alma mekanizmalarının olduğu söylenemez. Bunun yanında otonom sistemler, otomatik sistemlerin ötesinde kendi amacını belirleme ve bu amaç doğrultusunda kendi başlarına karar alabilen, kendisini geliştirebilen sistemlerdir. (Kapancı ve Retornaz 2021) Otomatik ve otonom bir sistem arasındaki en önemli fark, sistemin kendi kendine öğrenip öğrenemediği ve kendi kendini geliştirip geliştiremediğidir. Bir sistem, belirlenmiş kurallara göre hatasız hareket ettiğinde otonom sistem değil otomatik sistem olarak adlandırılır. Otonom sistem, hedefe ulaşmak için çevreyi, sistemin durumunu ve görevi anlamının yanı sıra doğru bir şekilde algılayabilmeli ve yargılayabilmeli, ilgili hedeflere ulaşabilmek için bağımsız olarak işleyerek sistemin kendisini ve durumu muhakeme edebilmeli ve farklı eylemleri formüle edip seçebilmelidir. Şu anda tamamen otonom bir sistem bulunmamaktadır. Ancak dünyanın dört bir yanındaki akademisyenler otonom sistemin hedefini tanımlamışlardır. (Chen, Wen, Zhu, Huang, Xiao, Wei, Hahn, 2021)

Çizelge 2.1. Otomatik ve Otonom Sistem Karşılaştırması

Otomatik Sistem	Otonom Sistem
Dışarıdan müdahale olmaksızın süreçlerine devam edebilirler.	Dışarıdan müdahale olmaksızın süreçlerine devam edebilirler.
Tek başına karar alma mekanizması yok.	Tek başına karar alma mekanizması var, amaç belirleyebilir ve bu doğrultuda kendini geliştirebilir.

2.1.4.Makine etiği

Makine etiği (makine ahlakı, yapay ahlak veya hesaplama etiği olarak da bilinir), bilgisayarlarda ve robotlarda ahlaki karar verme yetilerini uygulamayı amaçlayan, gelişmekte olan bir alandır. (Allen, Wallach, Smit, 2006) Bir başka deyişle makine etiği, kendi keline karar verebilen sistemlerin ahlaki sorunlarına odaklanan bir disiplindir. Bu disiplinde, yapay zeka sistemleri ve robotlar gibi otonom sistemlerin insanlarla olan etkileşimleri, insanlarla birlikte nasıl çalışabileceği, ahlaki kararları alma süreçleri ve etik ilkeleri ele alınır. Makine etiği, otonom sistemlerin insanların ahlaki değerlerine uygun şekilde tasarlanması gerektiğini savunarak Otonom Yapay Ahlaki Ajanlar (OYA-Autonomous Artificial Moral Agents (AMA)) olarak adlandırılan etik kuralları ve insanların ahlaki değerlerini sistemin parçası olarak işleyebilen, kendi kararlarını bu çerçevede vererek

eylemlerini yönlendirebilen yapay zeka sistemlerinin geliştirilmesi gerektiğini vurgular. OYA (AMA)'lar, doğru ve yanlış arasında ayırım yapabilen, ahlaki değerlere uyan ve insanların güvenebileceği kararlar verebilen yapay zeka sistemleri olarak tasarlanmıştır. Örneğin, bir robot, bir insan işçinin güvenliğini tehlikeye atabilecek bir hata yaptığında, üretimi durdurarak tehlikeyi uzaklaştırabilir. Robotun bu kararı verebilmesi, bireyin hayatının, üretim ile kıyaslandığında daha önemli olduğu bilgisinin sisteme işlenmiş olmasından kaynaklanır.

Makine etiği alanında çalışan araştırmacılar, belirli durumlarda yapılması gereken doğru eylemin ne olacağını bağımsız olarak kendi kendine belirleyebilen sistemlerin tasarlanması ve geliştirilmesi için çalışmaktadırlar (Vakkuri, Kemell, Kultanen, Abrahamsson, 2020). Zamanla karmaşılaşan akıllı sistemler, özerkleşerek insan kontrolü olmaksızın kendi kendine çalışabilecek otonom sistemlere doğru evrilmektedir. Bu durum, kendi kendilerine karar alarak uygulayabilen otonom sistemlerin aldıkları kararların ve fiillerinin ne kadar etik olduklarını sorgulatmaktadır. (Canbay, Demircioğlu, 2021)

Makine etiği konusunun, tez konumuzla ilgisi olduğundan bu konuya da kısaca değinmek gerekmiştir. İnsan müdahalesi olmaksızın kendi başlarına karar alarak uygulayabilen otonom sistemlerin karar verme mekanizmasının insanların etik değerleri ile paralellik göstermesi gerektiğini savunan bir disiplin olan makine etiği, felsefe alanında çalışmakta olan uzmanlar ile yapay zeka alanında çalışmakta olan uzmanların iş birliği yaptığı bir araştırma alanı olup, (Pană, Cizmeci, 2022) otonom sistemler ile ilgili bütün alanları ilgilendiren bir disiplindir.

2.1.5.Otonom araç seviyeleri

Bir aracın otomasyon derecesini belirleyebilmek için pek çok kuruluş farklı çerçeveler düzenlemiştir. Amerika merkezli bir kuruluş olan Otomotiv Mühendisler Derneği (SAE), J3016 Standart'ı sadece Amerika'da değil, aynı zamanda Avrupa Parlamentosu ve Avrupa Komisyonu belgelerinde, Avustralya ve Yeni Zelanda dahil olmak üzere Anglofon ülkelerde ve Birleşik Krallık'ta geniş çaplı kabul görmüştür. (Hopkins, Schwanen, 2021) Ancak SAE dışında Amerika'daki Ulusal Karayolu Trafik Güvenliği İdaresi (National Highway Traffic Safety Administration- NHTSA) ve Almanya'daki Alman Federal Karayolu Araştırma

Enstitüsü (Bundesanstalt für Straßenwesen-BAST) tarafından da otonom araç seviyeleri sınıflandırılmıştır. Bu üç sınıflandırmaya da çalışmamızda yer verilecektir.

Öncelikli olarak genel kabul gören Otomotiv Mühendisler Derneği (SAE), J3016 Standart'ına göre otonom araç seviyeleri açıklanacaktır. “Karayolu Motorlu Taşıtlar için Sürüş Otomasyon Sistemlerine İlişkin Terimlerin Sınıflandırılması ve Tanımları” isimli standart Otomotiv Mühendisler Derneği (SAE) tarafından 2014 yılında yayınlanarak 2018 yılında güncellenme yapılmıştır. SAE International (Society of Automotive Engineers), Amerika Birleşik Devletleri merkezli bir kuruluştur. 1905 yılında Henry Ford, Andrew Lawrence Riker, Edward Birdsall ve John Wilkinson tarafından kurulmuştur. SAE International, havacılık, otomotiv ve ticari araç endüstrilerinde çalışan mühendisler ve ilgili teknik uzmanları temsil eden küresel bir profesyonel birlik ve standartlar geliştirme kuruluşudur. Derneğin amacı, güvenli, temiz ve erişilebilir mobilite çözümleri sağlamak için mobilite bilgisini ve çözümlerini iletme ve iletme. Otomotiv Mühendisler Derneği (SAE), J3016 Standart'ı ile karayolundaki motorlu araçların otonom derecelerini 6 seviyede incelemektedir. (Bayındır, 2021)

Seviye 0- Otomatik yönlendirme yok (no driving automation): Aracın hem yatay hem dikey hakimiyetinin (gaz, fren, direksiyon) sürücüde olduğu, sürücünün hem aracı hem de yolu izlemek zorunda olduğu ve sürüş yardımcı sistemlerinin bulunmadığı seviyedir.

Seviye 1- Sürücü yardımı (driver assistance): Bu seviyede sürücünün yönlendirmesiyle aracın hızlanması ve yavaşlaması mümkündür, dikey hakimiyetin veya otomatik park sistemi gibi sistemler aracılığıyla yatay hakimiyetin devredilebildiği seviyedir. Ancak aracın yatay ve dikey hakimiyeti aynı anda sisteme devredilmemektedir. Bu seviyede aracın hâkimiyeti yine tamamen sürücüdedir.

Seviye 2- Kısmi otomatik yönlendirme (partial driving automation): Bu seviyede, yardımcı bir veya birden çok sistem aynı anda çalışabilmektedir. Hem yatay hem dikey hakimiyet sisteme bırakılabilmektedir. Bunun anlamı, sürücü ayaklarını gaz pedalından ve ellerini direksiyondan çekebilecektir. Seviye 0, 1 ve 2’de sürücü aracı kullanırken herhangi bir aksilikte araç hâkimiyetini devralacak şekilde hazır bulunmalıdır. Sürücünün dikkati her zaman yolda ve araçta olmalıdır.

Seviye 3- Koşullu otomatik yönlendirme (conditional driving automation): Bu seviyede araçta yine sürücü bulunmalıdır ancak bazı koşullarda, örneğin trafik olduğunda sürücü bütün hâkimiyeti otomatik pilota devredebilecek direksiyon hâkimiyeti, hız, yol kontrolü, seyir takibini sisteme bırakılabilecektir. Sürücü dikkatli olmalı ve ihtiyaç olduğunda sürüş

kontrolünü devralmalıdır. Seviye 2 ve Seviye 3 arasındaki fark, sürücü seviye 3'te sürüş sırasında sürekli olarak sürüşü takip etmek zorunda değildir.

Seviye 4- Yüksek otomatik yönlendirme (high driving automation): Hem yatay hem dikey hakimiyet artık sistemdedir. Sürücünün direksiyonu kontrol etme, ayaklarını pedalda bulundurma veya sürekli sürüşü izleme zorunluluğu yoktur. Sistem, insan müdahalesi olmadan sürüşü gerçekleştirebilir. Seviye 3 ve Seviye 4'te sürücü, sürücü koltuğunda otursa bile aracı kullanmayacaktır. Ancak Seviye 3'te acil durumlarda aracın kontrolünü sürücünün devralması beklenmekteyken, Seviye 4'te sürücünden bu beklememektedir.

Seviye 5 – Tam otomatik yönlendirme (full driving automation): Seviye 5 “sürücüsüz araç” olarak adlandırılan tam otonom seviyesidir. Her zaman ve her koşulda aracın tüm yatay ve dikey hakimiyeti sistemdedir. Tam otomatik yönlendirme sistemi devrede iken, aracın hakimiyetinin araç içindeki kimselerce devralınmasına gerek yoktur. (Buğra, 2020)

İkinci olarak, Amerika'daki Ulusal Karayolu Trafik Güvenliği İdaresi (National Highway Traffic Safety Administration- NHTSA) otonom araç seviyelerini 0'dan 4'e kadar 5 seviyede ele almıştır. Buna göre;

Seviye 0- Otomasyon yok (no-automation): Sürücü her zaman ana araç kontrollerinin (fren pedalı, direksiyon, gaz pedalı) tam ve tek kontrolüne sahiptir ve yolun izlenmesinden ve tüm araç kontrollerinin güvenli bir şekilde çalıştırılmasından tek başına sorumludur. Belirli sürücü destek/kolaylık sistemlerine sahip ancak direksiyon, frenleme veya gaz pedalı üzerinde kontrol yeteneği olmayan araçlar bu kategorizasyona göre yine "seviye 0" araçlar olarak kabul edilecektir.

Seviye 1- Fonksiyona özel otomasyon (function-specific automation): Sürücü genel kontrole sahiptir ve kullanımdan tek başına sorumludur, ancak otomatik sistem, belirli normal sürüş veya çarpışmanın kaçınılmaz olduğu durumlarda (örneğin acil durumlarda dinamik fren desteği) sürücüye yardımcı olmak için ek kontrol sağlayabilir. Araç, bireysel sürücü desteği ve çarpışmadan kaçınma teknolojilerini birleştiren birden fazla yeteneğe sahip olabilir ancak sürücünün dikkatinin yerini almadığı gibi sürüş sorumluluğunu da sürücünün üzerinden almaz. Sürücünün ellerini direksiyondan ve ayaklarını pedallardan çekerek fiziksel olarak aracı kullanmaktan kurtulmasını sağlayan, uyum içinde çalışan bir araç kontrol sistemi kombinasyonu mevcut değildir. Fonksiyona özel otomasyon sistemlerine örnek olarak şunlar verilebilir; hız sabitleyici, otomatik frenleme ve şerit takip sistemi.

Seviye 2- Birleşik fonksiyon otomasyonu (combined function automation): Sürücü hala yolu izlemekten ve sürüşten sorumludur. Ayrıca her zaman anlık kontrol için hazır olması

beklenir. Sistem önceden uyarıda bulunmadan kontrolü bırakabileceğinden, sürücünün aracı güvenli bir şekilde kontrol etmeye hazır olması gerekir. Seviye 2 birleşik fonksiyonlara örnek olarak şerit merkezleme sistemi verilebilir. Seviye 1 ve Seviye 2 arasındaki en önemli fark, Seviye 2'de sistemin tasarlandığı belirli çalışma koşullarında, sürücünün ellerini direksiyondan ve ayağını pedaldan aynı anda çekerek aracı fiziksel olarak kullanmasını engelleyecek şekilde otomatik bir çalışma modunun etkinleştirilebilmesidir.

Seviye 3- Sınırlı sürücüsüz otomasyon (limited self-driving automation): Bu otomasyon seviyesindeki araçlar, sürücünün belirli trafik veya çevre koşullarında güvenlik açısından kritik tüm işlevlerin tam kontrolünü devretmesine ve bu koşullarda sürücü kontrolüne geri dönülmesini gerektiren değişiklikleri izlemek için büyük ölçüde araca güvenmesine olanak tanır. Sürücünün ara sıra kontrole hazır olması beklenir. Araç, otomatik sürüş modu sırasında güvenli seyri sağlayacak şekilde tasarlanmıştır. Örnek olarak, yol çalışması gibi sistemin artık otomasyonu destekleyemediği durumları belirleyebilen ve ardından sürücüye sürüş görevine yeniden başlaması için sinyal veren ve sürücüye manuel kontrolü güvenli bir şekilde yeniden devralması için uygun bir devralma süresi sağlayan otomatik veya kendi kendine giden bir araç verilebilir. Seviye 2 ile seviye 3 arasındaki en önemli fark, seviye 3'te aracın, sürücünün sürüş sırasında yolu sürekli olarak izlemesinin beklenmeyeceği şekilde tasarlanmış olmasıdır.

Seviye 4- Tam sürücüsüz otomasyon (full self-driving automation): Araç, güvenlik açısından kritik tüm sürüş işlevlerini gerçekleştirmek ve tüm yolculuk boyunca yol koşullarını izlemek üzere tasarlanmıştır. (NHTSA)

Üçüncü olarak Almanya'daki Alman Federal Karayolu Araştırma Enstitüsü (Bundesanstalt für Straßenwesen-BAST) otonom araç seviyelerini 3 seviyede ele almıştır. Buna göre;

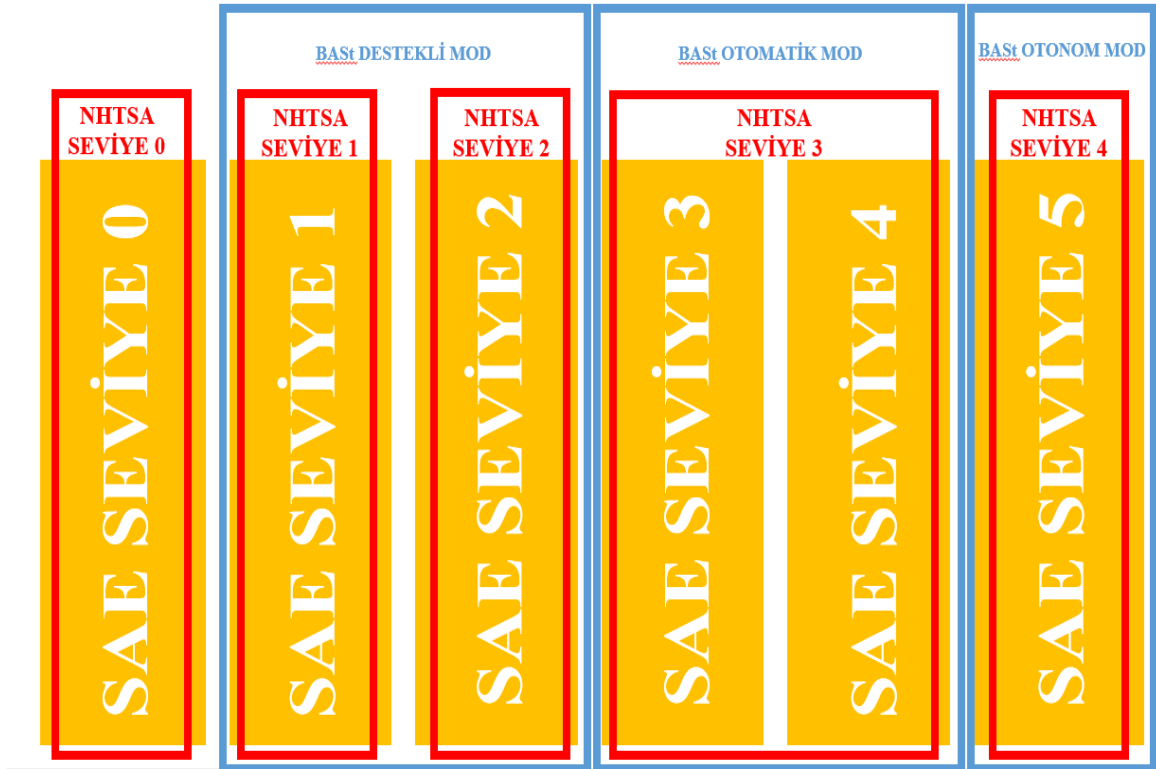
Destekli mod (assisted mode): Sürücü destek sistemleri, dikey ve yatay araç hareketini kontrol etmede sürücüyü destekler. Örneğin, bu sistemler aracı şeritte tutabilir. Ancak bu destek sistemleri mevcut hız sınırlarını algılayamayabilir veya şerit işaretleri olmadığında anlık destek sağlayamayabilir. Bu nedenle sürücünün sistemi denetlemesi ve çevreyi sürekli olarak izlemesi ve gerekirse herhangi bir durumda sistemi devralmak için müdahale etmesi gerekir. Bu nedenle, sürücü uzun bir süre boyunca böyle hissetmese bile, sürüşten hala sürekli olarak sorumludur. Örnek olarak; BMW profesyonel sürüş asistanı ve Tesla otomatik pilot verilebilir.

Otomatik mod (automated mode): Otomatik modda sürücü, aracın aktif sürücüsü rolünden çıkarılır. Bu nedenle otomatik moddaki sürücüler "kullanıcı" haline gelir. Sistem aracı

kontrol ederken kullanıcı, sürüşle ilgili olmayan görevler olarak adlandırılan, sürüş göreviyle hiçbir ilgisi olmayan diğer faaliyetlere yönelebilir. Kullanıcının, sistemin sürüş görevini istediği zaman devralma taleplerine karşı takipte olması gerekir. Bu, örneğin bir kullanıcının otomatik modda uykuda olması durumunda güvenilir bir şekilde mümkün olmayacaktır. Bu nedenle uyumak, kullanıcı rolünü ihlal eder ve bu seviyede mümkün değildir. Örnek olarak; Audi yapay zeka destekli trafik sıkışıklığı pilotu verilebilir.

Otonom mod (autonomous mode): Otonom sürüş sırasında sistem tüm sürüş görevini üstlenir. Bir yolculuk otonom modda yürütüldüğü sürece, araçtaki tüm kişiler yolcudur ve sürüşle ilgili hiçbir görevleri yoktur. Örnek olarak; Monheim'daki (NRW) otonom otobüsler verilebilir. (BASt)

Çizelge 2.2. Otonom Araç Seviyeleri Sınıflandırmalarının Karşılaştırması



2.1.6. Otonom araçların veriye yönelik mimarisi

Çevrelerinde gerekli tespitleri yaparak karar verebilmeleri ve navigasyon ile yol almaları için, otonom araçlar çeşitli sensörlerle donatılmıştır. (Campbell, O'Mahony, Krpalcova, Riordan, Walsh, Murphy, Ryan, 2018)

2.1.6.1.Otonom araçlarda sensör teknolojisi

Otonom araçlar, farklı sensör teknolojileri ile donatılmıştır.

2.1.6.1.1.Harici sensörler (Dışsal duyuşal sensörler) (Exteroceptive sensors)

Otonom araçlardaki sensörlerin ana görevi, araç çevresi hakkında en güvenilir ve sürekli bilgileri sağlamaktır. Özellikle bu sensörlerin yoldaki sürülebilir alanlar hakkında bilgi vermesi ve yol seviyesinin üzerindeki kaçınılması gereken tüm engelleri bildirmesi beklenir. Bu nedenle sensörlerin araçlar, yayalar, direkler ve korkuluklar gibi çeşitli tipik nesneleri algılaması, yerini belirlemesi ve sınıflandırması gerekir. Araç çevresi hakkında kapsamlı ve doğru bilgilere tek bir pratik sensörle ulaşılamaz. Bu nedenle, otonom araçlar tipik olarak birçok sensör ile donatılmıştır. (Bilik, Longman, Villeval, Tabrikian, 2019)

2.1.6.1.1.1.LiDAR (Işık algılama ve mesafe ölçme)

Işık Algılama ve Mesafe Ölçme (Light Detection and Ranging) yaygın kullanılan adı ile LiDAR; oldukça yaygın ve çeşitli kullanım alanlarına sahip bir lazer tarama sistemidir. LiDAR teknolojisi; tarım, arazi modellemesi, haritalama, orman yönetimi, ulaşım, sel risk analizleri ve akarsu izleme, mevcut yapıların modellenmesi, arkeoloji ve robotik gibi pek çok alanda kullanılmaktadır. LiDAR sistemleri, yüksek yoğunluklu lazer ışınlarının bir nesneye gönderilmesi ve yansıması sonucu gidip gelen ışının süresini ölçerek mesafe hesaplanması işlemine dayanmaktadır. (Çalışır, 2021) Bu sistem, bir uzaklık ölçüm tekniğidir. LiDAR, aynı zamanda nesnelerin yüzeylerinden yansıyan ışının yoğunluğa göre nesnelerin renkleri, dokuları ve malzeme özellikleri hakkında da bilgi verir. Bu ölçümler, nokta bulutu olarak adlandırılan 3 boyutlu bir veri kümesinde kaydedilir. Otonom araçlarda bu sistem, araçların çevrelerinde gerekli tespitleri yapmalarına ve navigasyon ile yol almalarına olanak sağlarlar.



Şekil 2.1. LiDAR (Işık Algılama ve Mesafe Ölçme) Sensörü (Horton, 2019)

2.1.6.1.1.2.Kamera

Aracın çevresinin görüntülerini, videosunu kaydeder. Otonom araçlar, çeşitli işlevler için farklı kameralar ile donatılmışlardır. Örneğin, araba takibi için ön görüş kamerası, şerit değiştirme için yan görüş kamerası ve park için arka görüş kamerası vb. (Xie, Cao, Long, Yang, Zhao, Li, 2022)



Şekil 2.2.Kamera Sensörü (Horton, 2019)

2.1.6.1.1.3.Radar

İnsan sürücü görüşüne benzediği için kameralar, otonom sürüş için en doğal sensörler olabilir. Maliyetleri düşüktür ve nesnelerin rengi ve dokusu ile birlikte çevre hakkında yoğun ve zengin bilgiler sağlayan küçük bir forma sahiptirler. Ancak kameraların önemli eksiklikleri vardır; ışığa ve hava koşullarına karşı duyarlıdırlar. Bu nedenle kameraların, arkasında bulunan şeffaf bir malzeme veya cam panel gibi bir yüzeye takılması gerekir. Bu şekilde, kameranın çalışması sırasında etkilenebileceği toz, nem veya diğer zararlı unsurlardan korunabilir. Bunun yanı sıra kameralar doğrudan mesafe ve hız ölçümleri sağlamazlar. Kameranın aksine, radarlar olumsuz hava koşullarına karşı dayanıklıdır, ışık değişimlerine karşı duyarsızdır, uzun mesafeleri doğru bir şekilde ölçebilir ve şeffaf olmayan bir yüzey arkasına kolayca yerleştirilebilir. (Bilik, Longman, Villeval, Tabrikian, 2019)



Şekil 2.3. Radar Sensörü (Horton, 2019)

2.1.6.1.1.4.Ultrasonik

Ultrasonik sensörler engelleri algılar ve çevreyi yüksek frekanslı ses dalgalarıyla aktif bir şekilde inceleyip yankılarını alarak nesnelerin konumlarını ve mesafeyi ölçer. Ultrasonik sensörler, aracın yakınında bulunan nesneleri tespit etmek ve engelleri algılamak için kullanılır. Bu sensörler, özellikle park etme ve geri manevra yapma gibi düşük hızlarda çalışırken otonom araçların çevrelerini algılamasına yardımcı olur. Park sensörleri açısından, Avrupa ve Asya'daki yeni araçların yarısından fazlasında arka park sensörleri bulunmaktadır ve Hindistan hükümeti, geriye doğru giderken çarpma riskini azaltmak için yakında tüm yeni araçların bu tür sensörlerle donatılmasını zorunlu kılacağını açıklamıştır. (Xu, Yan, Jia, Ji, Liu, 2018).



