BİLGİ GÜVENLİĞİNİN YASAL DÜZENLEMELER KAPSAMINDA İNCELENMESİ: LOJİSTİK SEKTÖRÜNDE BİR ARAŞTIRMA

Ayşe İLAGA ÇAKIR
181157104

DOKTORA TEZİ

Uluslararası Ticaret ve Lojistik Anabilim Dalı
Lojistik ve Tedarik Zinciri Yönetimi Doktora Programı
Danışman: Prof. Dr. Mehmet TANYAŞ

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Eylül, 2024

BİLGİ GÜVENLİĞİNİN YASAL DÜZENLEMELER KAPSAMINDA İNCELENMESİ: LOJİSTİK SEKTÖRÜNDE BİR ARAŞTIRMA

Ayşe İLAGA ÇAKIR
181157104
ORCID: 0000-0003-1291-7564

DOKTORA TEZİ

Uluslararası Ticaret ve Lojistik Anabilim Dalı
Lojistik ve Tedarik Zinciri Yönetimi Doktora Programı
Danışman: Prof. Dr. Mehmet TANYAŞ

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Eylül, 2024



JÜRİ VE ENSTİTÜ ONAYI

AYŞE İLAGA ÇAKIR'ın "Bilgi Güvenliğinin Yasal Düzenlemeler Kapsamında İncelenmesi: Lojistik Sektöründe Bir Araştırma" başlıklı tezi 23.09.2024 tarihinde aşağıdaki jüri tarafından değerlendirilerek "Maltepe Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliği" nin ilgili maddeleri uyarınca Uluslararası Ticaret ve Lojistik Anabilim Dalı Yüksek Lisans/Doktora/Sanatta Yeterlik tezi oy birliğiyle/oy çokluğuyla, başarılı/başarısız olarak kabul edilmiştir.

	Unvanı. Adı ve Soyadı	İmza
Üye (Tez Danışmanı)	Prof.Dr.Mehmet TANYAŞ (Danışman) Maltepe Üniversitesi	.....
Üye	Prof.Dr.Şeref DEMİR Maltepe Üniversitesi	.....
Üye	Doç.Dr.Samet AYDIN Maltepe Üniversitesi	.....
Üye	Dr.Öğr.Üyesi Şafak Ümit DENİZ İstanbul Nişantaşı Üniversitesi	.....
Üye	Dr.Öğr.Üyesi Turkay ÖZDEMİR İstanbul Üniversitesi	.....

Enstitü Müdürü

ETİK İLKE VE KURALLARA UYUM BEYANI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" ile bildirilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

TEŞEKKÜR

Doktora çalışmamın her safhasında beni destekleyen, yol gösteren, cesaretlendiren ve her daim zaman ayırarak yardımlarını esirgemeyen değerli hocam ve tez danışmanım Sayın Prof. Dr. Mehmet Tanyaş hocama teşekkürü bir borç bilirim. Tez izleme komitemde bulunarak beni onurlandıran, komite toplantılarındaki görüş ve yorumları ile katkı ve destek sağlayan kıymetli hocalarım Prof. Dr. Şeref Demir ve Dr. Öğr. Üyesi Şafak Ümit Deniz'e çok teşekkür ederim. Tez savunma jürimde bulunmayı kabul ederek onurlandıran değerli hocalarım Doç. Dr. Samet Aydın ve Dr. Öğr. Üyesi Turkay Özdemir'e değerli katkılarından dolayı çok teşekkür ederim.

Tez çalışmam sırasında görüşlerine başvurduğum tüm sektör temsilcilerine ve doktora anketine katılan bütün katılımcılara teşekkür ederim.

Doktora çalışmam ailemin destek, sevgi ve sabrı olmadan tamamlanamazdı. Her daim desteklerini yanımda hissettiğim sevgili eşim Ümit'e ve canım kızım Duru'ya çok teşekkür ederim. Son olarak çalışmamı, hayatımın her döneminde yanımda olan ve şu an beni çok güzel bir yerden izlediklerine emin olduğum Rahmetli canım annem Neriman İlaga ve Rahmetli canım babam Adem İlaga'ya ithaf etmek istiyorum. Güzel ruhları şad olsun. Sevgi, saygı ve şükranlarımla…