Şekil 2.4. Ultrasonik sensörler (Jahromi, 2019)

2.1.6.1.2.Dahili sensörler (Kendinden duyuşal sensörler) (Proprioceptive sensors)

2.1.6.1.2.1.GPS (Küresel konumlandırma sistemi)

GPS, yani Global Positioning System; “küresel konumlandırma sistemi” anlamına gelen sözcüklerin baş harflerinden oluşan kısaltmadır. GPS uydularından en az 3 ya da yükseklik bilgisi de gerekiyor ise 4 tanesinden gelen hassas atomik saat sinyalleri sayesinde dünya üzerindeki bir konumu bulabilen cihazlardır. GPS, Amerika Birleşik Devletleri’nin geliştirdiği küresel bir konumlandırma hizmetidir. GPS’in dışında Rusya’nın geliştirmiş olduğu GLONASS, Hindistan’ın geliştirmiş olduğu IRNSS, Çin’in geliştirmiş olduğu BeiDou (BDS) ve Avrupa ülkelerinin geliştirdiği Galileo gibi küresel konumlama sistemleri de kullanılmaktadır. Tüm bu sistemlerin birleşimine de Global Navigation Satellite System (küresel uydu seyrüsefer sistemi, GNSS) ismi verilmektedir. (Başer, 2022)



Şekil 2.5. GPS (Küresel Konumlandırma Sistemi) Sensörü (Horton, 2019)

2.1.6.1.2.2.IMU (Atalet Ölçüm Birimi)

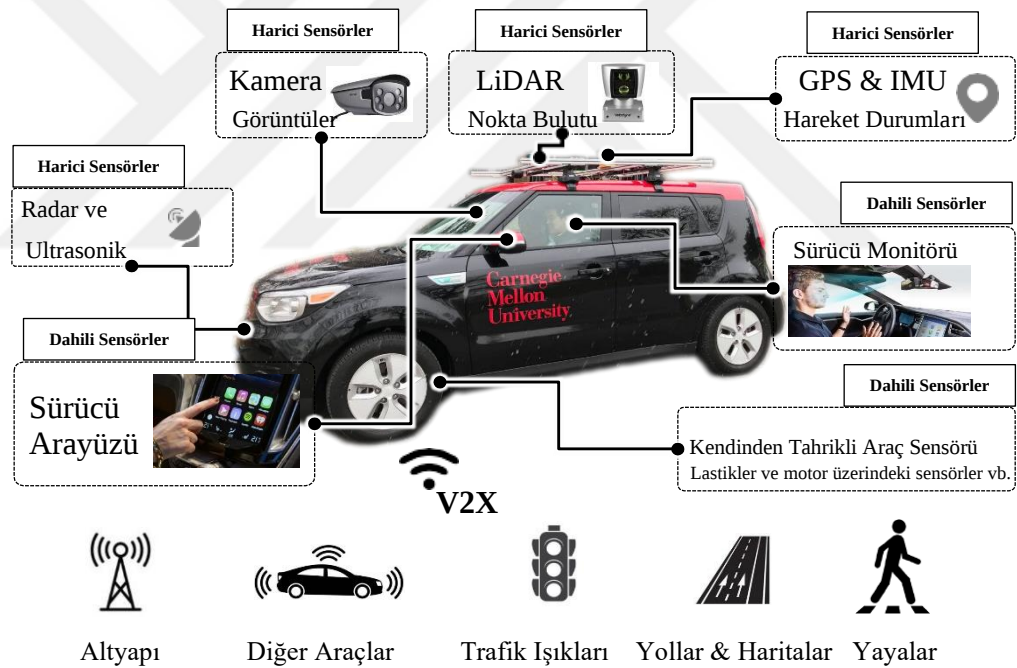
IMU yani Inertial Measurement Unit; atalet ölçüm birimidir. Hız, ivme, yönelim ve bazen dönme hızı gibi hareket parametrelerini ölçmek için kullanılan bir elektronik cihazdır. Bu cihazlar, günümüzde insansız hava araçları (İHA'lar), uzay araçları, robotlar gibi otonom sistemlerde konum belirleme, hareket kontrolü ve stabilizasyon gibi birçok hareketli platformun hareketinin stabilize edilmesinde, sanal gerçeklik (VR) ve artırılmış gerçeklik (AR) başlıkları gibi hareket tabanlı kullanıcı arayüzlerinde, spor analizi uygulamalarında, navigasyon sistemlerinde ve daha birçok alanda IMU'lar önemli bir rol oynarlar. Uzayda hareket halindeki bir cismin üstünde oluşan 3 eksen ivme ve 3 eksen dönme kuvvetini ölçmek için bir takım sensörlerden oluşmaktadır. IMU'nun temel bileşenleri genellikle üç eksenli bir jiroskop, üç eksenli bir ivmeölçer ve bazen üç eksenli bir manyetometredir. Bu sensörler, cihazın hareketine ilişkin verileri ölçer ve bu verileri birleştirerek cihazın konumunu, hızını, ivmesini ve yönelimini hesaplar. Jiroskoplar, cihazın dönme hızını ölçer. İvmeölçerler, cihazın ivmesini ve yerçekimi etkilerini tespit eder. Manyetometreler ise cihazın manyetik alan içindeki konumunu belirler. (Başer, 2022)



Şekil 2.6. IMU (Atalet Ölçüm Birimi) (Teschler)

2.1.6.1.2.3.Kodlayıcılar

Kodlayıcılar (encoders), tekerleklerin dönme hareketini algılamak ve ölçmek için kullanılan cihazlardır. Bu kodlayıcılar, tekerleklerin konumunu, hızını ve dönüş açısını belirlemek için kullanılır. Kodlayıcılar genellikle tekerleğin şaftına veya motorun çıkışına monte edilir. Tekerlek veya motor döndüğünde, kodlayıcı belirli bir sayıda darbe üretir. Bu darbeler, dönme hareketinin miktarını ve yönünü temsil eder. Kodlayıcılar, otonom araçlarda hareket kontrol sistemlerine geri bildirim sağlamak için kullanılır. Bu geri bildirim, tekerleklerin konumunu ve hızını doğru bir şekilde takip etmeyi ve aracın istenen hareketlerini sağlamayı mümkün kılar. Örneğin, araçların konum ve hızını hassas bir şekilde kontrol etmek, rota planlaması, engel algılama ve çevreyle etkileşim gibi otonom araçlardaki önemli işlevlerin yerine getirilmesine yardımcı olur.



Şekil 2.7. Otonom Araçlarda Veriye Yönelik Kullanılan Teknoloji (Xie, Cao, Long, Yang, Zhao, Li, 2022)

2.1.6.2.V2X (Araçtan- Her Şeye)

V2X (Vehicle-to-Everything) teknolojisi içinde yer alan birkaç farklı iletişim türü:

-Araçtan-Araca (V2V): Bu iletişim türü, araçlar arasında doğrudan iletişim kurmayı sağlar. Örneğin, bir araç sürücüsü, önündeki araç sürücüsüne bir uyarı mesajı gönderebilir veya

araçlar birbirlerine konum ve hız bilgisi gibi verileri paylaşabilirler. V2V teknolojisi, trafik kazalarını önlemek, trafik akışını iyileştirmek ve sürüş güvenliğini artırmak gibi birçok fayda sağlar.

-Araçtan-Altyapıya (V2I): Bu iletişim türü, araçlar ile yol altyapısı arasında iletişim kurmayı sağlar. Örneğin, bir araç trafik ışıklarının durumunu altyapıya bağlı olarak önceden öğrenebilir ve bunu sürücüsüne bildirerek trafik sıkışıklığını azaltabilir. Bu teknoloji, trafik yönetimini iyileştirmek, emisyonları azaltmak ve enerji verimliliğini artırmak gibi birçok fayda sağlar.

-Araçtan-Yolcuya (V2P): Bu iletişim türü, araçtaki yolcularla iletişim kurmayı sağlar. Örneğin, bir araçtaki sürücü, yolcularına yol durumu veya varış saatleri hakkında bilgi verebilir. Bu teknoloji, yolculukları daha konforlu ve keyifli hale getirir.

-Araçtan-Ağa (V2N): Bu iletişim türü, araçların internete bağlanarak bir ağa entegre olmasını sağlar. Örneğin, bir araç internet bağlantısı üzerinden trafik durumu, hava durumu veya navigasyon güncellemeleri gibi verilere erişebilir. Bu teknoloji, sürücülerin yolculuk sırasında internete bağlı kalmalarını sağlar ve sürücülerin yolculukları sırasında dijital hizmetlerden yararlanmalarını mümkün kılar.

2.1.7. Otonom araçlarda toplanan veri türleri

Otonom bir aracın, belirtilen hedefe güvenli ve doğru yoldan gitmesi beklenir. Bunun için otonom araç hem çevreden hem de sürücüden sürekli olarak çeşitli veriler toplamak zorundadır. Bu veriler açısından da veri mahremiyetinin ihlali riski vardır. (Xie, Cao, Long, Yang, Zhao, Li, 2022).

-Dış Algılama Verileri; aracın dış çevresindeki nesneleri algılayan sensörler (harici sensörler) tarafından toplanan verileri ifade eder. Aracın çevresindeki nesneleri algılayan harici sensörler güvenli sürüş deneyimi sunmasının yanında veri de toplamaktadır. Bu veriler, aracın dış ortamını izlemek için LiDAR, radarlar, kameralar ve ultrasonik dahil olmak üzere harici sensörler yardımıyla toplanır. (Xie, Cao, Long, Yang, Zhao, Li, 2022).

-İç Algılama Verileri; aracın içindeki sensörler (dahili sensörler) tarafından toplanan verileri ifade eder.

-Araçtan- Her Şeye Verileri (V2X Data); araçların birbirleriyle ve çevreleriyle iletişim kurmalarına olanak tanıyan bir teknolojidir. V2X verileri, araçların konumları, hızları, ivmeleri ve diğer önemli parametreleri gibi birçok farklı bilgiyi içerebilir. Bu veriler, araçlar

arasında ve araçlar ile altyapı arasında (yani yol işaretleri, trafik ışıkları, otoyol sistemleri vb.) paylaşılabılır.

Bağlı arabalar (Connected Cars) hangi verileri izleyebiliyor?

Merkezi Brüksel'de bulunan FIA (Fédération Internationale de l'Automobile) Avrupa, Orta Doğu ve Afrika'dan 113 otomobil ve tur kulübü ile onların 37 milyon üyesini temsil eden bir tüketici organıdır. FIA, teknik, yasal ve kamuoyu çalışması yürüterek bağlı arabalarla ilgili “My Car My Data” ismini verdiği bir çalışma yürütmüştür. Çeşitli araba markalarını inceleyerek piyasada mevcut bağlı araba firmalarının, kullanıcıların hangi verilerini izleyebildiğini tespit etmiştir.

Çizelge 2.3. Araç Modellerine Göre Kaydedilen Veriler (MEP, Verhofstadt)

<i>İzlenen Veri Türü</i>	<i>BMW 320d</i>	<i>Mercedes B-Serisi</i>	<i>Renault Zoe</i>	<i>BMW i-3</i>
<i>Sürücü Profili</i>	•Sürücünün farklı sürüş modlarını kullandığı süre •Ani kopma nedeniyle emniyet kemerlerinin sıkılması •Yapılan yolculuk sayısı ve kat edilen kilometre miktarı	•Ani kopma nedeniyle emniyet kemerlerinin sıkılması •Şehir içi/otoyol koşullarında kilometre	•Pilin şarj durumu	•Sürüş modu •Araba nasıl ve nerede şarj edildi
<i>Araç konumu</i>	•Navigasyon sistemine girilen son hedefler	•Aracın GPS konumu (her 2 dakikada bir)	•GPS konumu (istek üzerine sağlanır ve maksimum 30 dakikalık aralıklarla gönderilir)	•Son 100 park yeri •Sürücünün başka bir ulaşım şekline (tren/otobüs)

				bağlı olduğu yer
<i>Bakım bilgileri</i>	•Maksimum motor devri •Kilometre okuma •Araç farlarının durumu	•Yüksek motor devri sayısı •Kilometre okuma •Yakıt tüketimi ve seviyesi •Lastik basıncı	•Yüksek voltajlı akünün şarj seviyesi ve hücre voltajı	•Pil şarjının kalitesi •Kilometre okuma •Şarj fişi kullanımı
<i>İletişim bilgileri</i>	•Cep telefonlarından senkronize edilen kişisel bilgiler			

FIA, otomobil üreticilerinin her bir model için toplanan, işlenen, depolanan ve harici olarak iletilen tüm araç verilerini bir liste halinde yayınlaması gerektiğini ve bu listenin, tüketiciler tarafından kolayca erişilebilir ve anlaşılır olması gerektiğini belirtmiştir.

2.1.8.Otonom araçlarda mahremiyet türleri

Otonom araçlarda mahremiyet türleri pek çok farklı yönden ele alınarak farklı başlıklarda incelenebilir. Otonom araçlarda mahremiyet türleri, çalışmamızda esas olarak üç başlık altında ele alınmıştır:

-Bireysel Mahremiyet: Aracın içerisinde bulunan sürücü ve yolculardan elde edilen verilerin mahremiyetini ifade eder. Örneğin; araca bağlanan telefonda elde edilen veri, araç içi kamerası ile elde edilen görüntüler bu mahremiyet kapsamında ele alınır.

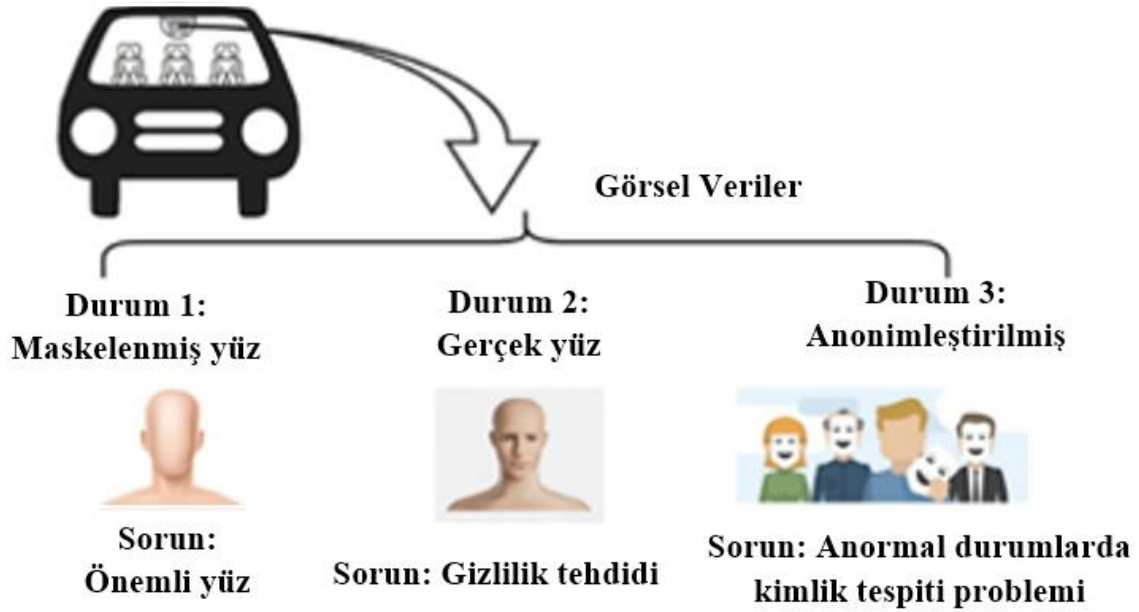
- Topluluk Mahremiyeti: Aracın çevresinde bulunan yayalardan ve çevreden elde edilen verilerin mahremiyetini ifade eder. Örneğin; aracın dışında bulunan kameralar vasıtasıyla aracın yanından geçen yayaların görüntüleri, çevredeki diğer araç plaka bilgileri, eğer araç kamerası yakındaki bir konutun içerisini görebiliyorsa konuttaki kişilerden elde edilen görüntüler bu mahremiyet kapsamına girer.

-Araç Üreticisinin Sahip Olduğu Özel Bilgi Mahremiyeti; Bu bilgi, ticari sırlar, patentler, telif hakları, işlem yöntemleri, veri tabanları gibi birçok farklı konuyu içerir.

2.1.9.Otonom araçlarda mahremiyete yönelik kullanılan yöntemler

2.1.9.1.128D (128-Dimensional face embedding)

Kabin İçi İzleme



Şekil 2.8. Kabin İçi İzleme Sonucu Elde Edilen Görsel Verilerin İşlenmesinde İzlenebilecek Yollar (Mishra, Cha, Kim, 2022)

Yüzleri bulanıklaştırmak, maskelemek veya yüzler üzerinde bir yama oluşturmak, diğer tüm yüz anonimleştirme yaklaşımlarından biraz daha kolaydır; ancak, bu yöntemler yüz bilgisinin önemli ölçüde kaybolmasına neden olur. Bu durum da hırsızlık, şiddet gibi otonom araçta yaşanabilecek anormal durumlarda şüphelinin kimliğini tespit etmeyi zorlaştırmaktadır.

128 boyutlu yüz gömülmesi özelliği, anonimleştirilmiş bir alanda doğru yüz tanıma için önemli bir yöntemdir. Bir çift kimliğin (orijinal ve anonimleştirilmiş) saklanması kavramı, herhangi bir gizlilik tehdidi olmaksızın yeniden tanımlamaya yol açar. Sadece 128D kimlik özellikleri ile orijinal yüzü bilmek mümkün değildir. Yeniden tanımlama için hem orijinal görsel giriş hem de kimlik gereklidir. Bulutta, orijinali ile anonimleştirilmiş görsel birlikte

saklanır. Bu nedenle, gizlilik ihlali tehdidi yoktur. Akıllı şehirlerde yüz tanıma için yaygın uygulamalar olacağı öngörülmektedir.

“128-dimensional face embedding” yani 128 boyutlu yüz gömülmesi (embedding), yüz tanıma veya yüz benzerlik karşılaştırmalarında kullanılan bir tekniktir. Bir yüzün özelliklerini tanımlayan ve her yüz için özgün bir 128 sayı dizisi oluşturan bir algoritmadır. Yüz gömülmesi algoritması, bir yüzün fotoğrafını alır ve o fotoğraftaki yüz özelliklerini analiz ederek her bir özelliği belirli bir sayısal değere dönüştürür. Bu işlem sonucunda her yüz için özgün bir 128 boyutlu sayı dizisi elde edilir. Bu sayı dizisi, aynı kişiye ait farklı yüz fotoğrafları arasındaki benzerlikleri belirlemek veya farklı kişilere ait yüz fotoğraflarını karşılaştırmak için kullanılabilir. Yüz gömülmesi algoritması, güvenlik sistemleri, sosyal medya uygulamaları ve yüz tanıma teknolojileri gibi birçok farklı alanda kullanılmaktadır.

128 boyutlu yüz gömülmesi, bir yüzün özelliklerini tanımlayan sayısal bir ifade olduğu için, bir resimle aynı boyutta değildir. Dolayısıyla, 128 boyutlu yüz gömülmesi ile orijinal resim arasında doğrudan bir karşılaştırma yapılamaz.

Bir yüzü anonimleştirmek için, öncelikle yüz gömülmesi algoritması kullanılarak yüzün 128 boyutlu sayı dizisi elde edilir. Daha sonra, bu sayı dizisi, orijinal yüz fotoğrafı yerine kullanılabilir. Bunun nedeni, 128 boyutlu yüz gömülmesinin bir yüzü tanımlamak için yeterli bilgiye sahip olmasıdır, ancak yüzün kendisine ilişkin detaylı bilgi içermemesidir.

Yüzün anonimleştirilmesi sırasında, 128 boyutlu yüz gömülmesi, yüzü benzersiz bir şekilde tanımlayabilirken, yüzün kendisine ilişkin bilgileri gizli tutar. Bu sayede, anonimleştirilmiş yüz fotoğrafı, orijinal yüz fotoğrafına göre daha az kişisel bilgi içeren bir hale gelir.

128 boyutlu yüz gömülmesi sayısal bir ifade olduğu için, orijinal yüz fotoğrafını tekrar elde etmek mümkün değildir. Yüz gömülmesi algoritması, bir yüzün benzersiz özelliklerini sayısal olarak kodlar, ancak bu kodlama orijinal yüz fotoğrafının kendisi değildir. Dolayısıyla, yüz gömülmesi ile elde edilen fotoğraftan, orijinal yüz fotoğrafını geriye döndürmek mümkün değildir.

Ancak, anonimleştirilmiş bir video kaydı, bir suç işlendiği takdirde delil olarak kullanılabilir ve yasal süreçte kullanılmak üzere saklanabilir. Yüzlerin anonimleştirilmesi, kişisel

bilgilerin korunmasını amaçlar ve yüzlerin tekrar tanımlanmasını zorlaştıracak şekilde tasarlanmıştır.

2.1.9.2.MMFE (Morphable model-based facial exchange)

Morphable model-based facial exchange (MMFE), yüz modelleme teknolojileri kullanılarak gerçekleştirilen bir yüz değiştirme işlemidir. Bu yöntem, bir kişinin yüzünden başka bir kişinin yüzüne geçiş yapmak için kullanılır.

MMFE, yüz modelleri oluşturmak için kullanılan morphable model (şekil değiştirilebilir model) adı verilen bir teknolojiyi temel alır. Bu model, bir yüzü 3D geometrik şekil ve yüzey özellikleri olarak tanımlar. Bu şekil ve yüzey özellikleri, bir yüz görüntüsünü oluşturan piksellerin aksine, yüzeyi geometrik olarak tanımlayan verilerdir.

MMFE, öncelikle iki ayrı yüz modeli oluşturur. Birincisi, hedef olarak belirlenen kişinin yüz modelidir. İkincisi ise kaynak olarak kullanılacak yüz modelidir. Daha sonra, iki yüz modeli arasındaki farklılıklar ve benzerlikler analiz edilir ve bu analiz sonucunda bir geçiş modeli oluşturulur. Bu geçiş modeli, iki yüz modeli arasındaki farklılıkları ve benzerlikleri birbirine karıştırarak, kaynak yüzünden hedef yüze doğru bir yüz değiştirme işlemi gerçekleştirir. MMFE, video efektleri ve diğer dijital sanat işlemlerinde yaygın olarak kullanılır. Ayrıca, güvenlik alanında da kullanılabilmektedir.

MMFE sırasında kaynak yüz modelinin orijinal görünümü kaybolur ve sonuçta elde edilen yüz modeli, kaynak yüz modeli ve hedef yüz modelinin bir karışımıdır. Bu nedenle, MMFE ile oluşturulan yüz modelinin orijinal yüz modelinden geriye dönük olarak elde edilmesi mümkün değildir.

2.1.9.3."De-Identification" (Anonimleştirme) "Release-And-Forget" (Yayınlama ve unutma) Modeli

"De-identification release-and-forget model", veri gizliliği ve güvenliği ile ilgili olan bir terimdir ve kullanıcıların kişisel verilerini korumak amacıyla kullanılan bir yöntemi ifade eder.

"De-identification" (anonimleştirme), kişisel verilerin kimlik bilgilerini gizleme veya ortadan kaldırma sürecini ifade eder. Bu, kullanıcıların kimliklerini belirlemek için kullanılabilecek bilgileri kaldırmak veya değiştirmek suretiyle verilerin anonim hale getirilmesini içerir.

"Release-and-forget" (yayınlama ve unutma), anonimleştirilmiş verilerin bir kez yayınlanıp daha sonra unutulduğu bir yöntemi ifade eder. Yani, veriler bir kez anonimleştirildikten sonra yayınlanır ve daha sonra kaynak sistemlerden veya orijinal veri kaynaklarından silinir veya erişim engellenir.

"De-identification release-and-forget model" yaklaşımı, kullanıcıların gizlilik ve güvenliklerini korumak için kullanılmaktadır ve kişisel verilerin yetkisiz erişim veya kötüye kullanıma karşı korunmasına yardımcı olur. Özellikle veri paylaşımı veya araştırma amaçları için kullanıldığında, de-identification release-and-forget modeli, kullanıcıların gizliliğini korurken aynı zamanda anonimleştirilmiş verilere erişimin kolaylaştırılmasına yardımcı olabilir.

"De-identification release-and-forget model" terimi, Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation - GDPR) kapsamında yer almaktadır. Anonimleştirme, GDPR'ın temel prensiplerinden biri olan veri koruma ilkesine (uygunluk ilkesi) uygun olarak, kişisel verilerin gizliliğini ve güvenliğini sağlamak için kullanılır. GDPR'ye göre, anonimleştirilmiş veriler, artık kişisel veri olarak kabul edilmez ve GDPR'ın uygulanabilir olduğu bazı yükümlülüklerden muaf tutulabilir.

2.2.İlgili Araştırmalar

Araştırmanın amaçlarına cevap bulabilmek için Türkiye’de YökTez, Dergi Park, uluslararası alanda IEEE, Springer veri tabanlarında bulunan tez ve makalelerden yararlanılmıştır. Veri tabanlarında; “otonom sistem”, “otonom araç”, “kişisel veri”, “privacy in autonomous vehicles” kavramları anahtar kelime olarak kullanılmıştır. Bu kapsamda 1 kitap ve 12 makale belirlenmiş ve tamamına ulaşım sağlanmıştır. Bu alanda yapılan araştırmalara, tarihleri dikkate alınarak önce Türkiye’de sonra da diğer ülkelerde yapılanlar şeklinde yer verilmiştir.

2.2.1.Gizlilik ve kişisel veriler ile ilgili yapılan araştırmalar

Çelik (2017) tarafından; özel hayatın gizliliği, kişisel verilerin korunması ve unutulma hakkı olmak üzere; bu üç temel hakkın birbirleriyle ilgilerini ortaya koyarak genelden özele tümünden gelimsel bir yöntem ile konuyu incelemiştir.

Aşıkoğlu (2018) tarafından, Avrupa Birliği ve Türkiye'deki kişisel verilerin korunması kapsamında mevcut hukuki düzenlemeler incelenmiş, büyük veri uygulamaları bakımından kişisel verilerin korunması ele alınmıştır.

Warren ve Brandeis (1890) tarafından; özel yaşamın korunması, bir hak olarak ilk defa bu çalışmada ortaya atılmış ve mahremiyetin tanımı yapılmıştır.

2.2.2.Otonom sistem ve araçlar ile ilgili yapılan araştırmalar

Buğra (2020) tarafından; karayolları mali sorumluluk (trafik) sigortası yaptırma zorunluluğunun otonom araçlara uygulanabilmesi için ayrıca bir düzenlemeye gerek olup olmadığı, bu tür araçların yol açacağı zararlar için ödeme yapan sigortacının hangi durumlarda kimlere rücu edebileceği ve bu araçların siber rizikolara maruz kalması sonucunda meydana gelen veri kayıpları dışındaki zararların zorunlu karayolları mali sorumluluk (trafik) sigortası ve kasko sigortası teminatı kapsamında olup olmadığı ele alınmıştır.

Bayındır (2021) tarafından; otonom araçların bir türü olan sürücüsüz araçların sözleşme dışı hukuki sorumlulukları ele alınmıştır.

Watson ve Scheidt (2005) tarafından; otonom sistemlerin tarihçesine değinilerek, bu sistemlerin kullanım alanları ile bu sistemlerde kullanılan teknoloji açıklanmıştır.

Campbell, O'Mahony, Krpalcova, Riordan, Walsh, Murphy ve Ryan (2018) tarafından; otonom bir araçta kullanılan ana sensör teknolojileri incelenerek, bu sensörlerin her birinin nasıl çalıştığı, avantajları ve dezavantajları ile otonom araçlar için daha optimum ve verimli bir sistem oluşturmak için sensör füzyon tekniklerinin nasıl kullanılabileceği açıklanmıştır.

Xu, Yan, Jia, Ji ve Liu (2018) tarafından; otonom araçlarda yol durumunu ölçmek ve sürüş kararları vermek için kullanılan sensörler arasında en büyük pazar payına sahip olan ultrasonik sensörler ele alınarak, ultrasonik sensörlerin ve otonom araçların güvenliğini artırmak için iki savunma stratejisi önerilmiştir; sinyalleri fiziksel düzeyde doğrulayan tek sensör tabanlı fiziksel kaydırma kimlik doğrulaması ve sinyalleri sistem düzeyinde doğrulamak için birden fazla sensör kullanan çoklu sensör tutarlılık kontrolü.

Bilik, Longman, Villeval ve Tabrikian, (2019) tarafından; otonom araçlardaki radar teknolojisi ele alınarak geleneksel uygulamaların sınırlamaları vurgulanmış ve alternatif sinyal işleme çözümleri sunulmuş, araç radar performansını artırmak için geleceğe yönelik araştırma önerisinde bulunmuşlardır.

Chen, Wen, Zhu, Huang, Xiao, Wei ve Hahn, (2021) tarafından; otomasyon sistemlerinden otonom sistemlere gelişme sürecini gözden geçirerek tipik otomatik sistemlerin mimarisini sınıflandırmış ve özetlemiş, otonom sistemlerin özellikleri özetlenerek bu özelliklerden gelecekteki ana araştırma yönergeleri ve otonom sistemlerin getirdiği zorluklar ele alınmıştır.

2.2.3.Otonom sistemlerde ve araçlarda gizlilik ve kişisel veri ile ilgili yapılan araştırmalar

Canbay ve Demircioğlu (2021) tarafından; otonom makinelerin üretim ve geliştirme aşamalarında dikkate alınması gereken etik ve ahlaki sorumluluklar ele alınarak, bu sorumluluklara neden ihtiyaç duyulduğu ve bu sorumlulukların karşılanması için sunulan mevcut yaklaşımlar değerlendirilmiştir.

Mishra, Cha ve Kim (2022) tarafından; otonom aracın içerisinde anormal bir durum ile karşılaşıldığında, anonimleştirilmiş sanal bireysel yüzleri yeniden tanımlayabilen, gizliliği koruyan bir kabin içi izleme sistemi önerilmiştir.

Xie, Cao, Long, Yang, Zhao ve Li (2022) tarafından; otonom araçlarda gizliliğe ilişkin riskler ve koruma yöntemleri için yeni bir sınıflandırma sunulmuş, otonom araçlardaki gizlilik kategorize edilerek açıklanmaya çalışılmış, bu mahremiyet düzeylerinin her birini

korumaya yönelik güncel zorluklar sıralanarak, bu zorluklara yönelik mevcut çözümler özetlenmiştir.

Yapılan araştırmalarda, otonom sistemlerin genellikle teknik özellikleri ön plandadır. Bu araştırmalarda, otonom sistemlerin ve otonom araçların nasıl çalıştığını, hangi teknolojileri kullandığını, performansını ve güvenliğini geliştirmek gibi konular ele alınmaktadır. Otonom sistemlerin ve özellikle otonom araçların teknik özelliklerine dair birçok çalışma bulunmaktadır. Ancak, mevcut literatürde gizlilik ve kişisel verilerin korunması konusunda yeterli bir derinlikte ve kapsamda çalışmaların olmadığı gözlemlenmiştir. Otonom sistemlerin teknik özellikleri üzerine yapılan araştırmalar genellikle bu sistemlerin sensör entegrasyonu, yapay zeka algoritmaları, karar alma mekanizmaları gibi teknik yönlerini incelemiştir. Ancak, mevcut literatürde otonom sistemlerin kullanıcıların gizliliğini ve kişisel verilerini nasıl koruyacaklarına dair yeterli bilgi içermeyen bir boşluk bulunmaktadır. Otonom araçlar gibi sistemlerin geniş kapsamlı veri toplama ve işleme faaliyetleri, kullanıcıların mahremiyeti üzerinde potansiyel etkilere sahip olabilir. Bu alandaki eksiklik, otonom sistemlerin halk tarafından daha fazla kabul edilmesi ve güvenilirliğini arttırması için giderilmesi gereken bir zorunluluktur.



3.YÖNTEM

Bu bölümde araştırma modeli, çalışma grubu, veri toplama aracı, verilerin analizine yer verilerek, her bir alt başlıkla ilgili yapılan çalışmalar ayrıntılı bir şekilde açıklanmıştır.

3.1.Araştırmanın Modeli

Araştırma soruların yanıt bulmak amacıyla toplanan verilerde betimsel analiz yöntemleri kullanılmıştır. Betimsel tarama modeli ile yürütülen bu çalışmada, verilerin analiz yöntemi olarak hem nicel hem nitel veri analiz teknikleri kullanılmıştır.

Ayrıca doküman analizi yöntemi kullanılmıştır. Doküman analizi yöntemi, yazılı veya basılı belgelerin içeriğini titizlikle ve sistematik olarak analiz etmek için kullanılan nitel araştırma yöntemlerinden bir tanesidir (Wach, 2013). Bu yöntem, başta basılı ve elektronik dokümanlar olmak üzere tüm belgeleri incelemek ve değerlendirmek için kullanılan sistemli bir modeli ifade etmektedir (Strauss ve Corbin, 1998).

Bu çalışmanın nitel boyutunda uygulama sürecinde elde edilen dokümanlar ile çalışma grubundaki katılımcıların görüşleri yer almaktadır. Başka bir ifadeyle çalışma sürecinde otonom araçlar ile alanda çalışmakta olan katılımcılarla yapılacak görüşmeler araştırmanın nitel verilerine kaynaklık etmektedir.

Nitel araştırmalarda önemli bir veri toplama tekniği olan görüşme daha çok öznel görüşlerin ortaya çıkarılmasında tercih edilir. Merriam'ın (2015) de belirttiği gibi gözlemlenemeyen davranışları, duyguları veya bireylerin dünyayı nasıl anlamlandırıdığını öğrenmek için kullanılır. Görüşme de kendi içinde yapılandırılmış, yarı-yapılandırılmış ve yapılandırılmamış görüşme tekniği olarak alt kategorilere ayrılır. Yarı yapılandırılmış görüşmede, sorular önceden hazırlanmasına karşın görüşme sırasında da soruların yeniden düzenlenmesine ve tartışılmasına (Ekiz, 2017) imkân vermesi nedeniyle araştırmacılar tarafından daha çok tercih edilmektedir. Diğer taraftan görüşme ile bireyin bilgi, duygu ve tutumlarına ilişkin görüşlerini derinlemesine ele alma imkânı sağladığı için de tercih edilmektedir. Bu kapsamda eldeki araştırmanın bu boyutu içinde araştırmacılara sağladığı esneklikten ötürü yarı yapılandırılmış görüşme tekniği kullanılmıştır.

3.2.Çalışma Grubu

Otonom araçlar alanında çalışan üç kişi ile görüşme yapılmıştır. Otonom araçlar alanında çalışan kişi sayısı az olduğundan ancak üç kişiye erişilebilmiştir. Literatür araştırması yapılarak görüşme formundaki sorular hazırlanmış ve çalışma grubuna sorulmuştur.

Seviye 3 otonom araç kullanıcısı 37 kişiye anket soruları yöneltilmiş ve yanıtları alınmıştır. Literatür araştırması yapılarak anket formundaki sorular hazırlanmış ve çalışma grubuna sorulmuştur.

3.3.Verİ Toplama Aracı

Birinci ve ikinci alt amaca yönelik olarak çalışmada doküman inceleme yöntemi kullanılmıştır. Doküman analizi, yazılı belgelerin içeriğini titizlikle ve sistematik olarak analiz etmek için kullanılan bir nitel araştırma yöntemidir (Wach, Ward, 2013). Doküman analizi, basılı ve elektronik materyaller olmak üzere tüm belgeleri incelemek ve değerlendirmek için kullanılan sistemli bir yöntemdir. Nitel araştırmada kullanılan diğer yöntemler gibi doküman analizi de anlam çıkarmak, ilgili konu hakkında bir anlayış oluşturmak, ampirik bilgi geliştirmek için verilerin incelenmesini ve yorumlanmasını gerektirmektedir (Strauss, Corbin, 1998).

Üçüncü alt amaca yönelik olarak çalışmada Araştırmada veri toplama aracı olarak literatür taraması gerçekleştirilmiş ve anket tekniği kullanılmıştır. Seviye 3 otonom araç kullanıcısı olan kullanıcıların görüşlerini almak amacıyla veri toplama aracı olarak araştırmacı tarafından anket formu geliştirilmiştir. Veri toplama aracındaki cümlelere; araştırmacı, alan uzmanları, konu ile ilgilenen öğretim elemanlarının görüşleri alındıktan sonra son şekli verilmiştir ve böylece kapsam geçerliliğinin sağlanmıştır. Tüm bu işlemlerden sonra veri toplama aracı çalışma grubuna uygulanmıştır. Anket 18 adet soru hazırlanmış ve otonom araç kullanıcılarına sorulmuştur.

Dördüncü alt amaca yönelik olarak çalışmada Otonom araçlarda gizlilik ve kişisel verilerin korunması ilişkin uzmanların görüşleri ise araştırmacı tarafından geliştirilmiş yarı yapılandırılmış görüşme formu kullanılmıştır. Araştırma esnasında toplanan veriler yüz yüze kişisel görüşme ile sağlanmıştır. Katılımcılardan derinlemesine bilgi elde etmek amacıyla,

tercih edilen yarı yapılandırılmış görüşme formu, geniş bir alan yazın taraması neticesinde Otonom araçlar konusunda uzmanlar için geliştirilmiştir. İlgili literatür araştırmasına bağlı olarak önce soru havuzu ardından da yarı yapılandırılmış görüşme formu oluşturulmuştur. Formun kapsam geçerliği için en az 3 uzman akademisyenden ve alanda çalışan uzmandan görüş alınmıştır. Uzmanlardan alınan dönütler neticesinde gerekli düzeltmeler yapılmıştır. Son olarak soruların anlaşılabilirliğini kontrol etmek için en az iki deneme görüşmesi yapılarak forma son şekli verilmiştir. Sorularının hazırlanmasında; çalışmanın amacına uygun tür ve sayıda olmasına, açık, anlaşılır, yansız, açık uçlu, betimleyici ve tek amaçlı sorular (Karasar, 1999; Merriam, 2015) olması gibi özelliklere dikkat edilmiştir. Veri toplama aracı olarak görüşme formu 7 adet soru hazırlanmış ve alanda çalışan uzmanlara sorulmuştur.

3.4.Verilerin Analizi

Araştırma kapsamında doküman inceleme yönteminde içerik analizi yapılmıştır. Araştırma kapsamında incelenen YökTez, Dergi Park, IEEE, Springer veri tabanlarından elde edilen çalışmaları kodlama işleminin ardından içerik analizi yapılmıştır. Araştırma kapsamında incelenen çalışmaların kimliği içerik analizi ile oluşturulmuştur. Kullanıcı görüşlerinin belirlenmesi amacı için frekans ve yüzde dağılımları kullanılmıştır. Uzman görüşleri ise nitel olarak değerlendirilmiştir. Ulaşılan sonuçlar bulgular kısmında çalışmalara ait tablo halinde gösterilerek yorumlanmıştır.



4.BULGULAR VE YORUM

Bu bölümde araştırmada ele alınan alt problemler doğrultusunda elde edilen bulgular sunulmuş ve bulgulara dayanılarak yorumlar yapılmıştır.

4.1.Gizlilik ve Kişisel Verilerin Korunmasına İlişkin Türkiye'deki Hukuki Düzenlemelerin İncelenmesi

Mahremiyet hakkı ve insan onuru birbirine bağlı iki teker gibidir. (Javed, Hussain, Maitla)
Bu sebeple de devletler tarafından koruma altına alınmıştır.

Anayasamızın 20., 21. ve 22.maddelerinde “özel hayatın gizliliği ve korunması” ana başlığı altında yer verilmiş olup 20.madde “Özel hayatın gizliliği”, 21.madde “Konut dokunulmazlığı” ve 22.madde “Haberleşme hürriyeti” başlığını taşımaktadır. Anayasamızın 20/3.maddesi “*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.*” diyerek kişisel verilerin korunmasını anayasal güvence altına almıştır. 4721 Sayılı Türk Medeni Kanunu’nun kişiler hukuku başlıklı birinci kitabın gerçek kişiler başlıklı birinci kısmının kişilik başlıklı birinci bölümü 24.maddesi kişilik haklarına karşı saldırıya karşı kişilerin korunmasını konu almaktadır. 4982 Sayılı Bilgi Edinme Hakkı Kanunu’nun “özel hayatın gizliliği” başlığını taşıyan 21.maddesine göre; “*Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır.*” denmektedir.

5237 Sayılı Türk Ceza Kanunu’nun dokuzuncu bölümü “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlığını taşımaktadır. TCK’nın 134.maddesi “Özel hayatın gizliliğini ihlal”, 135.maddesi “Kişisel verilerin kaydedilmesi” ve 136.maddesi “Verileri hukuka aykırı olarak verme veya ele geçirme” başlığını taşımaktadır. Böylece özel hayatın gizliliğine ve

kişisel verilerin korunmasına aykırı fiiller kanunda suç kapsamına alınarak bu haklar koruma altına alınmıştır.

4.1.1.Kişisel verilerin korunması kanunu (KVKK)

6698 Sayılı Kişisel Verilerin Korunması Kanunu’nun 1.maddesinde “*Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.*” Yine bu maddenin gerekçesinde; “*Amaç, kişisel verilerin işlenmesinin disiplin altına alınması ve Anayasada öngörülen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin korunmasıdır. Son yıllarda önem kazanan kişinin mahremiyet hakkı ile bilgi güvenliği hakkının korunması da bu kapsamda değerlendirilmektedir.*” denilmek suretiyle Kanunun çıkış amacının başta özel hayatın gizliliğini korumak olduğu belirtilmiştir.

4.2.Gizlilik ve kişisel verilerin korunmasına ilişkin Avrupa Birliği’ndeki hukuki düzenlemelerin incelenmesi

Kişisel verilerin korunmasına ilişkin dünyada çeşitli ülkelerde hukuki düzenlemeler mevcuttur. Hükümetler, mahremiyet hedeflerini dünyaya duyurmak için uluslararası kabul görmüş ilkeleri kullanmışlardır. Bu ilkeler, Adil Bilgi Uygulama İlkeleri, Adil Bilgi İlkeleri, kısaca "ilkeler" veya en yaygın olarak FIPP'ler (Fair Information Practice Principles-FIPPs) olarak adlandırılır. FIPP'ler, 1970'ler ve 80'lerde popülaritelerinin artmasından bu yana düzenleme için bir çerçeve oluşturulmasına yardımcı olmuştur. O zamandan beri pek çok değişikliğe uğramış olsalar da, FIPP'ler sürekli olarak kişisel bilgiler üzerindeki kontrolü, bilgi yaşam döngüsünü ve bireylerin kişisel bilgileriyle ilgili haklarını vurgulamıştır. FIPP’lerin tarihçesine baktığımızda, ABD’de 1973 yılında HEW (Sağlık, Eğitim, Refah) Otomatik Veri Sistemleri Danışma Komitesi'nin yayınlamış olduğu rapordaki “Adil Bilgi Uygulamaları Kuralları (The Code of Fair Information Practices)” 5 ilkeye kadar götürebiliriz. Bu raporun yayınlanmasından birkaç yıl sonra, ülkelerin ekonomik ve sosyal refahı iyileştirmek için küresel standartlar ve hedefler geliştirmeye teşvik eden uluslararası bir kuruluş olan OECD (Ekonomik Kalkınma ve İşbirliği Örgütü)’nin bu rapordan yola çıkarak oluşturulan 1981 tarihli Gizliliğin Korunmasına ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin OECD İlkeleri ile 8 ilke benimsenmiştir. OECD’nin bu ilkeleri

yayınlandıktan sonra, veri korumaya ilişkin yasal olarak bağlayıcı ilk uluslararası anlaşma, 1981'de Avrupa Konseyi tarafından “Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına İlişkin Sözleşme” (Treaty Office) imzaya açılmıştır. 108 numaralı bu sözleşmenin amacı, taraf ülkelerin OECD’nin belirlemiş olduğu ilkeleri kendi iç yasalarına dahil ederek veri kalitesini korumak, veri güvenliğini sağlamak ve sınır ötesi veri akışını kolaylaştırmaktır. Türkiye de bu sözleşmeyi imzalayan devletlerdendir. Bu sözleşmeden bu yana, küresel olarak kabul edilen hemen hemen her veri koruma yönetmeliği, ilkeleri (FIPP’leri) düzenlemeye yöneliktir. (Saniuk-Heinig, 2021) Avrupa Birliği Genel Veri Koruma Tüzüğü’nün “İlkeler” başlıklı 5.maddesinde, Türkiye’de ise 6698 Sayılı Kişisel Verilerin Korunması Kanunu’nun “Genel ilkeler” başlıklı 4.maddesinde FIPP’ler açıklanmıştır.

-Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi 12. Maddesi’ne göre; “Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılmaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır” (İnsan Hakları Evrensel Beyannamesi, 1949)

-Birleşmiş Milletler’in Kişisel ve Siyasal Haklar Sözleşmesi’nin 17. Maddesi’ne göre; “Mahremiyet Hakkı” (Right to Privacy) şeklinde düzenlenmiştir (Kişisel ve Siyasal Haklar Sözleşmesi, 1966)

-Ekonomik Kalkınma ve İşbirliği Örgütü (OECD-Organization for Economic Co-operation and Development-) 1980’de “Mahremiyetin Korunması ve Sınırışı Veri Akışına Dair Rehber İlkeler” başlıklı metni yayımlamıştır (OECD, 2013).

-Avrupa Konseyi’nin Avrupa İnsan Hakları Sözleşmesi’nin 8. Maddesi özel hayata ve aile hayatına saygı hakkı şeklinde tanımlanmıştır (Avrupa Konseyi, 1950).

-Avrupa Birliği’nin 95/46 sayılı “Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımı” isimli Yönergesi, Birlikteki her üye ülkede kişisel verilerin eşit seviyede korunmasının garanti altına alınmasını amaçlamıştır. Avrupa Komisyonu tarafından üye ülkelerde uygulanmakta olan AB veri koruma kurallarında, Veri Koruma Direktifi’nde benimsenen ilkelerin modernize edilmesi ve gelecekte vatandaşların mahremiyet hakkının garanti altına alınması amacıyla, kapsamlı bir reforma gidilmesi ihtiyacı ortaya çıkmıştır. Bu çerçevede Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihinde “Genel Veri Koruma Tüzüğü (General Data Protection Regulation–GDPR)” onaylanmıştır (Akıncı, 2017).

4.2.1.Avrupa Birlięi genel veri koruma tüzüęü (General data protection regulation-GDPR)

Tüzük, 99 madde ve 173 paragraflık resital bölümünden oluşmaktadır. GDPR’da Başlangıçtan itibaren (privacy by default) ve tasarımdan itibaren veri koruması (privacy by design) yükümlülüęü getirilmiştir ve çalışmamızın konusu gereęi bu yükümlülükleri açıklamak gerekmektedir.