Ayşe İLAGA ÇAKIR

Eylül, 2024

ÖZET

BİLGİ GÜVENLİĞİNİN YASAL DÜZENLEMELER KAPSAMINDA İNCELENMESİ: LOJİSTİK SEKTÖRÜNDE BİR ARAŞTIRMA

Ayşe İlaga Çakır
Doktora Tezi
Uluslararası Ticaret ve Lojistik Anabilim Dalı
Lojistik ve Tedarik Zinciri Yönetimi Doktora Programı
Danışman: Prof. Dr. Mehmet Tanyaş
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü,2024

Bilgi teknolojileri ile, verilerin dijital ortamlarda kayıt altına alınması kolaylaşmıştır. Ancak bu gelişme ile birlikte bilgiye izinsiz erişim ve kullanım riski artmıştır. Bu durum, ulusal güvenlik ve rekabet gücü gibi önemli konuları etkilemiş, devletler nezdinde ve ülkemizde çeşitli düzenlemeler yapılmıştır. Yasal düzenlemelere göre verilerin korunması bir zorunluluktur. Lojistik sektöründe çok sayı ve türde veri kaydı yapılmaktadır ve hizmetlerin kesintisiz devamı için doğru bilginin zamanında ve kesintisiz paylaşılması gereklidir.

Lojistik sektörüne ilişkin literatür çalışmalarında, bilgi güvenliğinin çok boyutlu bir disiplin olduğu belirtilerek hukuki boyutunun önemine vurgu yapılmıştır. Bilgi güvenliği politikaları konusunda da literatürde az sayıda bilimsel çalışmaya ulaşılmıştır. Önemine vurgu yapılmasına karşın, bilgi güvenliğini hukuki açıdan inceleyen bir çalışmaya rastlanılmamıştır. Literatürdeki bu eksiklik tez çalışması için temel motivasyonu oluşturmuştur. Çalışmada, bilgi güvenliği hukuki boyutu ile ele alınarak, yasal düzenlemeler çerçevesinde değerlendirilmek suretiyle literatüre katkı sağlanması hedeflenmiştir.

Araştırmada, bilgilerin korunması ile ilgili yasal düzenlemeler, yargı ve kurul kararları betimleyici tarama yöntemi ile incelenmiştir. Bilgi güvenliğine ilişkin uluslararası ISO 27001 Bilgi Güvenliği Yönetim Sistemi standartları, doküman analizi elde edilen veriler ile lojistik işletmelere uygulanan anket sonuçlarından yararlanılarak, lojistik işletmeleri için, öneri olarak bir model bilgi güvenliği politikası oluşturulmuştur. Diğer taraftan,

Türkiye Ulaştırma Politika Belgesi siber güvenliğin sağlanmasına yönelik düzenlemelerin lojistik sektörü için uygunluk ve yeterliliği değerlendirilmiştir.

Lojistik işletmelerin bilgi güvenliği uygulamalarının belirlenebilmesi için Türkiye genelinde anket yönteminden yararlanılmıştır. Lojistik firmalarının bilgi güvenliklerini tam ve yeterli seviyede sağlayamadıkları, hukuki düzenlemelerinin yeterli olmadığı, politikaları oluşturamadıkları ve risklere açık halde oldukları bulgusuna ulaşılmıştır.

Anahtar Sözcükler: Bilgi güvenliği, Bilgi güvenliği politikaları, ISO 27001 Bilgi Güvenliği Yönetim Sistemi, Kişisel Verilerin Korunması Kanunu, Lojistik, Yargıtay ve Kurul kararları, Yasal düzenlemeler.

ABSTRACT

EXAMINATION OF INFORMATION SECURITY WITHIN THE SCOPE OF LEGAL REGULATIONS: A RESEARCH IN THE LOGISTICS SECTOR

Ayşe İlaga Çakır
PhD Thesis
Department of International Trade and Logistics Management
Logistics and Supply Chain Management Doctorate Program
Thesis Advisor: Prof. Dr. Mehmet Tanyaş
Maltepe University Graduate School, 2024

With advancements in information technologies, the recording of data in digital environments has become easier. However, this development has also increased the risk of unauthorized access and use of information. This situation has impacted critical issues such as national security and competitive power, leading to various regulations at both national and international levels. According to legal regulations, the protection of data is mandatory. In the logistics sector, numerous types and volumes of data are recorded, and to ensure uninterrupted service, the timely and seamless sharing of accurate information is essential.

Literature studies of the logistics sector emphasize that information security is a multidisciplinary field, with particular attention given to its legal dimension. However, there are limited scientific studies on information security policies. Despite the emphasis on its importance, no study examining information security from a legal perspective has been encountered. This gap in the literature has formed the primary motivation for this thesis. The study aims to contribute to the literature by examining information security from a legal perspective and evaluating it within the framework of legal regulations.

In this research, legal regulations, judicial decisions, and board rulings related to the protection of information were examined using a descriptive research method. A model information security policy has been developed as a recommendation for logistics companies by utilizing the international ISO 27001 Information Security Management System standards, document analysis, and survey results obtained from logistics

companies. In addition, the compliance and adequacy of the regulations outlined in Turkey's Transport Policy Document for ensuring cybersecurity in the logistics sector were evaluated.

A survey method was employed across Turkey to determine the information security practices of logistics companies. The findings revealed that logistics companies were unable to fully and adequately ensure their information security, that legal regulations were insufficient, that they failed to establish proper policies, and that they remained exposed to risks.

Keywords: Information security, Information security policies, ISO 27001 Information Security Management System, Legal regulations, Logistics, Personal Data Protection Law, Supreme Court and Board decisions.

İÇİNDEKİLER

JÜRİ VE ENSTİTÜ ONAYI ii
ETİK İLKE VE KURALLARA UYUM BEYANI iii
TEŞEKKÜR iv
ÖZET v
ABSTRACT vii
İÇİNDEKİLER ix
TABLOLAR LİSTESİ xv
ŞEKİLLER LİSTESİ xx
KISALTMALAR xxii
SEMBOLLER xxiv
1. GİRİŞ 1
1.1 Problem 1
1.2 Literatür Araştırması 5
1.3 Amaç 27
1.4 Önem 30
1.5 Varsayımlar 36
1.6 Sınırlılıklar 36
1.7 Tanımlar 38
2. GENEL BİLGİLER 40
2.1 Veri, Enformasyon ve Bilgi 40
2.2 Bilgi Güvenliği 40
2.3 Tedarik Zinciri, Lojistik ve Lojistik Bilgi Sistemleri 41
2.3.1 Tedarik zinciri ve lojistik 41

2.3.2 Lojistikte doğru bilginin önemi ve dijitalleşme 43
2.3.3 Lojistikte bilgi paylaşımı ve bilişim sistemleri 46
2.3.4 Risk ve lojistikte bilgi güvenliği 49
2.4 Hukukumuzda Kişiler ve Veriler 51
2.4.1 Gerçek ve tüzel kişi 51
2.4.2 Veri 52
2.4.2.1 Kişisel veriler 52
2.4.2.2 Tüzel kişi verileri 53
2.4.2.2.1 Ticari sır 55
2.4.2.2.2 Müşteri verileri 57
2.4.2.2.3 Kişisel veriler 58
2.4.2.2.4 Diğer veriler 58
2.5 Yasal Düzenlemeler 58
2.5.1 Kişisel verilerin korunmasına ilişkin yasal düzenlemeler 58
2.5.1.1 Ulusal düzenlemeler 58
2.5.1.1.1 1982 Anayasası 59
2.5.1.1.2 6698 Sayılı Kişisel Verilerin Korunması Kanunu 60
2.5.1.1.3 5237 Sayılı Türk Ceza Kanunu 76
2.5.1.1.4 4721 Sayılı Türk Medeni Kanunu 77
2.5.1.1.5 6098 Sayılı Türk Borçlar Kanunu 78
2.5.1.1.6 Diğer ulusal düzenlemeler 79
2.5.1.2 Uluslararası düzenlemeler 79
2.5.1.2.1 Avrupa Konseyi düzenlemeleri 80
2.5.1.2.2 Avrupa Birliği düzenlemeleri 82
2.5.1.2.3 Diğer uluslararası düzenlemeler 84

2.5.1.3 Kişisel Verilerin Korunması Kanunu ve Genel Veri Koruma Tüzüğü (GDPR) değerlendirme 85

2.5.2 Tüzel kişi verilerinin korunmasına ilişkin yasal düzenlemeler 89

2.5.2.1 Ulusal düzenlemeler 89

2.5.2.1.1 1982 Anayasası 89
2.5.2.1.2 4721 Sayılı Türk Medeni Kanunu 90
2.5.2.1.3 6102 Sayılı Türk Ticaret Kanunu 90
2.5.2.1.4 5237 Sayılı Türk Ceza Kanunu 96
2.5.2.1.5 6098 Sayılı Türk Borçlar Kanunu 98
2.5.2.1.6 6698 Sayılı Kişisel Verilerin Korunması Kanunu 101
2.5.2.1.7 Diğer ulusal düzenlemeler 101
2.5.2.2 Uluslararası düzenlemelerde ticari sırların korunması 104