Tasarımdan itibaren veri koruması (privacy by design) Ann Cavoukian tarafından Bilgi ve İletişim Teknolojilerinin ve büyük ölçekli ağ bağlantılı veri sistemlerinin sürekli büyüyen ve sistemik etkilerini ele almak için 90’lı yıllarda geliştirilen bir kavramdır. (Cavoukian, 2009) Başlangıçtan itibaren (privacy by default) ve tasarımdan itibaren veri koruması (privacy by design) yükümlülüęü Avrupa Birlięi Genel Veri Koruma Tüzüęü (GDPR)’nın 25.maddesinde yer almaktadır. Buna göre; veri sorumlusunun kişisel verilerin işlenmesi bağlamında gerçek kişilerin hak ve özgürlüklerinin korunması amacıyla gerekli teknik ve organizasyonel önlemleri alması gerektięi ifade edilmektedir. Bu kapsamda, veri sorumlusu, iç işleyişi ile alakalı politikalarını belirleyerek başlangıçtan itibaren veri koruması (data protection by default) ve tasarımdan itibaren veri koruması (data protection by design) ilkelerini karşılamaya yönelik gerekli tedbirleri almalıdır. Bu ilkeye göre veri sorumlusu, gerek veri işleme vasıtalarının belirlenmesi sırasında gerekse veri işleme anında Tüzük’te öngörülen veri koruma kurallarının etkili bir biçimde uygulanması için gerekli araçları kullanarak, örneğin bulanıklaştırma (pseudonymisation) veya veri minimizasyonu gibi, uygun teknik ve organizasyonel önlemleri almalıdır. (Akıncı, 2017)

Tasarımdan itibaren veri koruması yedi ilkedен oluşmaktadır:

-Cezalandırıcı deęil önleyici, risk gerçekleşdikten sonra deęil risk gerçekleşmeden önce harekete geçen: Reaktif önlemlerden ziyade proaktif önlemlerle karakterize edilir. Buna göre veri sorumlusu, gizlilięi ihlal eden olayları gerçekleşmeden önce tahmin eder ve önler. Tasarımdan itibaren veri koruması, mahremiyet risklerinin gerçekleşmesini beklemey ve mahremiyet ihlallerini meydana geldikten sonra çözmek için çareler sunmaz, bunların meydana gelmesini önlemeyi amaçlar. Kısacası, tasarımdan itibaren veri koruması, olaydan sonra deęil, olaydan önce gelir.

-Varsayılan veri koruması: Kişisel verilerin herhangi bir Bilişim Teknolojileri sisteminde veya iş uygulamasında otomatik olarak korunmasını sağlayarak maksimum düzeyde gizlilik

sağlamayı amaçlar. Bir kişi hiçbir şey yapmazsa, mahremiyeti bozulmadan kalır. Bu ilke uyarınca ilgili kişinin sessiz kalması halinde kişisel verilerinin işlenmesine ilişkin olarak rıza vermediği kabul edilmelidir. Bireyin gizliliğini korumak için herhangi bir işlem yapması gerekmez, varsayılan olarak sistemde yerleşiktir.

-Veri koruma içeren tasarım: Tasarımı bütünsel olarak ele alarak her aşamasında devam eden bir veri korumanın tesisi gerekmektedir. İlke uyarınca başlangıçtan itibaren ve eklenecek olan yeni süreçlerde de devam eden şekilde tarafların çıkarlarının bütünleştirilmesi amaçlamaktadır. Tasarımla mahremiyet, Bilişim Teknolojileri sistemlerinin ve iş uygulamalarının tasarımına ve mimarisine yerleşiktir, dışarıdan bir eklenti değildir. Mahremiyet, işlevselliği azaltmadan sistemin ayrılmaz bir parçasıdır.

-Tam işlevsellik, Pozitif toplamı Sıfır toplamı değil (Positive-Sum, not Zero-Sum): Tasarımla mahremiyet, gereksiz takasların yapıldığı tarihi geçmiş, sıfır toplamı bir yaklaşımla değil, pozitif toplamı “kazan-kazan” tarzında tüm meşru çıkarları ve hedefleri barındırmayı amaçlar. Ya mahremiyet ya güvenlik gibi yanlış ikilemlerin iddiasından kaçınarak her ikisine de sahip olmanın mümkün olduğunu gösterir.

-Uçtan uca güvenlik, Tam yaşam döngüsü koruması: Bir kurum ya da kuruluş içerisindeki kişisel verinin yaşam döngüsü kapsamında, toplamadan imha aşamasına kadar, veri koruma genel ilkeleri ile uyumlu işlenmesini ifade etmektedir. Bu ilke veri güvenliği ile ilgili olan uçtan uca şifreleme ve diğer teknolojiler ile karıştırılmamalıdır. İlke uyarınca güvenlikle beraber genel ilkelerin dikkate alınması gerekmektedir. Bu, tüm verilerin güvenli bir şekilde tutulmasını ve ardından sürecin sonunda, zamanında, güvenli bir şekilde imha edilmesini sağlar. Bu nedenle, tasarımla mahremiyet, uçtan uca, bilginin beşikten mezara, güvenli yaşam döngüsü yönetimini sağlar.

-Görünürlük ve şeffaflık, açık tutun: Kişisel verilerin işlenmesinde yer alan sistemleri ve süreçleri doğrulamaya dayanmaktadır. Kurum ya da kuruluş bünyesinde gerçekleşen süreçlerin şeffaf bir şekilde yürütülmesi ve teknik sistemlerin denetime açık olması gerekmektedir. Tasarımla mahremiyet, ilgili iş uygulaması veya teknoloji ne olursa olsun, aslında bağımsız doğrulamaya tabi olarak belirtilen vaatlere ve hedeflere göre çalıştığına dair tüm paydaşlara güvence vermeyi amaçlamaktadır. Bileşen parçaları ve işlemleri, hem kullanıcılar hem de sağlayıcılar için görünür ve şeffaf kalır. Unutma, güven ama doğru.

-Kullanıcı mahremiyetine saygı, kullanıcıyı merkezde tutma: Kişisel veri işleme süreçlerinin birey merkezli olmasını ve bireye kişisel verileri üzerinde kontrol imkânı tanınmasını, bireyin çıkarlarını en üst düzeyde tutulmasını ifade etmektedir. (Aşıkoğlu, 2018).

4.2.2.Avrupa veri koruma kurulu- kişisel verilerin video cihazları aracılığıyla işlenmesine ilişkin 3/2019 sayılı yönerge

Avrupa Veri Koruma Kurulu, Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)'nın 68.maddesinde bahsedilmektedir ve buna göre; Kurul bu Tüzük'le bir Birlik organı olarak kurulur ve tüzel kişiliğe sahiptir. GDPR'ın 70.maddesi Kurul'un görevleri başlığını taşımaktadır ve 1/e bendinde; *“Kurul bu Tüzük'ün tutarlı bir şekilde uygulanmasını sağlar. Bu amaçla, Kurul, kendi inisiyatifıyla veya üyelerinden birinin talebi üzerine ya da Komisyonun talebi üzerine, bu Tüzük'ün uygulanmasına ilişkin her türlü konuyu inceler ve bu Tüzük'ün tutarlı bir şekilde uygulanmasını teşvik etmek üzere kılavuzlar, tavsiyeler ve en iyi uygulamaları yayınlar.”* Avrupa Veri Koruma Kurulu'nun yayınlamış olduğu Kişisel verilerin video cihazları aracılığıyla işlenmesine ilişkin 3/2019 sayılı Yönerge, GDPR'ın söz konusu maddesi çerçevesinde yayınlanmış olup, tavsiye niteliğindedir. Bu Yönerge, otonom araçlardaki kamera sistemleri için de uygulama alanı bulduğundan, söz konusu Yönerge'nin konumuz ile alakalı maddelerine değinmek gerekmektedir.

Yönerge'nin giriş bölümünde; bireyler, örneğin belirli bir güvenlik amacı için kurulan video gözetimi konusunda rahat olsalar da, tamamen farklı ve veri sahibi için beklenmeyen amaçlarla (örneğin pazarlama amacı, çalışan performansının izlenmesi vb.) kötüye kullanımdan kaçınmak için garantiler alınmalıdır denmiştir. Gizlilik sorunlarına ek olarak, bu cihazların olası arızaları ve neden olabilecekleri önyargılarla ilgili riskler de vardır. Araştırmacılar, yüz tanıma, tanıma veya analiz için kullanılan yazılımın, tanımladığı kişinin yaşına, cinsiyetine ve etnik kökenine göre farklı performans gösterdiğini bildirmişlerdir. Altta yatan amaca ulaşmak için başka araçlar olduğunda, video gözetimi varsayılan olarak bir gereklilik değildir. Aksi takdirde, genel başlangıç olarak mahremiyet eksikliğinin kabul edilmesine yol açan kültürel normlarda bir değişiklik riskiyle karşı karşıya kalırız.

Söz konusu Yönerge'nin “uygulama kapsamı” başlığı altında verilen bir örnekte; park yardımı sağlamak için araca bir video kamera entegre edilmiştir. Kamera, gerçek bir kişiyle ilgili herhangi bir bilgi (araç plakaları veya yoldan geçenleri tanımlayabilecek bilgiler gibi) toplamayacak şekilde yapılmış veya ayarlanmışsa, kişisel veri toplanmadığından GDPR geçerli değildir, burada GDPR uygulama alanı bulamayacaktır. Burada Yönerge, araç kameralarının nasıl ayarlanması gerektiğiyle ilgili genel bir çerçeve çizmiştir.

Yine verilen başka bir örnekte; birisi kendi bahçesini izliyor ve kaydediyor. Mülk çitle çevrili ve bahçeye düzenli olarak sadece kontrolörün kendisi ve ailesi girmektedir. Bu, video gözetiminin bir kamusal alanı veya komşu mülkü kısmen de olsa kapsamaması koşuluyla hane halkı muafiyeti kapsamına girecektir. Benzer şekilde Yönerge’de verilen başka bir örnekte; bir kitapçı binasını vandalizme karşı korumak istemektedir. Genel olarak, kameralar sadece binayı kayda almalıdır, çünkü amacına uygun olarak kitapçının binasının çevresindeki komşu binaları veya halka açık alanları izlemesi gerekli değildir. Bu örnekler her ne kadar bir güvenlik kamerası ile ilgili olsa da park halindeki otonom bir aracın uzaktan kamerasına erişim imkanına sahip olduğu varsayımında araç kamerası ile ilgili kısıtlılık çerçevesini de çizmektedir.

Yönerge’nin “işleme faaliyetinin yasallığı” başlığı altında GDPR’a da atıfta bulunarak, video görüntülerinin işlenmesinin hangi durumlarda yasal olduğunun çerçevesi çizilmiştir. Buna göre, kullanımdan önce, işleme amaçları ayrıntılı olarak belirtilmelidir. Video gözetimi birçok amaca hizmet edebilir, bu izleme amaçları yazılı olarak belgelenmeli ve kullanılan her güvenlik kamerası için ayrı ayrı belirtilmelidir. Yalnızca "güvenlik" veya "güvenliğiniz için" amacına dayalı video gözetimi yeterince spesifik değildir. Bu maddede “amacın sınırlandırılması” ilkesinin açıklandığı GDPR’ın 5/1-b maddesine ve “hesap verebilirlik” ilkesinin açıklandığı 5/2 maddelerine atıf yapılmıştır.

Bazı durumlarda, görüntülerin belirli bir depolama süresinden sonra otomatik olarak silindiği ve yalnızca anormal bir olay durumunda erişimin olduğu kara kutu çözümlerinin kullanılması gerekebilir. Diğer durumlarda, video materyalini kaydetmek hiç gerekli olmayabilir, bunun yerine gerçek zamanlı izlemeyi kullanmak daha uygun olabilir. Kara kutu çözümleri ile gerçek zamanlı izleme arasındaki karar da izlenen amaca dayalı olmalıdır. Örneğin, video gözetiminin amacı kanıtların korunmasıysa, gerçek zamanlı izleme yöntemi genellikle uygun değildir. Bazen gerçek zamanlı izleme, sınırlı bir zaman diliminden sonra materyali depolamak ve otomatik olarak silmekten daha müdahaleci olabilir (örneğin, birisi sürekli olarak monitörü izliyorsa, hiç monitörün olmadığı ve görüntünün doğrudan kara kutuda saklandığı durumdan daha müdahaleci olabilir). Veri minimizasyonu ilkesi bu bağlamda ele alınmalıdır. Bu maddede video kayıt cihazları açısından, anlık izleme ile kara kutuda depolama ihtimalleri değerlendirilerek hangisinin tercih edilmesi gerektiği konusunda “veri minimizasyonu” ilkesinin açıklandığı GDPR’ın 5/1-c maddesine atıf

yapılmıştır. Bu maddeye göre, kişisel veriler, işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlıdır.

Yönerge'nin "çıkarların dengelenmesi" başlığı altında denetleyicinin, izlemenin bireylerin çıkarlarını, temel hak ve özgürlüklerini ne ölçüde etkilediğini ve bunun veri sahibinin haklarına ilişkin ihlallere veya olumsuz sonuçlara yol açıp açmadığını değerlendirmesi gerekir, denmiştir. Aslında, çıkarların dengelenmesi zorunludur. Bir yanda temel hak ve özgürlükler, diğer yanda kontrolörün meşru menfaatleri dikkatle değerlendirilmeli ve bu iki çıkar dengelenmelidir. Bu çıkarların dengelenmesinde iki ana kriterin belirlendiği söylenebilir; durum bazında karar verme ve veri sahiplerinin makul beklentileri.

-Durum bazında karar verme; Yönergeye göre çıkarların dengelenmesi zorunlu olduğundan, karar duruma göre verilmelidir. Kontrolör, veri öznesinin haklarına tecavüz risklerini değerlendirmelidir; burada belirleyici kriter, bireyin hak ve özgürlüklerine yönelik müdahalenin yoğunluğudur. Yönerge'de bu durumu açıklamak amacıyla bir örnek verilmiştir; araç kamerası varsa (örneğin bir kaza durumunda kanıt toplamak amacıyla), bu kameranın sürekli olarak trafiği ve yol kenarındaki kişileri kaydetmediğinden emin olunması önemlidir. Aksi takdirde, teorik bir durum olan trafik kazasının video kayıtlarının delil olarak elde edilmesi, veri sahiplerinin haklarına yönelik bu ciddi müdahaleyi haklı çıkaramaz.

-Veri sahiplerinin makul beklentileri; makul beklenti kavramının yorumlanması sadece subjektif beklentilere dayanmamalıdır. Daha ziyade belirleyici kriter, tarafsız bir üçüncü tarafın bu özel durumda izlemeye tabi tutulacağını makul bir şekilde bekleyip bu sonuca varıp varamayacağı olmalıdır.

Video kamera sistemleri ile büyük miktarda kişisel veri toplandığından özel nitelikli kişisel verilerin işlenmesi hususu da gündeme gelmektedir. Yönerge'de bu konuya da değinilmiştir. Video yoluyla toplanan görünüşte önemsiz veriler, farklı bir amaca ulaşmak için (örneğin, bir bireyin alışkanlıklarını haritalamak gibi) kullanılabilir. Bununla birlikte, video gözetimi her zaman özel nitelikli kişisel verilerin işlenmesi olarak değerlendirilmez. GDPR'ın "özel kategorilerdeki kişisel verilerin işlenmesi" başlığını taşıyan 9.maddesi "*İrk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile biyometrik verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır.*" diyerek özel nitelikli kişisel verilerin tanımını yapmış ve bu verilerin işlenmesini yasaklayarak maddenin devamında özel nitelikli

kişisel verilerin işlenmesinin çerçevesi çizilmiştir. GDPR’ın “tanımlar” başlıklı 4.maddesinde; “biyometrik veri” *yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel verilerdir*, şeklinde tanımlanmıştır. Bununla birlikte, bir kişinin kimliğinin belirlenmesine katkıda bulunmak amacıyla özel olarak teknikle işlenmemişse, bir kişinin video görüntüleri 9. madde kapsamında tek başına biyometrik veri olarak kabul edilemez. GDPR’ın 51 numaralı resitalinde de; “*Fotoğrafların işlenmesi, sistematik olarak özel kişisel veri kategorilerinin işlenmesi olarak değerlendirilmemelidir, çünkü bunlar yalnızca gerçek bir kişinin benzersiz olarak tanımlanmasına veya doğrulanmasına izin veren belirli bir teknik araçla işlendiğinde biyometrik veri tanımı kapsamındadır.*” denilmiştir. Bütün bu düzenlemeler ışığında Yönerge’ye göre biyometrik verinin işlendiğinin kabul edilebilmesi için üç kriter dikkate alınmalıdır:

Çizelge 4.1.Biyometrik Verinin İşlendiğinin Kabul Edilebilmesi İçin Dikkate Alınan Kriterler

Verinin niteliği	Gerçek kişinin fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin veriler
İşleme araçları ve şekli	"Belirli bir teknik işlemde kaynaklanan" veriler
İşlemenin amacı	Veriler, gerçek bir kişiyi benzersiz bir şekilde tanımlamak amacıyla kullanılmalıdır

Yönerge’de verilen bir örnek ise şöyledir; bir mağaza sahibi, reklamını müşterinin kamera sistemi tarafından yakalanan cinsiyet ve yaş özelliklerine göre özelleştirmek istiyor. Bu sistem, kişileri benzersiz bir şekilde tanımlamak için biyometrik şablonlar oluşturmaz, bunun yerine kişileri sınıflandırmak için yalnızca fiziksel özelliklerini tespit ederse (başka hiçbir özel kişisel veri kategorisi türü işlenmediği sürece), bu işlem GDPR’ın 9.maddesindeki özel kategorilerdeki kişisel verilerin işlenmesi kapsamına girmeyecektir. Bununla birlikte, kontrolörün bir kişiyi benzersiz bir şekilde tanımlamak için biyometrik verileri (genellikle biyometrik verilerin ham biçiminden, örneğin bir görüntüden yüz ölçümlerinin tespiti gibi, temel özelliklerin çıkarılmasıyla oluşturulan şablonlar aracılığıyla) depolaması durumunda GDPR’ın 9.maddesindeki özel kategorilerdeki kişisel verilerin

işlenmesi kapsamına girecektir. Yönerge’de verilen örnekte, bir otel, gelen konuğun yüzünü tanıyarak bir VIP'nin geldiği konusunda otel müdürünü otomatik olarak uyarmak için video kamera sistemi kullanmaktadır. Bu VIP'lerin, bu amaçla oluşturulmuş bir veri tabanına kaydedilmeden önce, yüz tanıma sisteminin kullanılmasına ilişkin açık rızalarının alınması gerekir. VIP'leri belirlemek için izlenen diğer tüm konuklar GDPR 9/2-a maddesi uyarınca işlemeye izin vermedikçe, bu biyometrik veri işleme sistemi yasa dışı olacaktır. Son olarak, GDPR 9.madde uyarınca onay gerekli olduğunda veri denetleyicisi, hizmete erişimi biyometrik işlenmesi işleminin kabulü şartına bağlayamaz. Başka bir deyişle, özellikle biyometrik işleme, kimlik doğrulama amacıyla kullanıldığında, veri denetleyicisi, kısıtlamalar veya veri sahibi için ek maliyet olmaksızın biyometrik işlemeyi içermeyen alternatif bir çözüm sunmalıdır.

4.3.Otonom Araçlarla İlgili Türkiye’deki Hukuki Düzenlemelerin İncelenmesi

4.3.1.Motorlu araçlar ve römorkları ile bunlar için tasarlanan aksam, sistem ve ayrı teknik ünitelerin genel güvenliği ve korunmasız karayolu kullanıcılarının ve yolcuların korunması ile ilgili tip onayı yönetmeliği (AB/2019/2144)

2918 sayılı Karayolları Trafik Kanunu’nda otonom araçlara ilişkin herhangi bir madde bulunmamaktadır. Ancak Sanayi ve Teknoloji Bakanlığı tarafından 14.05.2020 tarihinde yayımlanan Motorlu Araçlar ve Römorkları ile Bunlar İçin Tasarlanan Aksam, Sistem ve Ayrı Teknik Ünitelerin Genel Güvenliği ve Korunmasız Karayolu Kullanıcılarının ve Yolcuların Korunması İle İlgili Tip Onayı Yönetmeliği’nde (AB/2019/2144) otonom araç ve tam otonom araç kavramlarının tanımına yer verilmiştir. İlgili Yönetmelik’in “Tanımlar” başlıklı 3/1-t maddesinde “*Otonom araç: Sürücünün devamlı kontrolü olmadan, ancak sürücü müda-halesinin yine de beklendiği veya gerekli olduğu, belirli bir süre için otonom olarak hareket etmek üzere tasarlanmış ve imal edilmiş motorlu aracı*” olarak tanımlanmıştır. İlgili maddenin 3/1-z bendinde “*Tam otonom araç: Herhangi bir sürücü kontrolü olmadan otonom olarak hareket etmek üzere tasarlanmış ve imal edilmiş motorlu aracı*” ifade etmektedir. Tam otonom araçta sürücü olmadığından Yönetmelik madde 11/1’ de sürücü müsaitliği/uygunluğu izleme sisteminin tam otonom araçlar için uygulanmayacağı belirtilmiştir. Karayolları Trafik Kanunu madde 73’te ise sürücülerin seyir halindeyken cep ve araç telefonunu kullanması yasaklanmıştır. Karayolları Trafik Kanunu madde 73 bu kapsamda tam otonom araçlar için uygulama alanı bulamayacaktır (Bayındır, 2021). Çünkü

tam otonom araçların kullanım amacı, kişinin seyir halindeyken yol dışında işlerle meşgul olmasını (kitap okumak, film izlemek gibi) sağlamaktır.

1968 tarihli Viyana Karayolu Trafîği Konvansiyonu (“Konvansiyon”) 21 Mayıs 1977 tarihinde yürürlüğe girmiştir. Konvansiyonun eski halinde, madde 8/6’ya göre sürücü, sürüş esnasında başka bir işle meşgul olamazdı, dolayısıyla her araçta muhakkak bir sürücü bulunmalıydı ve madde 8/5 uyarınca sürücü, her zaman taşıt hakimiyetini sağlayabilecek durumda olmalıydı. Bu hüküm, kısmi otomatik yönlendirme (2. seviye), koşullu otomatik yönlendirme (3. seviye), yüksek otomatik yönlendirme (4. seviye) ve tam otomatik yönlendirme (5. seviye) seviyelerine sahip araçlar bakımından sorun teşkil etmekteydi. Bunun üzerine 2014 yılında, özellikle sürücü yardım sistemleri bakımından uygulama alanı bulması amaçlanan bir değişiklik önerisi kabul edilmiştir ve bu değişiklik ile madde 8/5’e 5bis hükmü eklenmiştir. Bu hükmü göre; araç sürüşüne etki eden araç sistemleri, tekerlekli araçlara takılabilen ve/veya bu araçlarda kullanılabilen aksam ve parçalar hakkında uygulanan uluslararası hukuki düzenlemeler uyarınca imal, montaj ve kullanım koşullarını yerine getirmeleri kaydıyla, madde 8/5 ve madde 13/1 hükümlerine uygun addedilir. Ayrıca söz konusu imal, montaj ve kullanım koşullarını yerine getirmeyen fakat araç sürüşüne etki eden sistemler, sürücü tarafından devre dışı bırakılabiliyorsa, madde 8/5 ve madde 13/1 hükümlerine uygun kabul edilir. Bu değişiklik ile, kısmi (2. seviye) ve koşullu (3. seviye) otomatik yönlendirme seviyelerinde kullanılabilen araçların karayolu trafiğine çıkmasının önündeki engellerin kaldırıldığı ileri sürülebilir. Hal böyle olmakla birlikte yüksek ve tam otomatik yönlendirme seviyelerinde (4. ve 5. seviye) kullanılabilen araçlar bakımından hala engeller bulunmaktadır. (Buğra, 2020).