2.5.3 Uluslararası sözleşmeler ve özel tedbirler 106

2.5.4 Avrupa Birliği Siber Güvenlik Kanunu 107

2.6 Bilgi Güvenliği 107

2.6.1 Bilgi güvenliği ve standardları 107

2.6.1.1 ISO/IEC 27001 Bilgi güvenliği standardı ve tarihçesi 111

2.6.1.2 ISO/IEC 27001 Bilgi Güvenliği standardı kapsamı, PUKÖ ile ilişkisi ve kanunlara uyum 117

2.6.1.3 ISO/IEC 27001 Bilgi Güvenliği standardı ve Kişisel Verilerin Korunması Kanunu 120

2.7 Veri İhlalleri 126

2.7.1 Siber saldırılar 127

2.7.2 Veri ihlaline ilişkin araştırmalar 128

2.8 Türkiye Ulaştırma Politika Belgesi, Ulaştırma ve Haberleşme Şurası 132

3. YARGI VE KURUL KARARLARI 134
3.1 Kişisel Verileri Koruma Kurulu Kararları 134
3.2 Yargıtay Kararları 142
3.3 Adli Karar İstatistikleri 149
4. YÖNTEM 154
4.1 Araştırma Modeli 154
4.2 Evren ve Örneklem 155
4.3 Veri Türleri 156
4.3.1 Kişisel veriler ile ilgili araştırma 158
4.3.2 Tüzel kişi verileri ile ilgili araştırma 159
4.4 Araştırma Hipotezlerinin Oluşturulması 165
4.5 Veriler ve Toplanması 166
4.5.1 Anket ve bulgular 166
4.5.1.1 Demografik özelliklere ait bulgular 169
4.5.1.2 Veriler bölümüne ilişkin bulgular 172
4.5.1.3 Bilgi güvenliği yönetim sistemine ilişkin bulgular 177
4.5.1.4 Veri ihlaline ilişkin bulgular 183
4.5.1.5 Bilgi güvenliğine ilişkin tedbir ve yükümlülüklere ait bulgular 187
5. BULGULAR VE TARTIŞMA 198
5.1 Bilgi Güvenliği ve Risk Yönetimi 198
5.1.1 Lojistik şirketlerinde veri güvenliği ve risk yönetimine bakış 199
5.2 Lojistik Şirketlerinde Veri Güvenliği Farkındalık ve Uygulamalar 201
5.3 Bilgi Güvenliğini Sağlamak Üzere Alınan Teknik, Hukuki ve İdari Tedbirler 205

5.3.1 Veri ihlaline yönelik tedbirler 208
5.3.2 Üçüncü kişilerden kaynaklanan ihlallere yönelik tedbirler 210
5.3.3 Personel kaynaklı veri ihlalleri 212
5.3.4 Bilgi güvenliği ve mali durum açısından değerlendirilmesi 216
5.4 Araştırma Hipotezi Bulguları ve Çözümlenmesi 218
5.4.1 Araştırma hipotezi bulguları 219
6. BİLGİ GÜVENLİĞİ POLİTİKA ÖNERİSİ 228
6.1 Amaç 228
6.2 Kapsam 229
6.3 Tanımlar ve Kısaltmalar 229
6.4 Bilgi Güvenliği Organizasyon Yapısı 232
6.5 Yetki ve Sorumluluklar 232
6.5.1 Şirket üst yönetim kademesinin yetki ve sorumlulukları 232
6.5.2 Bilgi güvenliği komisyonunun yetki ve yükümlülükleri 234
6.5.3 Şirket personeli ve diğer üçüncü kişilerin yükümlülükleri 238
6.6 Bilgi Güvenliği Risk Yönetimi 240
6.6.1 Risk yönetim sürecinde öncelikli yapılması gerekenler 240
6.6.2 Risk yönetimi kapsamında uygulanacak genel unsurlar 241
6.7 Bilgi Güvenliği Önlemleri 242
6.7.1 Fiziksel güvenlik önlemleri 242
6.7.2 Teknik kontroller 243
6.8 Hukuki Düzenlemeler ile Verilerin Korunması 246
6.8.1 Hukuki ve idari güvenlik önlemleri 246

6.9 Diğer Hususlar 251
7. SONUÇ VE ÖNERİLER 253
KAYNAKÇA 269
EKLER 305
Ek:1: Anket Formu 305
Ek:2: Etik Kurul Kararı 312
ÖZGEÇMİŞ 313

TABLOLAR LİSTESİ

Tablo 1. Siber Güvenlik İhlalleri Araştırması 4

Tablo 2. Literatür Araştırmasına Dahil Etme-Hariç Tutma Kriterleri 5

Tablo 3. Literatür Araştırması 6

Tablo 4. İnceleme Konuları ve Yöntemler 13

Tablo 5. Ayrıntılı Literatür İncelemesi 14

Tablo 6. Güncel Literatürün Kapsamlı Analizi 21

Tablo 7. Saldırı Gelen Ülkeler ve Saldırı Sayıları 33

Tablo 8. Dijital Dönüşüm ile Siber Güvenlik Harcamalarının Yüzdesel Oranları 46

Tablo 9. Kişisel Verilerin Korunması ile İlgili Ulusal Yasal Düzenlemeler 59

Tablo 10. Türk Ceza Kanunu Hürriyeti Bağlayıcı Cezalar 69

Tablo 11. İdari Para Cezaları 2024 Oranları 69

Tablo 12. Bilişim Suçları Düzenlemesi…….. 77

Tablo 13. Kişisel Verilerin Korunması ile İlgili Uluslararası Yasal Düzenlemeler 80

Tablo 14. ISO/IEC 27001:2022 BGYS Standardı Ana Maddeleri 118

Tablo 15.ISO/IEC 27001:2022 BGYS Standart Maddeleri ve PUKÖ Döngüsü İlişkisi 119

Tablo 16. ISO/27001:2013 BGYS Ek-A Maddeleri 121

Tablo 17. Kişisel Verilerin Korunması Kanunu İdari Tedbirler 123

Tablo 18.Kişisel Verilerin Korunması Kanunu Teknik Tedbirler 123

Tablo 19. KVKK ve ISO 27001:2013 BGYS Standardı Karşılaştırması 124

Tablo 20. TCK 'ya Göre Bilişim Suçları ile İlgili Olarak Şüpheli Kişiler Hakkında Verilen Kararlar 149

Tablo 21. TCK 'ya Göre Özel Hayatın Gizliliğine Karşı Suçlar ile İlgili Olarak Şüpheli Kişiler Hakkında Verilen Kararlar 150

Tablo 22. TCK 'ya Göre Ekonomi, Sanayi ve Ticarete İlişkin Suçlardan 239. Madde İle İlgili Olarak Şüpheli Kişiler Hakkında Verilen Kararlar 151

Tablo 23. TCK Uyarınca Bilişim Suçları ile İlgili Olarak Davalarda Verilen Kararlar ve Oranları 152

Tablo 24. TCK Uyarınca Özel Hayatın Gizliliğine Karşı Suçlar ile İlgili Olarak Davalarda Verilen Kararlar ve Oranları 152

Tablo 25. TCK Uyarınca Ekonomi, Sanayi ve Ticarete İlişkin Suçlardan 239. Madde İle İlgili Olarak Davalarda Verilen Kararlar 153

Tablo 26. Kişisel Veri Türleri 158

Tablo 27. Kişisel Veri Konusu Kişi Grupları 159

Tablo 28.Ticari Sır Örnekleri 164

Tablo 29. İşletmelerin Demografik Özellikleri 169

Tablo 30. Şirketin Kayıt Altına Aldığı Veri Türleri 172

Tablo 31. Kişisel Veriler ile Tüzel Kişi Verileri Hakkında Bilgi 172

Tablo 32. Kişisel ve Tüzel Kişi Verilerinin Muhafaza Ortamı 173

Tablo 33.Şirketin Veri Envanteri 173

Tablo 34. Şirket Verilerinin Risk ve Önemine Göre Gruplandırılması 174

Tablo 35. Şirket Verilerinin İhlalinde Zarar Çalışması 174

Tablo 36. Şirket Verilerinin Kayıt Altına Alınması 174

Tablo 37. Şirketin Kayıt Altına Aldığı Veri Türleri 175

Tablo 38. Mobil Ağa Bağlı Cihaz Veri Envanteri 176

Tablo 39. ISO 27001 BGYS Hakkında Bilgi Durumu 177

Tablo 40. Şirketin ISO 27001 BGYS Belgesine Sahip Olma Durumu..... 177

Tablo 41. Bilgi Güvenliğine İlişkin Yıllık Gider 178

Tablo 42. Bilgi Güvenliği Kurul/Komisyon Varlığı ve Kurulu Oluşturan Birimler.... 179