4.3.2.112 Acil çağrı servisi tabanlı araç içi acil çağrı sistemine ilişkin motorlu araçların tip onayına yönelik idari hükümlerin hazırlanması ve bu sistem kullanıcıları için gizlilik ve veri korumasına ilişkin yönetmelik (2017/78/AB)

31.03.2018 tarihinden itibaren Avrupa Birliği ülkelerinde tüm araçlar araç içi acil çağrı sistemine uyumlu halde üretilmekte olup, ülkelerin de Acil Çağrı Merkezlerini e-Call çağrılarını karşılayacak şekilde yeniden dizayn etmeleri istenmektedir. Bu sisteme sahip olan bir araç kaza yaptığı anda sistem otomatik olarak devreye girmekte ve 112 acil çağrı merkezini aramaktadır. 112 Acil Çağrı Merkezi, arayan aracın konum bilgisini araçta bulunan GPS ile tespit etmekte ve araçta bulunan sensörler sayesinde araçta meydana gelen hasarı da yaklaşık

olarak hesap edebilmektedir. Çarpma ile birlikte devreye giren sistem sayesinde araç içerisinde bulunan kişiler ile Acil Çağrı Merkezinde bulunan görevliler karşılıklı olarak görüşebilmektedirler. E- Call çağrısı alındıktan sonra Acil Çağrı Merkezinde (Polis, Jandarma, Ambulans, İtfaiye) bulunan tüm görevliler tarafından kaza yapan araca gerekli müdahale yapılacaktır. (T.C.İçişleri Bakanlığı Bilgi İşlem Dairesi Başkanlığı)

Bilim, Sanayi ve Teknoloji Bakanlığı tarafından 09.06.2018 tarihinde yayımlanan 112 Acil Çağrı Servisi Tabanlı Araç İçi Acil Çağrı Sistemine İlişkin Motorlu Araçların Tip Onayına Yönelik İdari Hükümlerin Hazırlanması ve Bu Sistem Kullanıcıları İçin Gizlilik ve Veri Korumasına İlişkin Yönetmeliği (2017/78/AB) ile bu sisteme yönelik bir düzenleme getirilmiştir. Bu Yönetmelikte direkt olarak “otonom araç” kavramına yer verilmesine de araç vasıtasıyla kaydedilen verilere yönelik bir çerçeve sunduğundan çalışmamız açısından önem arz etmektedir. Bu Yönetmeliğin “gizlilik ve verilerin korunması” başlığını taşıyan 8.maddesinde bu sistemlerin kullanıldığı araçlarda kişilerin verilerinin korunmasına yönelik düzenlemeler getirilmiştir. Buna göre, *“imalatçı, 112 tabanlı araç içi acil çağrı sisteminin veya 112 tabanlı araç içi acil çağrı ayrı teknik ünitesinin, normal işletme durumunda takip edilememesi ve sabit izlemeye maruz kalmamasını sağlayacak tedbirleri alır. İmalatçı ayrıca bu sistem veya ayrı teknik ünitenin dahili hafızasında yer alan verilerin otomatik ve sürekli şekilde yok edilmesini ve acil çağrı başlatılmadan önce bu bilgilerin araç içi sistem veya ayrı teknik ünite dışında, başka kurum/kuruluş veya kişilerin eline geçmesini engelleyecek tedbirleri alır.”* denilerek, araçta bulunan GPS sistemi vasıtasıyla kişilerin sürekli olarak takip edilemeyeceği, yalnızca acil durum arz eden durumda sistemin aktif olarak belirli bir süre aracın konumuna erişebileceği açıklanmıştır. Ayrıca imalatçıya araç sahibini alnan tedbirler konusunda bilgilendirme yükümlülüğü de getirilmiştir. Yine imalatçıya 112 tabanlı araç içi acil çağrı sistemi veya 112 tabanlı araç içi acil çağrı ayrı teknik ünitesinin dahili hafızasında yer alan kişisel bilgilerin güvenliğini koruma, izlenmesini ve istismarını önlemek amacıyla şifreleme teknolojilerinin kullanımı gibi uygun koruma tedbirlerini alma yükümlülüğü getirilmiştir.

4.4.Otonom Araçlarla İlgili Avrupa Birliği’ndeki Hukuki Düzenlemelerin İncelenmesi

4.4.1.Avrupa veri koruma kurulu- bağlı araçlar ve mobilite ile ilgili uygulamalar bağlamında kişisel verilerin işlenmesine ilişkin 01/2020 sayılı yönerge (Kılavuz ilkeler)

Yönerge’de belirtildiği üzere; araç içi bağlantı, lüks araç modellerinden ve birinci sınıf markalardan yüksek hacimli orta pazar modellerine hızla yayılmakta ve bu da araçları devasa veri merkezleri haline getirmektedir. Sadece araçlar değil, sürücüler ve yolcular da giderek daha fazla birbirine bağlı hale gelmektedir. Nitekim, son birkaç yılda piyasaya sürülen birçok model, diğer şeylerin yanı sıra gerçek bir kişiyi benzersiz bir şekilde tanımlamak amacıyla; motor performansını, sürüş alışkanlıklarını, ziyaret edilen yerleri, sürücünün göz hareketlerini, nabzını ve hatta biyometrik verilerini toplayabilmekte ve kaydedebilmektedir. Buna ek olarak, bağlı araçlar, sürücüler veya yolcularla ilgili çoğu kişisel veri olarak kabul edilebilecek büyük miktarda veri üretmektedir. Örnek olarak, sürüş tarzı veya kat edilen mesafe ile ilgili veriler, araç parçalarındaki aşınma ve yıpranma ile ilgili veriler, konum verileri veya kameralar tarafından toplanan veriler, sürücü davranışının yanı sıra içeride olan veya oradan geçmekte olan veri konusu diğer kişiler hakkındaki bilgileri de içerir. Bu tür teknik veriler, gerçek bir kişi tarafından üretilir ve veri sorumlusu veya başka bir kişi tarafından doğrudan veya dolaylı olarak kimliğinin tespit edilmesine olanak tanır. Araç, farklı kullanıcılar tarafından kullanılabilen bir terminal olarak düşünülebilir. Bu açıdan bakıldığında, bir kişisel bilgisayar gibi değerlendirirsek, bu potansiyel kullanıcı çokluğu, verilerin kişisel veri olma niteliğini etkilemez.

Yönerge’ye göre; bağlı araç ve buna bağlı cihaz (tıpkı bilgisayar, akıllı telefon veya akıllı TV gibi) “*terminal donanım*” olarak değerlendirilmelidir demektir. Buna göre bağlı araçlara e-Gizlilik Direktifi (2002/58/EC Gizlilik ve Elektronik İletişim Direktifi) madde 5/3 uygulanır demektir. Bu maddeye göre; “*Üye Devletler, bilgi depolamak veya bir abonenin veya kullanıcının terminal ekipmanında saklanan bilgilere erişim sağlamak için elektronik iletişim ağlarının kullanımına yalnızca ilgili aboneye veya kullanıcıya açık ve kapsamlı bilgi sağlanması koşuluyla izin verilmesini sağlayacaklardır. 95/46/EC sayılı Direktif uyarınca, diğer hususların yanı sıra, işleme amaçları hakkında ve veri denetleyicisi tarafından bu tür bir işlemeyi reddetme hakkı sunulmalıdır.*” Yani verilerin depolanması veya depolanmış verilere erişilebilmesi için veri sahibinin önceden izninin alınması gerekir ve veriyi paylaşmama seçeneği de sunulmalıdır. “*Terminal donanım*” teriminin tanımı,

2008/63/EC Telekomünikasyon Terminal Ekipmanı Piyasalarındaki Rekabete İlişkin Yönerge'nin 1/a maddesinde yapılmıştır. Buna göre; *“bilgi göndermek, işlemek veya almak için bir kamu telekomünikasyon ağının arayüzüne doğrudan veya dolaylı olarak bağlı ekipman; her iki durumda da (doğrudan veya dolaylı), bağlantı tel, fiber optik veya elektromanyetik olarak yapılabilir”* denilmiştir.

Rızanın alınması ilke olmakla birlikte, e-Gizlilik Direktifi madde 5/3 aşağıdaki kriterlerden birini karşılaması halinde, terminal donanımında depolanan bilgilerin saklanmasına veya bilgilere erişimin bilgilendirilmiş onay gerekliliğinden muaf tutulmasına izin verir:

- 1.*Muafiyet* : Yalnızca bir elektronik iletişim ağı üzerinden bir iletişimin iletimini gerçekleştirmek amacıyla;
- 2.*Muafiyet* : Abone veya kullanıcı tarafından açıkça talep edilen, bir “bilgi toplumu” hizmeti sağlayıcısının hizmeti sunabilmesi için kesinlikle gerekli olması.

Bu gibi durumlarda, terminal donanımındaki bilgilere erişilerek elde edilen kişisel veriler de dahil olmak üzere kişisel verilerin işlenmesi, GDPR'ın 6.maddesi kapsamında sağlanan yasal dayanaklardan birine dayanmaktadır. Örneğin, veri sahibi tarafından talep edilen GPS navigasyon hizmetlerini sağlamak için veri işlemenin gerekli olduğu ve bu tür hizmetlerin “bilgi toplumu” hizmetleri olarak nitelendirilebileceği durumlarda onay gerekli değildir.

Bu Yönerge'de bağlı aracın tanımı da yapılmıştır. Buna göre, bağlı araç tanımı, bu belgede geniş bir kavram olarak anlaşılmalıdır. Araç içi bir ağ aracılığıyla birbirine bağlanan birçok elektronik kontrol ünitesi (ECU) ve aracın hem içindeki hem de dışındaki diğer cihazlarla bilgi paylaşmasını sağlayan bağlantı olanakları ile donatılmış bir araç olarak tanımlanabilir.

Bağlı araçlarda kaydedilen veriler açısından konum verileri ve biyometrik veriler özellikle önem taşımaktadır. Yönerge'de bu veriler toplanırken uyulması gereken ilkeler belirtilmiştir.

Genel olarak, konum verilerinin toplanması aşağıdaki ilkelere uygunluğa tabidir:

-İşleme amacına göre toplanan konum verilerine erişim sıklığının ve ayrıntı düzeyinin yeterli şekilde yapılandırılması. Örneğin, bir hava durumu uygulaması, ilgili kişinin rızası olsa bile aracın konumuna her saniye erişememelidir.

-İşlemenin amacı hakkında doğru bilgi sağlamak, (örneğin, konum geçmişi saklanıyor mu? Eğer öyleyse, amacı nedir?)

- İşleme, rızaya dayalı olduğunda, örneğin araç bilgisayarında genel satış veya kullanım koşullarından farklı geçerli (ücretsiz, özel ve bilgilendirilmiş) rıza alınması,
- Konumun varsayılan olarak ve araç çalıştırıldığında sürekli olarak değil, yalnızca kullanıcı aracın konumunun bilinmesini gerektiren bir işlevi başlattığında etkinleştirilmesi,
- Özellikle simgeler kullanılarak (örneğin ekranda hareket eden bir ok) kullanıcıya konumun etkinleştirildiğini bildirmek,
- İstediği zaman konumu devre dışı bırakma seçeneği,
- Sınırlı bir saklama süresi tanımlanması.

Biyometrik veriler söz konusu olduğunda, özellikle aşağıdaki ilkelere uyarak, biyometrik kimlik doğrulama çözümünün yeterince güvenilir olmasını sağlamak önemlidir:

- Kullanılan biyometrik çözümün ayarlanması (örneğin, yanlış pozitif ve yanlış negatif oranı), gerekli erişim kontrolünün güvenlik seviyesine uyulanır;
- Kullanılan biyometrik çözüm, saldırılara karşı dayanıklı bir sensöre dayalıdır (parmak izi tanıma için düz baskılı (flat-printed) baskı kullanılması gibi);
- Kimlik doğrulama girişimlerinin sayısı sınırlanmalıdır;
- Biyometrik şablon/model, en son teknoloji ile uyumlu bir kriptografik algoritma ve anahtar yönetimi kullanılarak şifrelenmiş bir biçimde araçta saklanır;
- Biyometrik şablonu oluşturmak ve kullanıcı kimlik doğrulaması için kullanılan ham veriler, yerel olarak bile saklanmadan gerçek zamanlı olarak işlenir.

Özellikle, bu tür verilerin yetkili ulusal makamlar tarafından ceza soruşturması ve kovuşturması amacıyla işlenmesi durumunda, GDPR'ın "mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin işlenmesi" başlığını taşıyan 10.maddesinde öngörülen önlemler geçerli olacaktır. Buna göre; "*Mahkumiyet kararları ve ceza gerektiren suçlara ilişkin ya da ilgili güvenlik tedbirlerine ilişkin kişisel verilerin 6(1) maddesine dayalı olarak işlenmesi, ancak resmi mercinin denetimi altında veya veri sahiplerinin hakları ve özgürlüklerine uygun güvenceler sağlayan Birlik veya üye devlet hukuku çerçevesinde işleme faaliyetine onay verildiğinde gerçekleştirilir.*"

Bağlı araçlar açısından tartışmaya sebep olan bir diğer husus da araç kullanım alışkanlığının kaydedilerek sigorta priminin belirlenmesidir. Bağlı araçlar, gelişen teknolojiyle birlikte kullanıcıların/sürücülerin araç kullanma alışkanlıklarını kaydetme (örneğin ani hız ani fren, aşırı hız, trafik kurallarına uyup uymama alışkanlıkları) özelliğine sahiptir. Bu verilerin sigorta şirketleri ile paylaşılması sonucunda kişilerin sigorta primlerinin bu verilere göre arttırılması söz konusu olabilecektir. Yönerge'de de kullanıma dayalı sigorta konusuna da

değinilmiştir. Kullanıma dayalı sigorta e-Gizlilik Direktifi madde 5/3'e göre kullanıcının onayını gerektirmektedir. Poliçe sahibinin kullanıma dayalı olmayan bir sigorta poliçesine abone olma seçeneğine sahip olması gerekir. Aksi takdirde, sözleşmenin ifası rızaya bağlı olacağından, rıza serbestçe verilmiş sayılmaz. Kullanıma dayalı sigorta kapsamında, sürüş davranışına ilişkin kişisel veriler (fren pedalına uygulanan kuvvet, kat edilen kilometre vb.) araç içinde veya adına telematik hizmet sağlayıcı tarafından işlenerek belirli aralıklarla (örneğin aylık olarak) sigorta şirketine sayısal puanlar oluşturularak aktarılabilir. Bu şekilde, sigorta şirketi ham davranışsal verilere değil, yalnızca işlemenin sonucu olan toplam puana erişim elde eder. Bu yöntem veri minimizasyonu ilkelerinin tasarım tarafından karşılanmasını da sağlar. Yönerge'de bu ve benzeri uygulamaya yönelik pek çok öneri getirilmiştir.

4.4.2. Motorlu araçlar ve römorkları ile bunlar için tasarlanan aksam, sistem ve ayrı teknik ünitelerin genel güvenliği ve korunmasız karayolu kullanıcılarının ve yolcuların korunması ile ilgili tip onayı yönetmeliği (27 Kasım 2019 tarihli AB/2019/2144 sayılı)

Türkiye'de Sanayi ve Teknoloji Bakanlığı tarafından 14.05.2020 tarihinde yayımlanan "Motorlu Araçlar ve Römorkları ile Bunlar İçin Tasarlanan Aksam, Sistem ve Ayrı Teknik Ünitelerin Genel Güvenliği ve Korunmasız Karayolu Kullanıcılarının ve Yolcuların Korunması ile İlgili Tip Onayı Yönetmeliği (AB/2019/2144)" isminden de anlaşılacağı üzere Avrupa Birliği'nin aynı isimli yönetmeliğinden uyarlanmıştır. Yapılan bu düzenlemeler ile gözetilen amaç, yeni araçlarda zorunlu olarak bulunması gereken güvenlik önlemlerine ilişkin düzenlemeler yapılarak insanların can ve mal güvenliğinin gelişen teknolojiyle uyumlu hale getirilmesidir. Çalışmamızda belirtildiği üzere Türkiye'deki aynı isimli yönetmelik başlığı altında açıkladığımız hususlar, bu Yönetmelik için de aynen geçerlidir.

Yönetmelikte bahsedilen "olay veri kaydedicisi"ne değinilmesi gerektiğini düşünüyoruz. Yönetmeliğin "tanımlar" başlıklı 3.maddesinin 13.bendinde "olay veri kaydedicisi"; çarpışmadan hemen önce, çarpışma sırasında ve hemen sonrasında çarpışmanın kritik parametrelerini ve bilgilerini sadece kaydetme ve depolama amacıyla kullanılan sistem, şeklinde tanımlanmıştır. Yönerge'nin "Motorlu araçların tüm kategorileri için gelişmiş araç sistemleri" başlıklı 6.maddesinin 4.bendinde olay veri kaydedicilerin sağlaması gereken şartlar belirtilmiştir. Buna göre;

- Olay veri kaydedicisindeki veriler; aracın yoldaki hızını, frenlemesini, konumunu ve devrilmesini (yana yatma-devrilme durumunu), bütün güvenlik sistemlerinin aktivasyonunun durumunu ve oranını, 112 tabanlı araç içi acil çağrı sistemi, fren aktivasyonu ve araca monte aktif güvenlik ve kaza önleme sistemlerinin ilgili giriş parametrelerini, yüksek doğruluk ve verinin sürdürülebilirliğini sağlayacak şekilde içerir.

- Olay veri kaydedicileri devre dışı bırakılamaz.

- Aşağıdaki şekilde verileri kaydetme ve saklama kabiliyetine sahip olmalıdır:

1) Kapalı devre bir sistemde çalışır.

2) Topladığı veriler gizli tutulur ve manipülasyona ve kötüye kullanıma karşı korunur.

3) Topladığı veriler, kesin araç tipi, varyantı ve versiyonu ve özellikle araca takılan aktif güvenlik ve kaza önleme sistemlerini tanımlayabilmelidir.

- Kaydedilebilen veriler, standart bir arayüz üzerinden, sistem ve ayrı teknik ünite tip onayının amaçları dahil olmak üzere Birlik veya ulusal yasalara dayalı olarak, yalnızca kaza araştırma ve analizi amacıyla ve veri güvenliğine ilişkin gerekli her türlü teknik ve idari tedbir alınmak suretiyle GDPR'a uygun olarak ulusal makamlara sunulabilir.

Yönerge'nin 6/3.maddesinde sistem tarafından kaydedilen verilere yönelik olarak “Sürücü dalgınlık ve dikkat uyarı sistemi ve gelişmiş sürücü dikkat dağınıklığı uyarı sistemi, kapalı döngü sistemi içerisinde topladığı veya bunun dışında işlediği amaçla ilgili gerekli olanlar haricinde hiçbir veriyi sürekli olarak kaydetmeyecek veya saklamayacak şekilde tasarlanır. Ayrıca, hiçbir zaman bu verilere üçüncü taraflarca erişilemez veya üçüncü tarafların istifadesine sunulamaz ve işleme amacı ortadan kalktıktan sonra bu veriler derhal silinir.” denilmiştir.

4.4.3. Avrupa Birliği yapay zeka yasası

Yapay zeka ile ilgili Avrupa Birliği düzeyindeki tartışmalara öncülük eden Avrupa Parlamentosu, 2017 yılında robotikle ilgili medeni hukuk kurallarına ilişkin geniş kapsamlı tavsiyelerinde (Robotikle İlgili Medeni Hukuk Kuralları-Civil Law Rules on Robotics), Avrupa Komisyonu'nu yapay zekanın etkisini değerlendirmeye ve yapay zeka için Avrupa Birliği düzleminde bir çerçeve hazırlamaya çağırmıştır.

Avrupa Komisyonu, yapay zekanın yaygınlaşmasını teşvik etmek ve bu yeni teknolojinin belirli kullanımlarıyla ilişkili riskleri ele almak gibi amaçlarla hem düzenleyici hem de yatırım odaklı bir anlayış ile Şubat 2020’de Yapay Zeka Hakkında Teknik Doküman (White Paper on Artificial Intelligence)’ı yayınlamıştır. White paper (teknik doküman), bilindiği üzere bir ürünün amacını, kapsamını, getireceği yenilikleri, temel felsefesini ve teknik ayrıntılarını açıklayan bir belgedir ve genellikle satış öncesi pazarlama için kullanıcıları bilgilendirme ve ürünün özelliklerini ile avantajlarını vurgulayan bir belgedir.

Bu teknik dokümanın ardından Avrupa Komisyonu, 2020’de geniş bir kamu istişaresi başlatmış ve çeşitli paydaşlardan geri bildirim alan yapay zeka düzenlemesine ilişkin bir Etki Değerlendirmesi (Impact Assessment of the Regulation on Artificial Intelligence), destekleyici bir çalışma ve taslak bir teklif yayınlamıştır. Etki değerlendirmesinde Komisyon, yapay zeka sistemlerinin belirli özelliklerinden dolayı geliştirilmesi ve kullanılmasıyla ortaya çıkan çeşitli sorunları tespit etmiştir.

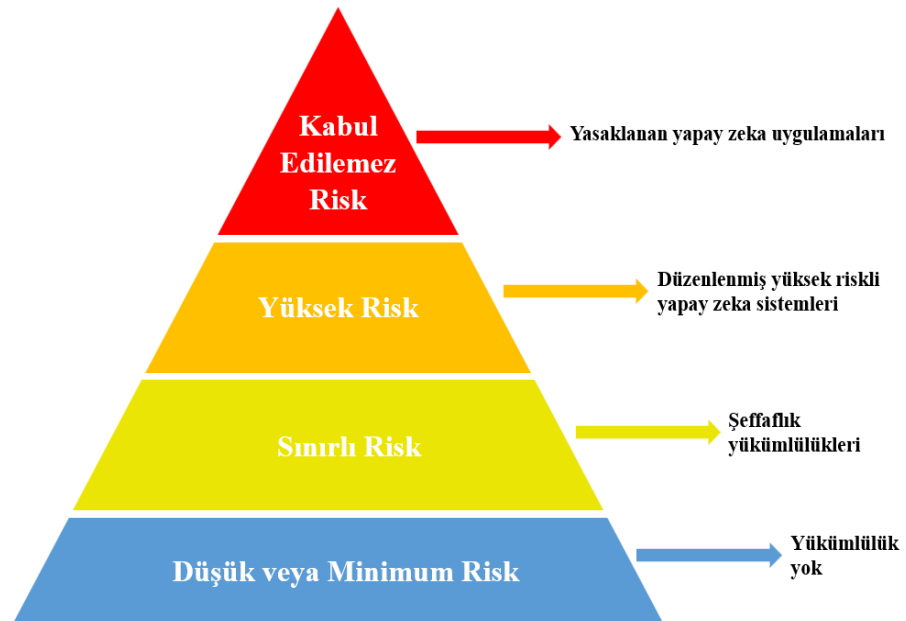
Avrupa Komisyonu tarafından 21 Nisan 2021 tarihinde Avrupa Birliği’nde yapay zekaya ilişkin kuralları (Yapay Zeka Yasası- EU AI Act) uyumlu hale getirmeyi amaçlayan bir düzenleme ve Komisyon ile üye devletler için bir dizi ortak eylem içeren koordineli bir plan için teklif yayınlanmıştır. Bu kural paketi, yapay zekaya olan güveni artırmayı ve yapay zeka teknolojisinin geliştirilmesini ve güncellenmesini teşvik etmeyi amaçlamıştır.

6 Aralık 2022 tarihinde, Avrupa Birliği Konseyi, Yapay Zeka Yasası hakkında genel bakış açısında (General approach) (Consilium) fikir birliğine varmıştır. Önerilen bu düzenleme, Avrupa Birliği pazarına sunulan ve Birlik içinde kullanılan yapay zeka sistemlerinin güvenli olmasını ve temel haklar ile Birlik değerlerine ilişkin mevcut yasalara saygılı olmasını sağlamayı amaçlamıştır. Bu genel bakış açısının benimsenmesi, Konsey’in Avrupa Parlamentosu ile müzakerelere girmesine olanak tanımıştır.