Tablo 43. Personele Bilgi Güvenliğine İlişkin Eğitim Verilme Durumu..... 179

Tablo 44. ISO 27001 BGYS'nin Şirkete Olumlu Etkileri 180

Tablo 45. Verilerin İşlenmesi, Saklanması Prosedür ve Politika Varlığı ile Denetim Durumu 181

Tablo 46. Şirketin Bilgi Güvenliğine Yatırım Yapma Nedenleri 182

Tablo 47. Veri İhlali Hakkında Bilgi ve Veri İhlali Yaşanması 183

Tablo 48. Veri İhlali Sebepleri 183

Tablo 49. Personele Uygulanacak Disiplin Süreci, Tedarikçilere Uygulanacak Politikalar ve Veri İhlalinde İzlenecek Süreç-Eylem Planı Düzenlemeleri 185

Tablo 50. Olası Veri İhlallerinin Zamanında Tespit Edilmesine İlişkin Prosedürlerin Varlığı 186

Tablo 51. Veri İhlalinin Şirkete Etkisi 186

Tablo 52. Şirket Verilerinin Korunmasından Yasal Sorumluluk Durumu 187

Tablo 53. Şirket Verilerinin Korunması İçin Alınan Önlemler 188

Tablo 54. Verilerin Korunması İçin Teknik Donanım ve Güvenlik Testlerinin Yapılması Durumu 189

Tablo 55. Verilerin Korunmasına İlişkin Düzenlemeler, Sorumlulukların Paylaşılması 190

Tablo 56. Bilgi Güvenliği İçin Şirket Üst Yönetiminin Desteği 191

Tablo 57. Yurt Dışına Kişisel Veri Aktarımına İlişkin Düzenlemelerin Varlığı 192

Tablo 58. Veri Paylaşılan İş Ortaklarının ISO 27001 BGYS Sahip Olmasının Önemi 192

Tablo 59. "Personel Sözleşmeleri" ve "İş Ortakları İle Yapılan Sözleşmelerde" Bilgi Güvenliği Düzenlemelerine Yer Verilme Durumu 193

Tablo 60. Verilere Erişim Yetkisi Bulunan Personelin Görev Değişikliğinde Yapılacak İşlem Durumu 194

Tablo 61. Verilerin Korunmasında İdari ve Hukuki Düzenlemeler ve Politika Uygulanmalarının Denetlenmesi, Teknik Destek Hizmet Alma Durumu 195

Tablo 62. "Tüzel Kişi Veriler" ile İlgili Sorumluluğa İlişkin Yasal Düzenlemeler..... 196

Tablo 63. "Kişisel Verilerin" İhlalinde Uygulanması Gereken Prosedür Durumu..... 197

Tablo 64. Risk Yönetimine İlişkin Sonuçlar 200

Tablo 65. ISO 27001 BGYS Hakkında Bilgi Sahibi Olunmasına İlişkin Sonuçlar..... 202

Tablo 66. Bilgi Güvenliği Politikalar, Eğitim ve Kurul/Komisyon Varlığına İlişkin Sonuçlar 204

Tablo 67. Bilgi Güvenliğine İlişkin Şirket Üst Yönetiminin Desteğine Dair Sonuçlar205

Tablo 68. Bilgi Güvenliğinin Sağlanmasına Yönelik Tedbirlere İlişkin Sonuçlar 206

Tablo 69.Veri İhlaline İlişkin Hukuki ve İdari Tedbirler 208

Tablo 70. Hukuki ve İdari Tedbirler 210

Tablo 71. Veri İhlali Sebeplerine İlişkin Bulgular..... 213

Tablo 72.Personel Kaynaklı İhlallere Karşı Disiplin Süreci Belirleme Durumu..... 213

Tablo 73. Bilgisayarlara Erişebilecek Yetkili Kişilerin Belirlenme Oranı 215

Tablo 74. Son Mali Yıla Ait Yıllık Gelir ile Bilgi Güvenliğine İlişkin Yıllık Gider İlişkisi 217

Tablo 75. Şirket Mali Durumları ile ISO 27001 Belgesi Sahibi Olma Durumu İlişkisi 219

Tablo 76. ISO 27001 Belgesi Sahibi Firma ile Tedarikçide ISO 27001 Belgesi Olmasının Önemi..... 220

Tablo 77. Bilgi Güvenliği Eğitimi ile Veri İhlali Hakkında Bilgi Sahibi Olma İlişkisi 221