9 Aralık 2023 tarihinde, Avrupa Birliği Konseyi ve Avrupa Parlamentosu Yapay Zeka Yasası (EU AI Act) üzerinde siyasi bir anlaşmaya vardıklarını basın açıklaması ile duyurmuştur. (EPRS) Avrupa Yapay Zeka Ofisi (European AI Office), Yapay Zeka

Yasasının üye devletlerde uygulanmasını denetleme amacıyla Şubat 2024'te Komisyon bünyesinde kurulmuştur. Yapay Zeka Yasası, birliğe dair yasaların ve resmi olayların kamuya açıklanması için çıkartılan bir yayın olan Avrupa Birliği Resmî Gazetesi'nde yayımlanmasından 20 gün sonra yürürlüğe girecek ve bazı istisnalar dışında iki yıl sonra tamamen geçerli olacaktır. Bu yeni yasaya geçişi kolaylaştırmak için Komisyon, Avrupa ve Avrupa dışındaki yapay zeka geliştiricilerini Yapay Zeka Yasasının temel yükümlülüklerine önceden uymaya davet eden gönüllü bir girişim olan Yapay Zeka Paktını (AI Pact) da başlatmıştır.

Taslak Yapay Zeka Yasası'na göre; bilim camiasının ortaklaşa kabul ettiği bir yapay zeka tanımı olmamakla birlikte, halihazırda OECD tarafından kullanılan tanıma (OECD Legal Instruments) paralel bir tanım benimsendiği belirtilmiştir. Buna göre yapay zeka sistemi; *"...[Ek 1'de listelenen] [belirli] teknikler ve yaklaşımlarla geliştirilen ve insan tarafından tanımlanan belirli bir dizi hedef için, etkileşimde bulundukları ortamları etkileyen içerik, tahminler, öneriler veya kararlar gibi çıktılar üretebilen yazılımlardır"* (EPRS) şeklinde tanımlanmıştır. Bu yasa taslağında, risk temelli yaklaşım benimsenmiş olup, yapay zeka sistemleri risk bazında kategorize edilmiştir. Bu sisteme göre 4 temel risk grubu belirlenmiştir.



Şekil 4.1. Risk temelli yaklaşıma göre yapay zeka sistemleri risk kategorileri

Kabul edilemez riskli yapay zeka sistemleri; taslak Yapay Zeka Yasası, insanların güvenliği, geçim kaynakları ve hakları açısından bu sistemlerin yarattığı tehdidin kabul edilemez riski sebebiyle bu zararlı yapay zeka uygulamalarını açıkça yasaklamakta ve bu sistemlerin Avrupa Birliği'nde piyasaya sürülmesini, hizmete sunulması veya kullanılmasını yasaklamaktadır. Bu sistemler şu şekilde sıralanmıştır; zararlı manipülatif bilinçaltı teknikleri uygulayan yapay zeka sistemleri, belirli hassas grupları (fiziksel veya zihinsel engelli) istismar eden yapay zeka sistemleri, kamu yetkilileri tarafından veya onlar adına sosyal puanlama amacıyla kullanılan yapay zeka sistemleri, istisnalar haricinde kolluk kuvvetlerinin amaçları doğrultusunda kamuya açık alanlarda 'gerçek zamanlı' uzaktan biyometrik tanımlama sistemleri.

Yüksek riskli yapay zeka sistemleri; insanların güvenliği veya temel hakları üzerinde olumsuz etki yaratan yapay zeka sistemleri iki kategoriye ayrılarak ele alınmıştır; birincisi, güvenlik bileşeni olarak kullanılan ürünler veya Avrupa Birliği sağlık ve güvenlik uyumlaştırma mevzuatı kapsamına giren sistemler (örneğin oyuncaklar, havacılık, arabalar, tıbbi cihazlar, asansörler), ikincisi, Komisyonun gerektiğinde yetki devri yoluyla güncelleyebileceği, Ek III'te tanımlanan sekiz spesifik alanda konuşlandırılmış sistemler (Madde 7). İkinci kategorideki sistemler şu şekilde sıralanabilir; vatandaşların yaşamını ve sağlığını riske atabilecek kritik altyapılar (örneğin ulaşım), bir kişinin eğitime erişimini ve yaşamının mesleki seyrini belirleyebilecek eğitimsel veya mesleki eğitim (örneğin sınavların puanlanması), ürünlerin güvenlik bileşenleri (örneğin robot yardımcı cerrahide yapay zeka uygulaması), istihdam, çalışanların yönetimi ve mesleğe erişim (örneğin işe alım prosedürleri için CV sıralama yazılımı), temel özel ve kamu hizmetleri (örneğin vatandaşların kredi alma fırsatını engelleyen kredi puanlama), insanların temel haklarına müdahale edebilecek kolluk kuvvetleri (örneğin delillerin güvenilirliğinin değerlendirilmesi), göç, iltica ve sınır kontrolü yönetimi (örneğin seyahat belgelerinin doğruluğunun doğrulanması), adaletin ve demokratik süreçlerin idaresi (örneğin kanunun somut olaylar dizisine uygulanması). (AI Act-Shaping Europe's digital future) Yüksek riskli yapay zeka sistemleri olarak sıralanan tüm bu sistemler, taslak yasa ile bir dizi yeni kurala tabi tutulmuştur. Buna göre, bu sistemlerin sağlayıcılarının, sistemleri piyasaya sürmeden veya hizmete sokmadan önce, Avrupa Birliği çapında bir veri tabanına kaydettirmeleri gerekmektedir. Ayrıca madde 8 ila 15'te öngörülen risk yönetimi, test, teknik sağlamlık, veri eğitimi ve yönetimi, şeffaflık, insan gözetimi ve siber güvenlik konularında bir dizi gerekliliğe de uymak zorunda kalacaklardır. Buna göre, yüksek riskli yapay zeka

sistemlerinin sadece sağlayıcıları değil, ithalatçıları, dağıtıcıları ve kullanıcıları da yasaya göre bir dizi yükümlülüğü yerine getirmek zorundadır. Avrupa Birliği dışından gelen sağlayıcıların ise bu yükümlülüklere ek olarak uygunluk değerlendirmesini sağlamak, pazar sonrası izleme sistemi kurmak ve gerektiğinde düzenleyici önlemler almak için Avrupa Birliği'nde yetkili bir temsilci bulundurması gerekmektedir. Yüz tanıma teknolojilerine (Facial recognition Technologies-FRTs) ayrı bir parantez açılarak, mevcut mevzuata (örneğin GDPR) ek olarak, yüz tanıma teknolojileri için kullanım özelliklerine göre yüksek veya düşük riskli olarak ayrımının yapılarak yeni kurallar getirilmesini öngörmektedir. Gerçek zamanlı yüz tanıma sistemlerinin (real-time facial recognition systems) ise, Avrupa Birliği'ne üye devletlerin kendi iç hukuklarında kamu güvenliği sebebiyle uygun adli ve idari izinleri vermedikleri sürece, kolluk kuvvetlerinin amaçları doğrultusunda kamuya açık alanlarda kullanılmasının yasaklanması öngörülmüştür. Kayıp bir çocuğun aranması, belirli ve yakın bir terör tehdidinin önlenmesi veya ciddi bir cezai suçun failinin veya şüphelisinin tespit edilmesi, yerinin belirlenmesi veya kovuşturulması için gerekli olduğu durumlar gibi dar istisnalar kesin olarak tanımlanmış ve taslak yasada düzenlenmiştir. Ancak kolluk kuvvetlerine hizmet amacı dışında kullanılan yüz tanıma teknolojilerine Avrupa Birliği pazarına girmeden önce uygunluk değerlendirmesi ve güvenlik gerekliliklerine uygunluğa tabi tutularak izin verilebileceği öngörülmüştür.

Sınırlı riskli yapay zeka sistemleri; insanlarla etkileşime giren sistemler (örneğin sohbet botları), duygu tanıma sistemleri, biyometrik kategorizasyon sistemleri, ses, görüntü veya video içeriği üreten veya manipüle eden yapay zeka sistemleri (örneğin deepfake) sınırlı risk arz eden yapay zeka sistemleri olarak bu kategoride ele alınmış ve şeffaflık yükümlülüğüne tabi tutulmuştur. Bu yükümlülüğe göre, sağlayıcılar, koşullar ve kullanım bağlamından açıkça anlaşılamadığı sürece, gerçek kişilerin bir yapay zeka sistemiyle etkileşimde oldukları konusunda bilgilendirilmesini sağlayacak şekilde tasarlanmasını ve geliştirilmesini sağlayacak, sistemin işleyişi hakkında maruz kalan gerçek kişileri bilgilendirecek ve içeriğin yapay olarak oluşturulduğunu veya manipüle edildiğini açıklayacaktır.

Düşük veya minimum riskli yapay zeka sistemleri; taslak yasaya göre, düşük veya minimum riskli yapay zeka sistemleri, (örneğin yapay zeka destekli video oyunları veya spam filtreleri gibi uygulamalar) herhangi ek bir yasal yükümlülük gerektirmeksizin Avrupa Birliği'nde geliştirilebilir ve kullanılabilir.

4.5. Otonom Araçlarda Gizlilik ve Kişisel Verilerin Korunması Çerçevesinde Kullanıcıların Görüşlerinin İncelenmesi

Otonom araç kullanıcılarının gizlilik ve kişisel verilerin korunması çerçevesinde görüşleri hakkında elde edilen veriler aşağıda sunulmaktadır.

Çizelge 4.2. Anket formuna katılan otonom araç kullanıcılarının kişisel özellikleri

ÖZELLİKLER	KATEGORİLER	f	%
Cinsiyet	Kadın	12	32,4
	Erkek	25	67,6
	Toplam	37	100
Eğitim düzeyi	Lisans	16	43,2
	Yüksek Lisans	12	32,4
	Doktora	4	10,8
	Diğer	5	13,5
	Toplam	37	100

Çizelge 4.2.'ye göre katılımcıların %67,6'lık kısmını erkekler oluşturmakta iken, %32,4'lik kısmını kadınlar oluşturmaktadır. Katılımcıların %43,2'sinin lisans, %32,4'si yüksek lisans, %10,8'ü doktora mezunu olduğu görülmekte iken katılımcıların %13,5'i diğer seçeneğini işaretleyerek verilen seçenekler harici bir eğitim düzeyine sahip olduğunu belirtmişlerdir. Katılımcıların %8,1'ünün 1 yıldan az süredir otonom araç kullandığı görülürken, %37,8'ünün 1 ile 5 yıldır otonom araç kullandığı, %27'unun 6 ile 10 yıldır otonom araç kullandığı, %16,2'sinin 11 ile 15 yıldır otonom araç kullandığı ve %10,8'inin ise otonom araç kullandığı görülmektedir.

Çizelge 4.3. Otonom araç kullanıcılarının tercih sebebi

GENEL GÖRÜŞLER	Yakıt Tasarrufu		Yüksek Güvenlik		Sürüş Kolaylığı		Trafik Durumuna Göre Yol Tarifi Vermesi		Diğer		TOPLAM	
	f	%	f	%	f	%	f	%	f	%	f	%
Otonom araç tercih etme sebebiniz nedir?	2	5,4	7	18,9	23	62,2	3	8,1	2	5,4	37	100

Çizelge 4.3.'e göre katılımcıların %62,2'lik çoğunluğunun otonom aracı tercih sebebinin sürüş kolaylığı olduğu görülmektedir. Katılımcıların %18,9'unun otonom aracı tercih etme sebebinin yüksek güvenlik olduğu, %8,1'inin otonom aracı tercih etme sebebinin trafik durumuna göre yol tarifi vermesi olduğu görülmekte iken, %5,4'ü yakıt tasarrufu sebebiyle otonom araç tercih ettiklerini belirtmişlerdir. Katılımcıların %5,4'ü otonom araç tercih sebebinin diğer olarak işaretlemiş ve formda belirtilen tüm seçenekler sebebiyle otonom aracı tercih ettiğini belirtmiştir.

Çizelge 4.4. "Bağlı araç" teriminin ne demek olduğunu bilinmesi

GENEL GÖRÜŞLER	EVET		HAYIR		TOPLAM	
	f	%	f	%	f	%
"Bağlı araç" (connected car) teriminin ne demek olduğunu biliyor musunuz?	18	48,6	19	51,4	37	100

Çizelge 4.4.'e göre, katılımcıların %48,6'sı "bağlı araç" teriminin tanımını bildiğini belirtmişken, %51,4'lük çoğunluk "bağlı araç" teriminin tanımını bilmediğini belirtmişlerdir.

Çizelge 4.5. Otonom araç satın alırken yapılan bilgilendirme

Otonom aracınızı satın alırken size hangi konularda bilgilendirme yapıldı?	İŞARETLENME SAYI VE YÜZDESİ	
	f	%
Bilgilendirme yapılmadı	8	16
Genel sürüş özellikleri	21	42
Ana ekranda mevcut kısa yollar	9	18
"Bağlı araç"(connected car) olmasından kaynaklı araçta mevcut özellikler	10	20
Aracın kaydettiği verilerin neler olduğu	1	2
Diğer	1	2
TOPLAM	50	100

(Çoktan seçmeli soru olmasından dolayı bazı seçenekler birden fazla kere tercih edildiğinden genel toplam sayısı fazla çıkmaktadır.)

Çizelge 4.5.'e göre, katılımcıların %42'sine otonom araçlarını satın alırken genel sürüş özellikleri hakkında bilgi verildiği görülmekte olup, bağlı araç olmasından kaynaklı araçta mevcut özellikler hakkında katılımcıların %20'sine bilgi verildiği, ana ekranda mevcut kısa yollara ilişkin katılımcıların %18'ine bilgi verildiği, aracın kaydettiği verilerin neler olduğuna ilişkin katılımcıların %2'sine bilgi verildiği görülmektedir. Katılımcıların %16'sına herhangi bir bilgilendirme yapılmadığı anlaşılmaktadır. Ayrıca katılımcıların %2'si diğer seçeneğini işaretlemiş olup, genel bilgilendirme yapıldığını belirtmişlerdir.

Çizelge 4.6. Otonom aracın kaydettiği verilerin kişisel veri olup olmadığına ilişkin görüşler

GENEL GÖRÜŞLER	EVET		HAYIR		TOPLAM	
	f	%	f	%	f	%
Otonom aracınızın kaydettiği verilerin kişisel veri olduğunu düşünüyor musunuz?	22	59,5	15	40,5	37	100

Çizelge 4.6.'ya göre, katılımcıların %59,5'u otonom araçların kaydettiği verilerin kişisel veri olduğunu düşünmekte olup, katılımcıların %40,5'i otonom araçların kaydettiği verilerin kişisel veri olmadığını düşünmektedir.

Çizelge 4.7. Otonom araçta kaydedilen verilerin güvenli şekilde saklanıp saklanmadığına ilişkin görüşler

GENEL GÖRÜŞLER	EVET		HAYIR		TOPLAM	
	f	%	f	%	f	%
Otonom aracınızda kaydedilen verilerin güvenli bir şekilde saklandığını düşünüyor musunuz?	17	45,9	20	54,1	37	100

Çizelge 4.7.'ye göre, katılımcıların %54,1'i otonom araçta kaydedilen verilerin güvenli bir şekilde saklanmadığını düşünürken, katılımcıların %45,9'u otonom araçta kaydedilen verilerin güvenli bir şekilde saklandığını düşünmektedir.

Çizelge 4.8. Otonom aracın veri kaydı özelliği devre dışı bırakılabiliyor olsaydı bu özelliğin kapatılmak istenip istenmeyeceği

GENEL GÖRÜŞLER	EVET		HAYIR		TOPLAM	
	f	%	f	%	f	%
Otonom aracınızın veri kaydı özelliğini devre dışı bırakabiliyor olsaydınız bu özelliği kapatmak ister miydiniz?	18	48,6	19	51,4	37	100

Çizelge 4.8.'e göre, katılımcıların %51,4'ü otonom araçlarının veri kaydı özelliğini devre dışı bırakabiliyor olsalardı bu özelliği kapatmak istediklerini belirtmişken, katılımcıların %48,6'sı bu özelliği devre dışı bırakabiliyor olsalar dahi kapatmak istemeyeceklerini belirtmişlerdir.

Çizelge 4.9. Otonom aracın kaydettiği verilerin kimlerle paylaşıldığı konusunda izin verilip verilmediği

GENEL GÖRÜSLER	EVET		HAYIR		TOPLAM	
	f	%	f	%	f	%
Otonom aracınızın kaydettiği verilerin kimlerle paylaşıldığı konusunda bir izin verdiniz mi?	5	13,5	32	86,5	37	100

Çizelge 4.9.'a göre, katılımcıların %86,5'u otonom araçlarının kaydettiği verilerin kimlerle paylaşıldığı konusunda bir izin vermediklerini belirtmişken, katılımcıların %13,5'u otonom araçlarının kaydettiği verilerin kimlerle paylaşıldığı konusunda izin verdiklerini belirtmişlerdir.

Çizelge 4.10. Otonom aracın kaydettiği verilerin üçüncü taraflar ile paylaşılmadan önce kullanıcılardan onay alınması

GENEL GÖRÜSLER	EVET		HAYIR		TOPLAM	
	f	%	f	%	f	%
Otonom aracınızın kaydettiği verilerin üçüncü taraflar ile paylaşılırken onayınızın alınmasını ister miydiniz?	34	91,9	3	8,1	37	100

Çizelge 4.10.'a göre, katılımcıların %91,9'u otonom araçlarının kaydettiği verilerin üçüncü taraflar ile paylaşılırken onaylarının alınmasını istediklerini belirtmişken, katılımcıların %8,1'i otonom araçlarının kaydettiği verilerin üçüncü taraflar ile paylaşılırken onaylarının alınmasını istemediklerini belirtmişlerdir.

Çizelge 4.11. Otonom araçta kaydedilen verilerden hangilerinin kontrol edilmek istendiği

Otonom aracınızda kaydedilen veriler ile ilgili olarak hangilerini kontrol etmek isterdiniz?	İŞARETLENME SAYI VE YÜZDESİ	
	f	%
Ne kadar süre paylaşılacağını	11	18,3
Üçüncü kişilerle yapılan paylaşımı	23	38,3
Verdiğim izni istediğim zaman geri alabilmeyi	24	40

Diğer	2	3,3
TOPLAM	60	100

(Çoktan seçmeli soru olmasından dolayı bazı seçenekler birden fazla kere tercih edildiğinden genel toplam sayısı fazla çıkmaktadır.)

Çizelge 4.11.'e göre, katılımcıların %40'ı otonom araçlarında kaydedilen veriler ile ilgili verdikleri izinleri istedikleri zaman geri alabilmeyi istediklerini belirtirken, katılımcıların %38,3'ü otonom araçlarında kaydedilen veriler ile ilgili üçüncü kişilerle yapılan paylaşımı kontrol etmek istediklerini, katılımcıların %18,3'ü otonom araçlarında kaydedilen veriler ile ilgili bu verilerin ne kadar süre paylaşılacağını kontrol etmek istediklerini, katılımcıların %3,3'ü otonom araçlarında kaydedilen veriler ile ilgili diğer seçeneğini işaretleyerek verilen tüm seçenekleri kontrol etmek istediğini belirtmiş, ayrıca bir diğer katılımcı ise nelerin ne amaçla kaydedildiğini daha detaylı bilmek istediğini belirtmiştir.

Çizelge 4.12. Otonom araçta kaydedilen veriler ile ilgili kullanıcıları endişelendiren konular

Otonom aracınızda kaydedilen veriler ile ilgili olarak sizi en çok hangileri endişelendirebilir?	İŞARETLENME SAYI VE YÜZDESİ	
	f	%
Kişisel bilgilerimin ifşa olması	20	26,3
Kişisel verilerimin ticari/reklam amacıyla kullanılması	20	26,3
Araç korsanlığı (araçtaki verilerinize yetkisiz erişim)	19	25
Araç konum takibi	16	21,1
Diğer	1	1,3
TOPLAM	76	100

(Çoktan seçmeli soru olmasından dolayı bazı seçenekler birden fazla kere tercih edildiğinden genel toplam sayısı fazla çıkmaktadır.)

Çizelge 4.12.'ye göre, katılımcıların %26,3'ü otonom araçlarında kaydedilen veriler ile ilgili kişisel bilgilerinin ifşa olmasından endişelenebileceğini belirtirken, katılımcıların %26,3'ü

otonom araçlarında kaydedilen veriler ile ilgili kişisel verilerinin ticari/reklam amacıyla kullanılmasından endişelenebileceğini belirtmişlerdir. Katılımcıların %25'i otonom araçlarında kaydedilen veriler ile ilgili araç korsanlığından endişelenebileceğini belirtmiş, katılımcıların %21,1'i otonom araçlarında kaydedilen veriler ile ilgili araç konum takibinden endişelenebileceğini belirtmiştir. Ayrıca katılımcıların %1,3'ü otonom araçlarında kaydedilen veriler ile ilgili diğer seçeneğini işaretleyerek verilen tüm seçeneklerin kendisini endişelendireceğini belirtmiştir.

Çizelge 4.13. Otonom aracın kaydettiği hangi verileri paylaşırken kullanıcılar rahat hisseder

Otonom aracınızın kaydettiği verilerden hangilerini paylaşırken rahat hissedersiniz?	İŞARETLENME SAYI VE YÜZDESİ	
	f	%
Araç arıza bilgileri	29	29,6
Araca ait veriler (kilometre bilgisi, yağ-su-yakıt seviyeleri vb)	20	20,4
Sürüş profili (hız bilgisi, fren kullanım alışkanlığı vb)	13	13,3
Sürüş alışkanlıkları (ana ekran kısa yollarının kullanımı, koltuk oturma tercihleri vb)	11	11,2
GPS Konum	8	8,2
Eğlence tercihleri (müzik, film, oyun vb)	5	5,1
"Bağlı araç" özelliklerinin kullanımı (sıklık, süre, konum, kişisel tercihler)	3	3,1
Araç kamera kayıtları	5	5,1
Sürücünün kimlik bilgileri	2	2
Araca bağlanan telefon, tablet vb aletlerden alınan veriler (mesaj, email, telefon numaraları vb)	2	2
TOPLAM	98	100

(Çoktan seçmeli soru olmasından dolayı bazı seçenekler birden fazla kere tercih edildiğinden genel toplam sayısı fazla çıkmaktadır.)

Çizelge 4.13.'e göre, katılımcıların %29,6'sı otonom araçlarında kaydedilen araç arıza bilgilerini paylaşırken rahat hissedeceğini belirtmiş, katılımcıların %20,4'ü otonom araçlarında kaydedilen araca ait verileri (kilometre bilgisi, yağ-su-yakıt seviyeleri vb)

paylaşırken rahat hissedeceğini belirtmiş iken katılımcıların %13,3'ü otonom araçlarında kaydedilen sürüş profilini (hız bilgisi, fren kullanım alışkanlığı vb) paylaşırken rahat hissedeceğini belirtmiştir. Katılımcıların %11,2'si otonom araçlarında kaydedilen sürüş alışkanlıklarını (ana ekran kısa yollarının kullanımı, koltuk oturma tercihleri vb) paylaşırken rahat hissedeceğini belirtmiş, katılımcıların %8,2'si otonom araçlarında kaydedilen GPS konum bilgisini paylaşırken rahat hissedeceğini belirtmiş, katılımcıların %5,1'i otonom araçlarında kaydedilen eğlence tercihlerini (müzik, film, oyun vb) ve araç kamera kayıtlarını paylaşırken rahat hissedeceğini belirtmiş, katılımcıların %3,1'i otonom araçlarında kaydedilen "bağlı araç" özelliklerinin kullanımını (sıklık, süre, konum, kişisel tercihler) paylaşırken rahat hissedeceğini belirtmiş, katılımcıların %2'si otonom araçlarında kaydedilen sürücünün kimlik bilgileri ve araca bağlanan telefon, tablet vb aletlerden alınan veriler (mesaj, email, telefon numaraları vb) paylaşırken rahat hissedeceğini belirtmiştir.

Çizelge 4.14. Otonom aracın kaydettiği verilerin kullanıcılar hangi durumlarda paylaşılmasını kabul eder

Aşağıdaki durumlardan hangisinde aracınızın kaydettiği verilerin paylaşılmasını kabul ederdiniz?	İŞARETLENME SAYI VE YÜZDESİ	
	f	%
Aracınız bozuldu ve yol yardım yetkilisi aracınızın konumuna ve bilgilerine ulaşmak istiyor	32	38,6
Aracınızı bakım yaptırdığınız servis uzaktan aracınızın bilgilerine erişmek istiyor	16	19,3
Sigorta şirketi aracınızın kilometre bilgisini öğrenerek sigorta primi teklifinde bulunmak istiyor	11	13,3
Sigorta şirketi aracınızı kullanma alışkanlıklarınıza (hızlanma, frenleme vb) göre sigorta primi teklifinde bulunmak istiyor	5	6
Aracınızı üreten firma, araç güncellemelerini otomatik olarak bildirebilmek için aracınızı izlemek istiyor	12	14,5
Aracınız, telefonunuzdaki kişileri, epostaları, mesajları, arama geçmişinizi senkronize etmek istiyor	7	8,4
TOPLAM	83	100

(Çoktan seçmeli soru olmasından dolayı bazı seçenekler birden fazla kere tercih edildiğinden genel toplam sayısı fazla çıkmaktadır.)

Çizelge 4.14.'e göre, katılımcıların %38,6'sı otonom aracı bozulduğunda yol yardım yetkilisi aracınızın konumuna ve bilgilerine ulaşmak istemesi durumunda aracının kaydettiği verilerin paylaşılmasını kabul edeceğini belirtmiş, katılımcıların %19,3'ü aracını bakım yaptırdığı servis uzaktan aracın bilgilerine erişmek istemesi durumunda aracının kaydettiği verilerin paylaşılmasını kabul edeceğini belirtmiş, katılımcıların %14,5'i aracını üreten firma, araç güncellemelerini otomatik olarak bildirebilmek için aracını izlemek istemesi durumunda aracının kaydettiği verilerin paylaşılmasını kabul edeceğini belirtmiş, katılımcıların %13,3'ü sigorta şirketi aracının kilometre bilgisini öğrenerek sigorta primi teklifinde bulunmak istemesi durumunda aracının kaydettiği verilerin paylaşılmasını kabul edeceğini belirtmiş, katılımcıların %8,4'ü aracın, telefondaki kişileri, epostaları, mesajları, arama geçmişini senkronize etmek istemesi durumunda aracının kaydettiği verilerin paylaşılmasını kabul edeceğini belirtmiş, katılımcıların %6'sı ise sigorta şirketi aracı kullanma alışkanlıklarına (hızlanma, frenleme vb) göre sigorta primi teklifinde bulunmak istemesi durumunda aracının kaydettiği verilerin paylaşılmasını kabul edeceğini belirtmiştir.

Çizelge 4.15. Otonom araç bozulduğunda kullanıcıların bir tuş ile yardım çağırma ve arıza hakkında bilgi gönderebilme durumunda verilerini paylaşmak isteyip istemedikleri

GENEL GÖRÜSLER	EVET		HAYIR		TOPLAM	
	f	%	f	%	f	%
Aracınız bozulduğunda, araçta bulunan bir tuş ile, yardım çağırma ve arızanız hakkında bilgi gönderebilme durumunda verilerinizi paylaşmak ister misiniz?	37	100	0	0	37	100

Çizelge 4.15.'e göre, katılımcıların %100'ü otonom araçları bozulduğunda, araçta bulunan bir tuş ile, yardım çağırma ve arıza hakkında bilgi gönderebilme durumunda verilerini paylaşmak istediklerini belirtmişlerdir.

Çizelge 4.16. Otonom araç bozulduğunda kullanıcıların yardım çağırma ve arıza hakkında bilgi gönderebilme durumunda verilerini paylaşacağı yol yardım servisini seçmek isteyip istemeyecekleri

GENEL GÖRÜSLER	EVET		HAYIR		TOPLAM	
	f	%	f	%	f	%
Yardım çağırma ve arızanız hakkında bilgi gönderebilme durumunda verilerinizi paylaşacağınız yol yardım servisini kendiniz seçmek ister miydiniz?	34	91,9	3	8,1	37	100

Çizelge 4.16.'ya göre, katılımcıların %91,9'u yardım çağırma ve arıza hakkında bilgi gönderebilme durumunda verilerini paylaşacağı yol yardım servisini kendisi seçmek istediğini belirtmişken, katılımcıların %8,1'i böyle bir durumda yol yardım servisini kendisi seçmek istemediğini belirtmişlerdir.

Çizelge 4.17. Otonom araç kullanıcılarının kaydedilen veriler ile alakalı hukuki bir düzenleme gerekip gerekmediği ile alakalı düşünceleri

GENEL GÖRÜSLER	EVET		HAYIR		TOPLAM	
	f	%	f	%	f	%
Otonom aracınızda kaydedilen veriler ile alakalı hukuki bir düzenleme olması gerektiğini düşünüyor musunuz?	34	91,9	3	8,1	37	100

Çizelge 4.17.'ye göre, katılımcıların %91,9'u otonom araçta kaydedilen veriler ile alakalı hukuki bir düzenleme olması gerektiğini düşündüğünü belirtirken, katılımcıların %8,1'i hukuki bir düzenlemeye ihtiyaç olmadığını belirtmiştir.

4.6.Otonom Araçlarda Gizlilik ve Kişisel Verilerin Korunması Çerçevesinde Uzmanların Görüşlerinin İncelenmesi

Otonom araç alanında çalışan uzmanların gizlilik ve kişisel verilerin korunması çerçevesinde yöneltilen sorulara verdikleri cevaplar veriler sunulmaktadır.

Çizelge 4.18.Otonom araç alanında çalışan uzmanların gizlilik ve kişisel verilerin korunması çerçevesinde görüşleri

SORULAR	GÖRÜŞLER
<i>Otonom araçların güvenli olduğunu düşünüyor musunuz?</i>	A Kişisi: Otonom araçlar belirli hesaplamalar sonucunda tasarlanmıştır. Örneğin viraja hangi hızla girilirse araç içerisindeki yolcular savrulmaz, hangi hızla gidilirse yolcular ayakta yolculuk yaparken zorlanmazlar gibi durumlar önceden hesap edilmiştir ve araç buna uygun hareket etmektedir. Ayrıca otonom araçta araç takip sistemi bulunmaktadır. Önündeki araçla olan mesafesini önceden belirlenen takip mesafesine göre ayarlamaktadır. Araç takip sistemi sayesinde önündeki aracın aniden durması durumunda takip mesafesini koruduğundan herhangi bir kazaya mahal vermeyecektir. “Fault tolerance” (hata toleransı) sistem yani hata olduğunda tolere eden sistem geliştirilmeye çalışılmaktadır. Bunun anlamı şudur; %100 hatasız bir sistem geliştirmek çok zordur. Bunun yerine iki tane %98 hata oranlı sistem geliştirip hatayı tolere edebilir şekilde geliştirilmesi tercih edilendir. “Risk minör system” (riski minimize eden sistem) geliştirilmeye çalışılmaktadır. Tüketici yani insanlar “risk aware” (risk farkındalığı) değillerdir. Bu sebeple otonom araçlar çok daha güvenlidir.

<i>Otonom araçların kişisel verilerle ilgili problem teşkil edebileceğini düşünüyor musunuz? Düşünüyor iseniz hangi açıdan problem çıkabilir?</i>	A Kişisi: Otonom araçların kaydettiği veriler doğru bir şekilde işlenip korunamazsa kişisel veriler açısından problem yaratabilir. Sistem pek çok kamera ile çalıştığından çevredeki insanların yüzlerini, sokakları, evleri, araç plakalarını vb. görüntülemektedir. Bu kameralar ile kaydedilen görüntüler kişisel veriler açısından risk teşkil edebilir. B Kişisi: Aracın dış kamera sistemi ile çevresinin izlenebiliyor olması beraberinde başka problemleri de getirmektedir. Bu araçların kameraları uzaktan araç sahibinin kamerayı açıp izlediği durumda dışarıdaki kişilere kamera çalışıyor uyarısı vermemektedir. Aranan bir kişinin otonom araçlarda bulunan bu kamera sistemlerinin de katkısıyla bulunması sadece saniyeler sürer ve bu da kişilerin özgürlüğünün kısıtlanmasıdır. Keza bir kişi, sosyal medya kullanmayarak, internet kullanmayarak yüzünü gizli tutabilir. Ancak kişi, bir noktada sokağa çıkmak zorundadır ve yüzünü gizlemesi gibi bir durum söz konusu değildir. Bu ve benzeri durumlar otonom araçlarda kişisel veri riskini gündeme getirir.
<i>Otonom araçlarda etik ile ilgili herhangi bir kodlama var mıdır?</i>	A Kişisi: Bu noktada araçta etikle alakalı olarak herhangi bir kodlama yoktur. Önüne herhangi bir cisim çıktığında durmaktadır. Bu noktada felsefeci Philippa Foot ve Judith Jarvis'in ortaya attığı Vagon İkilemi (Trolley Dilemma)'ndeki durum gibi aracın önüne çıkan yol ayrımında bir kişinin mi yoksa dört kişinin mi üzerine sürecektir gibi bir ikilemde kalması söz konusu değildir. Bu noktada araç, önüne çıkan aracın hareketini engelleyici herhangi bir cisim gördüğünde durmak üzere tasarlanmıştır. Yola yaya çıktığında otomatik olarak durmaktadır. Bizlerin kullanmakta olduğu araçlarda yaya

	yola çıkmaya çalıştığında “nasılsa benim aracımı görüyor, yola devam edebilirim” şeklinde düşünerek aracı sürmeye devam ediyoruz. Bu sistemlerin böyle bir düşünce sistemi yoktur. Yola yaya çıktığında direkt olarak durmaktadır. Hatta önünden kuş geçtiğinde dahi durmaktadır. Yerel alanda mevcut hız sınırlarını aşmamaktadır. Çevredeki statik durumu bilmektedir.
<i>Geliştirdiğiniz sistem dışarı ile veri paylaşıyor mu?</i>	A Kişisi: Firma olarak dışarı ile veri paylaşımı yapılmamaktadır, dışarıdan yalnızca yazılım kullanılmaktadır.
<i>Otonom araçların ulusal güvenlik açısından risk taşıdığı söylenebilir mi?</i>	B Kişisi: Otonom araçlardan bahsedildiğinde ayrıca ulusal güvenlik meselesi gündeme gelmektedir. Keza özellikle askeri güvenlik çevresinde bu araçların dolanması, ülkeler için gizli olan askeri bilgilerin toplanması anlamına gelecektir. Devletlerin bu bilgilerin başka ülkelerle paylaşılmasını ve bu bilginin dışarı çıkmamasını talep etmesi muhtemeldir. Bu durum da araç üreticileri için farklı ülkelerde pazara girmede zorluklara sebep olmaktadır. Üreticiler bu bilgilerin kaydedilmesine meşru sebep olarak; sürüş, yaya ve yol güvenliği gibi sebepler öne sürebilirler. Özellikle external vehicle camera (araç dışı kameraları) bu anlamda data topladıkları için probleme yol açmaktadırlar. Avrupa Birliği bu açıdan sessiz kalmaktadır. Bu noktada bir düzenleme yapılması inisiyatifi her ülkenin kendisine bırakmıştır. Yani kamusal alanda veri toplanması ülkelerin kendisine bırakılmıştır.
<i>Paylaşımlı araçları; uber, ride share vb. otonom araçlar açısından nasıl değerlendiriyorsunuz?</i>	B Kişisi: Elde edilen veriler yolcu hakkında reklam açısından kullanılabilir bilgi demektir. Örneğin, araç içerisinde saç kesimine ihtiyacı olan kişinin belirlenmesi, araç içerisinde Netflix izlenirken kişisel tercihlerle ilgili

	bilgi toplanması ve buna göre kiřiye özel reklam gösterilmesi için kullanılabilir.
<i>Otonom araçlarda kaydedilen verilere kimlerin erişimi olmalı?</i>	C Kişisi: Otonom araçlarda kaydedilen verilere araç sahibinin erişimi kısıtlanmalıdır. Örneğin, bir araç kazasından sonra kusur belirlemek için otonom aracın kaydetmiş olduğu kayıtlara erişerek kusur oranının kolaylıkla belirlenmesi mümkündür. Ancak araç sahibinin bu verilere erişmesi demek, bu verilere üzerinde değişiklik yapabilmesinin yanında yok edebilmesi demektir. Bu sebeple tıpkı uçaklarda olduğu gibi araçta verilerin kaydedildiği bir kara kutu olmalı ve bu verilere ancak yetkili makamların izni ile erişilebilmelidir.

4.7.Otonom Araçlarda Mahremiyete İlişkin Olası Problemlerin İncelenmesi

Avrupa düzeyinde mahremiyetin yasal olarak korunması, Avrupa Konseyi'nin Avrupa İnsan Hakları Sözleşmesi'ni (AİHS) hazırladığı ve böylece bir kişinin kişisel özgürlüğünü koruduğu 1950 yılına kadar uzanmaktadır. Avrupa Birliği, 1995 yılında yayınlanan 95/46/EC sayılı Direktif aracılığıyla kişisel verilerin işlenmesini koruma ihtiyacı görmüştür. Bu Direktif, 25 Mayıs 2018 tarihinde Genel Veri Koruma Tüzüğü ile değiştirilmiştir (Mulder & Vellinga, 2021).

B kişinin görüşü çerçevesinde; araç içi ve dışı kameraların aldığı kayıtlar hem kişiler hem de ülkelerin ulusal güvenliği açısından risk teşkil etmektedir. Araç içinde ve dışında kayıt alan (internal, external) kameralar kişilerin biyometrik verilerini elde etmektedir. Bunun yanında bu araçlar, askeri bölgelerden geçerken bu kameralar sayesinde ülkelerin ulusal güvenliği kapsamında değerlendirilebilecek veriler toplamaktadırlar. Otonom araçlar, bağlı araçlar (connected car) kategorisinde yer almaktadır. Yani bu araçlarda internet erişimi mevcut olup, verileri aracın içindeki ve dışındaki diğer cihazlarla paylaşabilmektedir. Bu durum da araçların elde ettiği verilerin diğer ülkelere aktarılması ihtimalini gündeme getirmektedir.

Araç kullanım alışkanlığının kaydedilerek sigorta priminin belirlenmesi de bir diğer riski oluşturmaktadır. Otonom araçlar, gelişen teknolojiyle birlikte kullanıcıların/sürücülerin araç kullanma alışkanlıklarını kaydetme (örneğin ani hız ani fren, aşırı hız, trafik kurallarına uyup uymama alışkanlıkları) riskini taşımaktadır. Bu verilerin sigorta şirketleri ile paylaşılması sonucunda kişilerin sigorta primlerinin bu verilere göre arttırılması söz konusu olabilecektir. Araç sistemine izinsiz erişim de bir diğer risktir. Belirtildiği üzere, otonom araçlar bağlı araç (connected car) olduklarından, wi-fi erişimi özelliği, bu araçları siber saldırı ve izinsiz erişimlere açık hale getirmektedir.

B kişinin görüşü çerçevesinde; otonom araçlar hem sürücü hem de yolcuların pek çok verisini kaydedebilme özelliğine sahip olduklarından profillemeye yani kişiye özel reklam riskini de beraberinde getirmektedir. Örneğin, araçta konuşulan bir konuda sürücünün araca bağlı telefonuna bu konuşma konusuna göre reklam verilmesi, sürekli gidildiği belirlenen bir kafenin reklamlarının bu araç kullanıcısına gönderilmesi gibi sorunları beraberinde getirmektedir.

Özellikle otonom toplu taşımalarda yolcu verisinin kaydedilmesi de profillemeye açısından risk teşkil etmektedir. Örneğin otonom otobüsteki kadın-erkek oranına göre tıraş bıçağı reklamı mı yoksa bir kadın parfümü reklamının mı verileceğine karar verilmesi gibi sorunları beraberinde getirmektedir.

5.SONUÇ ve ÖNERİLER

Mevcut durumda otonom sistemlerin ve otonom araçların kaydettikleri veriler ile alakalı detaylı ve yeterli hukuki düzenlemeler olmadığı sonucuna ulaşılmıştır. Uygulamadan örnek vermek gerekirse; Tesla araçlarının sahip olduğu “sentry mode (nöbetçi modu)”un kişisel veriler açısından risk taşıdığı söylenebilir. Firma tarafından yapılan tanıtıma göre bu özellik, araçta olağandışı bir aktivite meydana geldiğinde araç sahibinin telefonuna bildirim göndererek araç çevresinin izlenmesini sağlamaktadır ve araç kamerasının kayıt yaptığına ilişkin araç çevresindeki kişilere hiçbir bildirim yapılmamaktadır. Bu özelliğin kullanılmasını engelleyici veya bu özelliğin hangi şartlar altında nasıl kullanılması gerektiğini düzenleyici herhangi bir hukuk normu bulunmamaktadır. Bu incelemelerden yola çıkarak uygulamaya yönelik önerimiz ise otonom aracın kamera görüntüleri, uzaktan anlık erişime açık olmamalıdır. Ancak açıkça tehlike arz eden durumlarda bu kurala istisna getirilebilir. Mevcut durumda araçlarda bulunan alarm mekanizmaları ve araç takip sistemleri hırsızlık gibi durumları engellemeye yönelik halihazırda işlev gören mekanizmalardır. Çalışmada yer verilen hukuksal düzenlemelerle çerçevesi çizilmiş olan mahremiyeti korumaya yönelik ilkeler kamera kullanımının amacının meşru olmasını, kullanım açısından orantılılığın esas alınması gerektiğini belirtmektedir. Bu durumda güvenlik açısından başka yollarla eğer risk bertaraf edilebiliyorsa kamera verilerine meşru bir sebep olmaksızın anlık erişim hukuki çerçevenin dışına çıkmak demektir. İstisna sayılabilecek durumlar ise yoruma açık olmaktan çıkartılarak çerçevesi net olarak çizilmelidir. Örneğin, sokakta oyun oynayan çocukların topunun araca çarpması gerçek bir risk olmayıp, basit bir alarm ile bertaraf edilebilir. Ancak aracın kapıları anahtar dışında bir alet kullanılarak açılmış veya direksiyon koltuğunda oturan sürücünün aracın sahibi olmadığının araç içi kamerası ile tespitinin yapılması durumunda araç sahibinin telefonuna bildirim gönderilerek anlık kamera görüntülerine erişim izni verilebilir. Bu durum da süre sınırına tabi olmalı, araç sahibinin güvenlik onayı vermesi ile kayda erişim sonlanmalı ya da araç sahibinin anlık onay vermemesi durumunda belirli bir süre kayda devam ettikten sonra kayıt otomatik olarak sonlandırılmalıdır. Benzer şekilde aracın kaydettiği kamera görüntülerine geçmişe dönük olarak araç sahibinin erişimine izin verilmemelidir. Bu durum hem kişisel veri hem de güvenlik sebebiyle önem arz etmektedir. Örneğin araç sahibinin kamera görüntülerini açarak kayıttaki kişilerin görüntülerini izlemesi özel hayatın gizliliğini ve araç çevresinde bulunan kişilerin mahremiyet beklentilerini ihlal edecektir. Aracın bir kazaya karışması durumunda ise araç sahibinin kazaya ilişkin görüntülere erişerek kendi

lehine görüntülerde değişiklik yapması veya silmesi söz konusu olabilecektir. Bu sebeple geçmişe dönük kamera verileri, yalnızca yetkili makamların izni ile erişime açılabilmelidir. Tıpkı sivil uçaklarda bulunan “kara kutu”lar gibi (askeri kara kutularda verilerin düşmana geçmeden ortadan kaldırılmasını sağlamak için bir silme tuşu mevcut iken sivil kara kutularda bu sistem bulunmamaktadır) otonom araçlara da bir “kara kutu” sistemi getirilerek verilere ancak belirli koşullar altında erişim sağlanabilmelidir.

KVKK ve GDPR’da öngörülen anonimleştirme bu sistemler açısından ciddi öneme sahiptir. Kamera kayıtları ile kaydedilen kişisel verilerin –özellikle biyometrik verilerin- anonimleştirilmesi şarttır. Anonimleştirme işleminin nasıl yapılması gerektiği üreticiler açısından detaylandırılmalı ve “anlık anonimleştirme” zorunlu hale getirilerek, kameranın kayıt almaya başladığı anda veri kaydedilirken anonimleştirme işlemi başlatılmalıdır. Veri kaydedildikten sonra anonimleştirilmesi, sisteme izinsiz giriş durumunda kişisel veriler açısından ciddi bir risk teşkil etmektedir ve bu araçların “connected car”(bağlı araç) özellikleri dikkate alındığında sisteme izinsiz girişlerin imkan dahilinde olduğu açıktır. Bağlı araçların bu özellikleri, askeri bölgelerde ayrıca risk oluşturmakta olduğundan ülkeler, askeri bölgelerde seyir eden otonom araçlar ile ilgili kendi iç hukuki düzenlemeleri ile bir çerçeve çizmelidir. Aksi durumda, kamera ile kayıt yapılmasının yasak olduğu askeri bölgelerde otonom araç kameraları ile kayıt alınması, ülkeler için güvenlik tehdidi oluşturacaktır.

Çalışmamızda belirttiğimiz üzere, FIA (Fédération Internationale de l’Automobile) otomobil üreticilerinin her bir model için toplanan, işlenen, depolanan ve harici olarak iletilen tüm araç verilerini bir liste halinde yayınlaması gerektiğini ve bu listenin, tüketiciler tarafından kolayca erişilebilir ve anlaşılır olması gerektiğini belirtmiştir. Bu görüşe katıldığımızı belirterek, tüketicilerin otonom araç satın alırken hangi verilerinin kaydedildiği konusunda bilgilendirilmesi gerekmektedir.

Otonom araçların günlük hayatlarımızı kolaylaştırması yanında mahremiyete ilişkin beraberinde getirdiği soru işaretleri ancak hukuk normları ile giderilebilir. Bu sebeple hem kullanıcılar hem de üreticiler açısından bu hukuk normlarının hayata geçirilmesi önem arz etmektedir. Böylece güvenilir otonom sistemler ve otonom araçlar üretilecek ve kişilerin özel hayatlarının gizliliğinin sağlanması ile özgürlükleri kısıtlanmamış olacaktır.

Kişisel verilerin güvenliğini sağlamak için, otonom sistem üreticilerine en başından itibaren açık talimatlar ve yönergeler oluşturmak gerekir. Bu belgeler, servis sağlayıcılar ve otomobil üreticileri tarafından daha iyi veri işlemeye yol açmalı ve böylece veri sızıntısını önlemeli ve ilgili riskleri azaltmalıdır.

Bu çalışmada, otonom sistemler gizlilik ve kişisel verilerin korunması çerçevesinde incelenmiş olup, otonom araçlara yönelik mahremiyet problemleri ele alınarak çözüm önerilerinde bulunulmuştur. Ancak bilindiği üzere, otonom araçların güvenliği meselesi de gündemdedir. Amerikan kredi kuruluşu LendingTree'nin 30 otomobil markası üzerinde sürücülerin yaptığı kaza oranlarına ilişkin yaptığı çalışmada en yüksek kaza oranına sahip marka bin sürücü başına 23,54 kaza oranı ile Tesla başta gelirken, bin sürücü başına Ram 22,76 kaza, Subaru 20,90 kazaya karışmıştır. (Oksijen, 2023) İleride yapılacak çalışmalarda, otonom araçların gerçekleştirdiği kazalar göz önüne alınarak, kazaya sebep olan faktörler bağlamında güvenlik açısından değerlendirilebilir. Ayrıca otonom araçlar dışında pek çok otonom sistem kullanılmaktadır. İleride yapılacak olan çalışmalarda farklı otonom sistemler teknik ve hukuki boyutuyla değerlendirilebilir.