Tablo 78. Bilgi Güvenliği Yıllık Giderleri ile Veri İhlalinin Şirkete Etkisi 222

Tablo 79. Son Mali Yıla Ait Yıllık Gelir ile Bilgi Güvenliğine Dair Yıllık Gider İlişkisi 223

Tablo 80. Verilerin Korunmasından Yasal Olarak Sorumlu Olduğunu Düşünme ile Şirket Verilerinin Korunması İçin Alınan Önlemler Arasındaki İlişkinin İncelenmesi..... 224

Tablo 81. Verilerin Korunmasından Yasal Olarak Sorumlu Olduğunu Düşünme ile Bilgi Güvenliğine Dair Yıllık Gider Arasındaki İlişkinin İncelenmesi 225

Tablo 82. Bilgi Güvenliğinden Sorumlu Bir Kurul/Komisyon/Birim Bulunması ile Verilerin İşlenmesi, Saklanması, Korunması ve İmhası Konusunda Prosedür ve Politikalar Belirlenmesi Arasındaki İlişkinin İncelenmesi 226

Tablo 83. Şirket Çalışanlarına Veriler ve Bilgi Güvenliğine İlişkin Eğitim Verilmesi ile Şirket Çalışanlarının İş Sözleşmelerinde, Bilgi Güvenliği Hükümlerine Yer Verilmesi Arasındaki İlişki..... 227

ŞEKİLLER LİSTESİ

Şekil 1. Yıllara Göre Yapılan Akademik Araştırmalar 13

Şekil 2. Tedarik Zinciri ve Lojistik İlişkisi 42

Şekil 3. Temel Lojistik Faaliyetler 43

Şekil 4. Lojistikte Malzeme, Hizmet ve Bilgi Akışı..... 44

Şekil 5. Dijital dönüşüm ve güvenlik harcamaları 2020 – 2024 tahmini 45

Şekil 6. Lojistik Fonksiyonlarda Bilgi Akışı 47

Şekil 7. Lojistik Bilişim Sistemi Bileşenleri 48

Şekil 8. PUKÖ Döngüsü ve BGYS nin Çalışması 118

Şekil 9. ISO/27001:2013 Ek-A ve Değişen ISO/IEC 27001:2022 Ek-A Kontrol Maddeleri 122

Şekil 10. ENISA Saldırı Ortamı 128

Şekil 11. Lojistik İş Süreçleri 160

Şekil 12. Nakliye Yönetim Modülü Sevkiyatlar 162

Şekil 13. Sipariş Modülü 162

Şekil 14. Stok ve Depo Modülü..... 163

Şekil 15.Şirketlerin Sunduğu Lojistik Hizmetler 171

Şekil 16. Şirket Verilerinin Kayıt Altına Alınma Şekline Göre Dağılımı..... 175

Şekil 17. Kayıt Altına Alınan Veri Türleri 176

Şekil 18. Veri İhlal Kaynakları..... 184

Şekil 19. Verilerin Korunması İçin Alınan Önlemler..... 188

Şekil 20. Tüzel Kişi Verileri İle İlgili Sorumluluğa İlişkin Yasal Düzenleme..... 197

Şekil 21. Araştırmaya Dahil Olan Şirketlerin Büyüklüğüne Göre Dağılımları..... 202

Şekil 22. Verilerin Kayıt Edildiği Ortamlara İlişkin Bulgular 214

Şekil 23. Verilerin Korunduğu "Fiziki Ortamların" Güvenliğinden Sorumlu Olanların Belirlenmesi 214