KAYNAKLAR

- Akıncı, A. N. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün getirdiği yenilikler ve Türk hukuku bakımından değerlendirilmesi: Çalışma raporu-6*. TC Kalkınma Bakanlığı.
- Allen, C., Wallach, W., & Smit, I. (2006). Why machine ethics?. *IEEE Intelligent Systems*, 21(4), 12-17
- Aşıkoğlu, Ş. İ. (2018). *Avrupa Birliği ve Türk hukukunda kişisel verilerin korunması ve büyük veri* (Master's thesis, Sosyal Bilimler Enstitüsü).
- Aull Davies, C. (1999). *Reflexive Ethnography A Guide to Researching Selves and Others*. London, New York: Routledge
- Başer, E. (2022). *Tarım robotları için IMU ve GPS destekli yersel koordinat sistemi platformunun geliştirilmesi*, Yüksek Lisans Tezi, Akdeniz Üniversitesi Fen Bilimleri Enstitüsü, Antalya.
- Bayındır, S. (2021) Otonom Araçlarda Sözleşme Dışı Hukuki Sorumluluk Hallerinin Değerlendirilmesi. *İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi*, 7(2), 383-410.
- Bilik, I., Longman, O., Villeval, S., & Tabrikian, J. (2019). The rise of radar for autonomous vehicles: Signal processing solutions and future research directions. *IEEE signal processing Magazine*, 36(5), 20-31.
- Buğra, A. (2020). *Sigorta Hukukunun İki Güncel Sorunu: İnsansız Araçlar - Sorumluluk ve Sağlık Sigortalarında Birden Çok Sigorta Sempozyumu*. S. Amasya (Yay. haz.), Otomatik Yönlendirme Seviyesi Yüksek Kara Araçları ve Sigorta. (Birinci Baskı) Türkiye: On İki Levha Yayıncılık, 2-9.
- Campbell, S., O'Mahony, N., Krpalcova, L., Riordan, D., Walsh, J., Murphy, A., & Ryan, C. (2018, June). Sensor technology in autonomous vehicles: A review. In *2018 29th Irish Signals and Systems Conference (ISSC)* (pp. 1-4). IEEE.
- Canbay, P., Demircioğlu, Z. (2021). Endüstri 5.0'a doğru: zeki otonom sistemlerde etik ve ahlaki sorumluluklar. *AJIT-e: Bilişim Teknolojileri Online Dergisi*, 12(45), 106-123.
- Cate, F. H. (2003). *The Privacy Problem*. A First Amendment Center Publication.
- Cavoukian, A. (2009). *Privacy by design, take the challenge*. Kanada: Information and Privacy Commissioner of Ontario.
- Chen, H., Wen, Y., Zhu, M., Huang, Y., Xiao, C., Wei, T., & Hahn, A. (2021). From automation system to autonomous system: An architecture perspective. *Journal of Marine Science and Engineering*, 9(6), 645.

Çalışır, K. (2021). Tarihi Yapıların 3 Boyutlu Belgelenme Sürecinde Nokta Bulutu Yönteminin Rolü: Yaylak Ulu Camii Örneği. *Harran Üniversitesi Mühendislik Dergisi*, 6(3), 212-219.

Çelik, Y. (2017). Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı. *Türkiye Adalet Akademisi Dergisi*, (32), 391-410.

Ekiz, D. (2017). Bilimsel Araştırma Yöntemleri. Ankara: Anı Yayıncılık.

Ersoy, Ç. (2017). Robotlar, Yapay Zekâ ve Hukuk. Türkiye: On İki Levha Yayıncılık

Güleç, R., Benzer, R. (2020) Siber Güvenlikte Yapay Zekâ. *7.Uluslararası Yönetim Bilişim Sistemleri Konferansı*, (95).

İnternet: AB/2019/2144 Motorlu Araçlar ve Römorkları ile Bunlar İçin Tasarlanan Aksam, Sistem ve Ayrı Teknik Ünitelerin Genel Güvenliği ve Korunmasız Karayolu Kullanıcılarının ve Yolcuların Korunması ile İlgili Tıp Onayı Yönetmeliği. (n.d.). URL: <https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=34512&mevzuatTur=KurumVeKurulusYonetmeliği&mevzuatTertip=5>, Son Erişim Tarihi: 10.06.2023.

İnternet: Avrupa Parlamentosu ve Avrupa Birliği Konseyi. (2016, Nisan 27). Genel Veri Koruma Yönetmeliği (GDPR). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>, Son Erişim Tarihi: 06.03.2023.

İnternet: AYM, Ahmet Acartürk, B. No: 2013/2084, 15/10/2015, § 46. URL: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/2084>, Son Erişim Tarihi: 03.05.2023.

İnternet: Anayasa Mahkemesi'nin 18.05.2011 tarihli ve 2009/1 E., 2011/82 K. sayılı kararı. URL: <https://www.lexpera.com.tr/ictihat/anayasa-mahkemesi/genel-kurul-e-2009-1-k-2011-82-t-18-5-2011>, Son Erişim Tarihi: 11.02.2023.

İnternet: Guidelines 3/2019 on processing of personal data through video devices. | European Data Protection Board. Avrupa Veri Koruma Kurulu - Kişisel Verilerin Video Cihazları Aracılığıyla İşlenmesine İlişkin 3/2019 Sayılı Yönerge (2019, March 20). URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf, Son Erişim Tarihi: 12.04.2023.

İnternet: Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications. | European Data Protection Board. Avrupa Veri Koruma Kurulu - Bağlı araçlar ve mobilite ile ilgili uygulamalar bağlamında kişisel verilerin işlenmesine ilişkin 01/2020 sayılı Yönerge (Kılavuz İlkeler) (2021, March 9). URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_en, Son Erişim Tarihi: 10.03.2023.

İnternet: Işıl Yaykır, B. No: 2013/2284, 15/4/2014, § 37. URL: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/2284>, Son Erişim Tarihi: 11.02.2023.

İnternet: Jahromi, B. S. (2019, August 14). *Ultrasonic sensors in self-driving cars*. Medium. URL: <https://medium.com/@BabakShah/ultrasonic-sensors-in-self-driving-cars-d28b63be676f>, Son Erişim Tarihi: 20.02.2023.

İnternet: KVKK. (2016, Nisan 7). Türkiye Cumhuriyeti. URL: <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>, Son Erişim Tarihi: 12.09.2023.

İnternet: MEP, C. S., & Verhofstadt, G. (n.d.). MyCarMyData. URL: <https://mycarmydata.eu/#>, Son Erişim Tarihi: 02.04.2023.

İnternet: Mike Horton, C. (2019, February 14). *IMU technology forms the brains of the Autonomous Vehicle*. 5G Technology World. URL: <https://www.5gtechnologyworld.com/imu-technology-forms-the-brains-of-the-autonomous-vehicle/>, Son Erişim Tarihi: 12.07.2023.

İnternet: Saniuk-Heinig, C. (2021, June 17). 50 years and still kicking: An examination of fipps in modern regulation. 50 years and still kicking: An examination of FIPPs in modern regulation. URL: <https://iapp.org/news/a/50-years-and-still-kicking-an-examination-of-fipps-in-modern-regulation/>, Son Erişim Tarihi: 12.04.2023.

İnternet: T.C.İçişleri Bakanlığı Bilgi İşlem Dairesi Başkanlığı. (n.d.). Uyumlaştırılmış Araç içi acil çağrı Sistemi Projesi. 112 Acil Çağrı Merkezi. URL: <https://www.112.gov.tr/uyumlastirilmis-arac-ici-acil-cagri-sistemi-projesi>, Son Erişim Tarihi: 03.01.2023.

İnternet: Teschler, L. (n.d.-a). *Inertial measurement units will keep self-driving cars on track*. Microcontroller Tips. URL: <https://www.microcontrollertips.com/inertial-measurement-units-will-keep-self-driving-cars-on-track-faq/>, Son Erişim Tarihi: 23.05.2023.

İnternet: Treaty Office. (n.d.). <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108>, Son Erişim Tarihi: 18.06.2023

İnternet: Warren, S., Brandeis, L. (1890). The Right to Privacy, Harward Law Review, 4(5), 193-201, URL: http://www.jstor.org/stable/1321160?origin=JSTORpdf&seq=1#page_scan_tab_contents, Son Erişim Tarihi: 03.05.2023.

İnternet: Hopkins, D., Schwanen, T. (2021). Talking about automated vehicles: What do levels of automation do? URL: <https://doi.org/10.1016/j.techsoc.2020.101488>, Son Erişim Tarihi: 18.02.2024.

İnternet: 2017/78/AB 112 Acil Çağrı Servisi Tabanlı Araç İçi Acil Çağrı Sistemine İlişkin Motorlu Araçların Tip Onayına Yönelik İdari Hükümlerin Hazırlanması ve Bu Sistem Kullanıcıları İçin Gizlilik ve Veri Korumasına İlişkin Yönetmelik. Mevzuat Bilgi

- sistemi. (n.d.). URL: <https://www.mevzuat.gov.tr/anasayfa/MevzuatFihristDetayIframe?MevzuatTur=7∓MevzuatNo=24658∓MevzuatTertip=5>, Son Erişim Tarihi: 25.08.2023.
- İnternet: Oksijen, G. (2023). En yüksek kaza oranına sahip otomobil markası Tesla oldu. URL: <https://Gazeteoksijen.Com/Otomobil/En-Yuksek-Kaza-Oranina-Sahip-Otomobil-Markasi-Tesla-Oldu-197877>. <https://gazeteoksijen.com/otomobil/en-yuksek-kaza-oranina-sahip-otomobil-markasi-tesla-oldu-197877>, Son Erişim Tarihi: 20.02.2024.
- İnternet: National Highway Traffic Safety Administration (NHTSA) Preliminary Statement of Policy Concerning Automated Vehicles. (n.d.). URL: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/automated_vehicles_policy.pdf, Son Erişim Tarihi: 25.02.2024.
- İnternet: BAST - Special Subjects – Automotive Engineering - User communication. (n.d.). URL: https://www.bast.de/EN/Automotive_Engineering/Subjects/f4-user-communication.html?nn=1844934, Son Erişim Tarihi: 19.02.2024.
- İnternet: Civil Law Rules on Robotics - 16 Şubat 2017. (n.d.). URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html, Son Erişim Tarihi: 22.02.2024.
- İnternet: White Paper on Artificial Intelligence- A European approach to excellence and trust (n.d.). URL: https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf, Son Erişim Tarihi: 18.02.2024.
- İnternet: Impact Assessment of the Regulation on Artificial intelligence | Shaping Europe's digital future. (n.d.). URL: <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence>, Son Erişim Tarihi: 24.02.2024.
- İnternet: Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights-Consilium. (n.d.). URL: <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/>, Son Erişim Tarihi: 21.02.2024.
- İnternet: EPRS. (n.d.). Briefing EU Legislation in Progress. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf), Son Erişim Tarihi: 18.02.2024.
- İnternet: European AI Office, Shaping Europe's digital future. (n.d.). URL: <https://digital-strategy.ec.europa.eu/en/policies/ai-office>, Son Erişim Tarihi: 24.02.2024.
- İnternet: AI Pact, Shaping Europe's digital future. (n.d.). URL: <https://digital-strategy.ec.europa.eu/en/policies/ai-pact>, Son Erişim Tarihi: 19.02.2024.
- İnternet: OECD Legal Instruments. (n.d.). URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>, Son Erişim Tarihi: 20.02.2024.

- Internet: AI Act, Shaping Europe's digital future. (n.d.). URL: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>, Son Erişim Tarihi: 18.02.2024.
- Javed, M. W., Hussain, N., & Maitla, M. A. CCTV Cameras Surveillance, Data Protection & Privacy Under International Human Rights Laws. *Journal of Law & Social Studies (JLSS)*, 3(2), 174-186.)
- Kapancı, B. (2021). *Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ*. E. E. Aksoy Retornaz & O. G. Güçlütürk (Yay. haz.), Özel Hukuk Perspektifinden Bir Değerlendirme: Yapay Zekâ ve Haksız Fiil Sorumluluğu (s. 128-140). Türkiye: On İki Levha Yayıncılık, 137
- Karasar, N. (1999). Bilimsel Araştırma Yöntemi. Ankara: Nobel Yayın Dağıtım.
- Korkmaz, Y. (2020). Hasta Hakkı Olarak Özel Hayatın Korunması Bağlamında Beden Mahremiyeti. *Uyuşmazlık Mahkemesi Dergisi*, (15), 573-598.
- Merriam, S. B. (2015). *Nitel araştırma: Desen ve uygulama için bir rehber*. Nobel.
- Mishra, A., Cha, J., & Kim, S. (2022). Privacy-Preserved In-Cabin Monitoring System for Autonomous Vehicles. *Computational Intelligence and Neuroscience*, 2022.
- Mulder, T., & Vellinga, N. E. (2021). Exploring data protection challenges of automated driving. *Computer Law & Security Review*, 40, 105530.
- Pană, Laura & Cizmeci Ümit, Esra (2022). Yapay Zek' ve Ahlaki Zek'. *Ahlâk Journal* 2 (1):97-115.
- SAE International. (2014). Taxonomy of driving automation systems for on-road motor vehicles.
- Strauss, A., & Corbin, J. (1998). Basics of qualitative research techniques. Sage Publications, Inc.
- Üzeltürk S. (2004). 1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı
- Vakkuri, V., Kemell, K. K., Kultanen, J., & Abrahamsson, P. (2020). The Current State of Industrial Practice in Artificial Intelligence Ethics. *IEEE Software*, 37(4), 50-57
- Wach, E., & Ward, R. (2013). Learning about qualitative document analysis.
- Watson, D. P., & Scheidt, D. H. (2005). Autonomous systems. *Johns Hopkins APL technical digest*, 26(4), 368-376.
- Xie, C., Cao, Z., Long, Y., Yang, D., Zhao, D., & Li, B. (2022). Privacy of Autonomous Vehicles: Risks, Protection Methods, and Future Directions. arXiv preprint arXiv:2209.04022.

Xu, W., Yan, C., Jia, W., Ji, X., & Liu, J. (2018). Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. *IEEE Internet of Things Journal*, 5(6), 5015-5029.

Yüksel, S. (2012). Özel yaşamın bir parçası olarak telekomünikasyon yoluyla yapılan iletişimin gizliliğine önleyici denetimle müdahale. *İstanbul: Beta Yayınları*, 8





EK-1.Katılımcı Anket Formu

Değerli Katılımcı,

Bu anket *"Otonom Sistemlerin Gizlilik ve Kişisel Verilerin Korunması Çerçevesinde İncelenmesi"* başlıklı yüksek lisans tez çalışması için oluşturulmuştur. Anketi doldurmanızı ve görüşme sorularına yanıt vermenizi istiyoruz.

Katılımınız için teşekkür ederiz.

Av. Naz Nebile KARATAŞ

Gazi Üniversitesi Bilişim Enstitüsü

Adli Bilişim Yüksek Lisans Öğrencisi

Cinsiyet:

☐ Kadın ☐ Erkek

Eğitim Düzeyi:

☐ Lisans

☐ Yüksek lisans

☐ Doktora

☐ Diğer

Otonom araç tercih etme sebebiniz nedir?

☐ Yakıt tasarrufu

☐ Yüksek güvenlik

☐ Sürüş kolaylığı

☐ Trafik durumuna göre yol tarifi vermesi

☐ Diğer

"Bağlı araç" (connected car) teriminin ne demek olduğunu biliyor musunuz?

☐ Evet

☐ Hayır

Otonom aracınızı satın alırken size hangi konularda bilgilendirme yapıldı?

☐ Bilgilendirme yapılmadı

☐ Genel sürüş özellikleri

☐ Ana ekranda mevcut kısa yollar

☐ "Bağlı araç"(connected car) olmasından kaynaklı araçta mevcut özellikler

☐ Aracın kaydettiği verilerin neler olduğu

☐ Diğer

Otonom aracınızın kaydettiği verilerin kişisel veri olduğunu düşünüyor musunuz?

☐ Evet

☐ Hayır

Otonom aracınızda kaydedilen verilerin güvenli bir şekilde saklandığını düşünüyor musunuz?

☐ Evet

☐ Hayır

Otonom aracınızın veri kaydı özelliğini devre dışı bırakabiliyor olsaydınız bu özelliği kapatmak ister miydiniz?

☐ Evet, devre dışı bırakmak isterdim.

☐ Hayır, devre dışı bırakmak istemezdim.

Otonom aracınızın kaydettiği verilerin kimlerle paylaşıldığı konusunda bir izin verdiniz mi?

☐ Evet

☐ Hayır

Otonom aracınızın kaydettiği verilerin üçüncü taraflar ile paylaşılırken onayınızın alınmasını ister miydiniz?

☐ Evet

☐ Hayır

Otonom aracınızda kaydedilen veriler ile ilgili olarak hangilerini kontrol etmek isterdiniz?

☐ Ne kadar süre paylaşılacağını

☐ Üçüncü kişilerle yapılan paylaşımı

☐ Verdiğim izini istediğim zaman geri alabilmeyi

☐ Diğer

Otonom aracınızda kaydedilen veriler ile ilgili olarak sizi en çok hangileri endişelendirebilir

☐ Kişisel bilgilerimin ifşa olması

☐ Kişisel verilerimin ticari/reklam amacıyla kullanılması

☐ Araç korsanlığı (araçtaki verilerinize yetkisiz erişim)

☐ Araç konum takibi

☐ Diğer

Otonom aracınızın kaydettiği verilerden hangilerini paylaşırken rahat hissedersiniz?

☐ Araç arıza bilgileri

- ☐ Araca ait veriler (kilometre bilgisi, yağ-su-yakıt seviyeleri vb)
- ☐ Sürüş profili (hız bilgisi, fren kullanım alışkanlığı vb)
- ☐ Sürüş alışkanlıkları (ana ekran kısa yollarının kullanımı, koltuk oturma tercihleri vb)
- ☐ GPS Konum
- ☐ Eğlence tercihleri (müzik, film, oyun vb)
- ☐ "Bağlı araç" özelliklerinin kullanımı (sıklık, süre, konum, kişisel tercihler)
- ☐ Araç kamera kayıtları
- ☐ Sürücünün kimlik bilgileri
- ☐ Araca bağlanan telefon, tablet vb aletlerden alınan veriler (mesaj, email, telefon numaraları vb)
- ☐ Diğer

Aşağıdaki durumlardan hangisinde aracınızın kaydettiği verilerin paylaşılmasını kabul ederdiniz?

- ☐ Aracınız bozuldu ve yol yardım yetkilisi aracınızın konumuna ve bilgilerine ulaşmak istiyor
- ☐ Aracınızı bakım yaptırdığınız servis uzaktan aracınızın bilgilerine erişmek istiyor
- ☐ Sigorta şirketi aracınızın kilometre bilgisini öğrenerek sigorta primi teklifinde bulunmak istiyor
- ☐ Sigorta şirketi aracınızı kullanma alışkanlıklarınıza (hızlanma, frenleme vb) göre sigorta primi teklifinde bulunmak istiyor
- ☐ Aracınızı üreten firma, araç güncellemelerini otomatik olarak bildirebilmek için aracınızı izlemek istiyor
- ☐ Aracınız, telefonunuzdaki kişileri, epostaları, mesajları, arama geçmişinizi senkronize etmek istiyor
- ☐ Diğer

Aracınız bozulduğunda, araçta bulunan bir tuş ile yardım çağırma ve arızanız hakkında bilgi gönderebilme durumda verilerinizi paylaşmak ister misiniz?

- ☐ Evet
- ☐ Hayır

Yardım çağırma ve arızanız hakkında bilgi gönderebilme durumda verilerinizi paylaşacağınız yol yardım servisini kendiniz seçmek ister miydiniz?

- ☐ Evet
- ☐ Hayır

Otonom aracınızda kaydedilen veriler ile alakalı hukuki bir düzenleme olması gerektiğini düşünüyor musunuz?

- () Evet, hukuki bir düzenleme olmalı
() Hayır, hukuki düzenlemeye ihtiyaç yok

EK-2.Uzman Görüşme Formu Soruları

- 1) Otonom araçların güvenli olduğunu düşünüyor musunuz?
- 2) Otonom araçların kişisel verilerle ilgili problem teşkil edebileceğini düşünüyor musunuz?
Düşünüyor iseniz hangi açıdan problem çıkabilir?
- 3) Otonom araçlarda etik ile ilgili herhangi bir kodlama var mıdır?
- 4) Geliştirdiğiniz sistem dışarı ile veri paylaşıyor mu?
- 5) Otonom araçların ulusal güvenlik açısından risk taşıdığı söylenebilir mi?
- 6) Paylaşımlı araçları; uber, ride share vb. otonom araçlar açısından nasıl değerlendiriyorsunuz?
- 7) Otonom araçlarda kaydedilen verilere kimlerin erişimi olmalı?

EK-3.Etik Kurul Onayı



T.C.
GAZİ ÜNİVERSİTESİ REKTÖRLÜĞÜ
Etik Komisyonu

Sayı : E-77082166-302.08.01-639367
Konu : Bilimsel ve Eğitim Amaçlı

20.04.2023

Dağıtım Yerlerine

Üniversitemiz Bilişim Enstitüsü Adli Bilişim Ana Bilim Dalı **Yüksek Lisans Öğrencisi Naz Nebile KARATAŞ'ın, Doç. Dr. Hüseyin ÇAKIR'ın** danışmanlığında yürüttüğü **"Otonom Sistemlerin Gizlilik ve Kişisel Verilerin Korunması Çerçevesinde İncelenmesi"** adlı tez çalışması ile ilgili konu Komisyonumuzun **18.04.2023** tarih ve **08** sayılı toplantısında görüşülmüş olup,

İlgilinin çalışmasının, yapılması planlanan yerlerden izin alınması koşuluyla yapılmasında etik açıdan bir sakınca bulunmadığına oybirliği ile karar verilmiş ve karara ilişkin imza listesi ekte gönderilmiştir.

Bilgilerinizi rica ederim.

Araştırma Kod No: 2023 - 544

Prof. Dr. İsmail KARAKAYA
Komisyon Başkanı

Ek:1 Liste
DAĞITIM
Gereği:
Sayın Doç. Dr. Hüseyin ÇAKIR

Bilgi:
Bilişim Enstitüsü Müdürlüğüne

TOPLANTI TARİHİ : 18.04.2023		TOPLANTI SAYISI : 08	
ADI – SOYADI		İMZA	
Prof. Dr. İsmail KARAKAYA BAŞKAN			
Prof.Dr.Zehra GÖÇMEN BAYKARA BAŞKAN YRD.			
Prof.Dr.C.Haluk BODUR			
Prof.Dr.Seçil ÖZKAN			
Prof.Dr.Cevriye TEMEL GENCER			
Prof.Dr.İlkay ULUTAŞ			
Prof.Dr.Aymelek GÖNENÇ			
Prof.Dr.Kemalettin DENİZ			
Prof.Dr.Makbule GEZMEN KARADAĞ			
Prof.Dr.İlyas OKUR			
Prof.Dr.Nihan KAFA			
Doç.Dr.Melek Gülşah ŞAHİN			
Doç.Dr. Gökhan DELİCEOĞLU			
Doç.Dr.Elvan İNCE AKA			

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : KARATAŞ, Naz Nebile
Uyruğu : T.C.
Doğum tarihi ve yeri :
Medeni hali :
Telefon :
e-mail :

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Adli Bilişim	2024
Lisans	Gazi Üniversitesi / Hukuk Fakültesi	2017
Lise	Dr.Binnaz Dr.Rıdvan Ege Anadolu Lisesi	2013

İş Deneyimi

Yıl	Yer	Görev
12/2022 – Devam ediyor	Ankara Barosu Hukuk, Bilişim, İnovasyon ve Teknoloji Merkezi	Genel Sekreter
02/2020 – Devam ediyor	Su Hukuk ve Danışmanlık Ofisi	Kurucu Avukat
11/2022 – 12/2023	Ankara Barosu Mülteci Hakları Merkezi	Genel Sekreter
11/2017 – 12/2018	Recep Turna Hukuk ve Danışmanlık Ofisi	Stajyer Avukat
07/2017 – 09/2017	RWE Supply & Trading GmbH	Stajyer Avukat

Yabancı Dil

İngilizce, Almanca

Yayınlar

Çakır, H., Uluyol, Ç. (2022). *Yapay Zekâ Kuramdan Uygulamaya*, Türkiye: Nobel, 435-453

Çakır, H., Karataş N.N. (2023). 5. Uluslararası Ankara Multidisipliner Bilimsel Çalışmalar Kongresi, *Otonom Araçların Kişisel Verilerin Korunması Çerçevesinde İncelenmesi*, 594-605

Hobiler

Keman çalmak, Okçuluk





GAZİLİ OLMAK AYRICALIKTIR.