Şekil 24.Şirket Büyüklüğü..... 216

KISALTMALAR

AB **:** Avrupa Birliği

BG : Bilgi Güvenliği

BGYS **:** Bilgi Güvenliği Yönetim Sistemi

CD **:** Ceza Dairesi

DTÖ **:** Dünya Ticaret Örgütü

ENISA **:** Avrupa Ağ ve Bilgi Güvenliği Ajansı

FSEK **:** Fikir ve Sanat Eserleri Kanunu

GDPR **:** Avrupa Birliği Genel Veri Koruma Tüzüğü

HD **:** Hukuk Dairesi

IEC **:** Uluslarası Elektroteknik Komisyonu

ISO **:** Uluslararası Standardizasyon Kuruluşu

KOBİ **:** Küçük ve Orta Ölçekli İşletme

KVKK **:** Kişisel Verilerin Korunması Kanunu

KVYS **:** Kişisel Veri Yönetim Sistemi

OECD **:** Uluslararası Çalışma Örgütü

PUKÖ **:** Planla, Uygula, Kontrol Et, Önlem Al

SOME **:** Siber Olaylara Müdahale Ekipleri

SPSS 25.0 **:** Sosyal Bilimler İçin İstatistik Programı

TBMM : Türkiye Büyük Millet Meclisi

T.C. : Türkiye Cumhuriyeti

TCK : Türk Ceza Kanunu

TIO : Taşıma İşleri Organizatörlüğü

TRIPS : Ticaretle Bağlantılı Fikri Mülkiyet Anlaşması

TSE : Türk Standartları Enstitüsü

TZ : Tedarik Zinciri

USOM : Ulusal Siber Olaylara Müdahale Merkezi

VERBİS : Veri Sorumluları Sicili

YLDA : Yurt Dışı Lojistik Dağıtım Ağları Projesi

SEMBOLLER

N **:** Evrendeki birey sayısı

n **:** Örnekleme alınacak birey sayısı

p **:** İncelenen olayın görülüş sıklığı(olasılığı)

q **:** İncelenen olayın görülmeyiş sıklığı(1-p)

t **:** Belirli serbestlik derecesinde ve saptanan yanılma düzeyinde t tablosunda bulunan teorik değer

d **:** Olayın görülüş sıklığına göre yapılmak istenen sapma

1. GİRİŞ

1.1 Problem

Günlük hayatımızda önemli bir yeri olan bilgisayar gibi elektronik cihazların kullanımı, internet teknolojisinin etkisiyle artmış ve bu durum, bilgiye erişimi daha da kolay hale getirmiştir.

Teknolojideki ilerlemeler, daha fazla bilginin depolanması ile taşınmasına olanak sağlayabilecek duruma gelmiştir. Diğer taraftan da bilginin yoğun olarak kullanılması ve paylaşımı çeşitli güvenlik risklerine de sebep olmaktadır. Bu durum, veri güvenliği ihlalleri, kişisel bilgi hırsızlıkları, kötü amaçlı yazılımların yayılması gibi potansiyel sorunlara yol açabilmektedir (Şahinaslan, Borandağ, Şahinaslan ve Kantürk, 2009).

Bilgi, büyük değere sahiptir ve kuruluşların can damarıdır. Finansal bilgiler, ticari sırlar, fikri mülkiyet, müşteri bilgileri ile personel bilgileri bu kapsamdadır (Tankard, 2015). Fiziki ortamda yapılabilen veri kayıtlarının teknolojideki gelişmeler ile birlikte dijital ortamda da işlenmeye başlaması ile veriye izinsiz erişim ve izinsiz kullanım risk seviyesi artmıştır. Ekonomik değeri olan verilerin, izinsiz bir şekilde üçüncü kişiler tarafından elde edilmesi de kolaylaşmıştır.

Öyle ki bu durum, ulusal güvenlik ve rekabet edebilme gücü bakımından önem kazanan bir mesele haline gelmiştir. Bu sebepledir ki, Ulaştırma Denizcilik ve Haberleşme Bakanlığı nezdinde 2013-2014, 2016-2019 tarihli ve Ulaştırma ve Altyapı Bakanlığı nezdinde 2020-2023 tarihli Ulusal Siber Güvenlik Stratejisi ve Eylem Planları hazırlanmıştır. Hazırlanan eylem planları, kamuya ait bilişim sistemleri ile özel sektör veya kamu tarafından yönetilen stratejik altyapıların bilgi teknolojisi sistemlerine ek olarak, küçük ve orta ölçekli sanayi ile tüm özel ve tüzel kişileri kapsayacak şekilde, ülkemizin ulusal siber uzayındaki tüm unsurları içine almaktadır. Eylem planlarında, "*Paydaşların güvenlik risklerini bilmeleri(...)farkındalık ve yetkinliğin sağlanması için eğitimlerin yapılması gerektiği"* önemle belirtilmiştir (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, s. 9,10,11).

Veri sorumluları, işlenen verilerin yetkisiz kişilerin izinsiz kullanımına karşı korunmasını sağlamak ister. Tüzel kişi şirketler de, bilgi varlıklarının korunmasına ihtiyaç duyar. Bu durum veri sorumluları için hem bir ihtiyaç hem de yasal bir zorunluluktur. Keza, verilere izinsiz erişim, izinsiz kullanım, izinsiz paylaşım konusunda mahkemelere intikal etmiş ihtilaflar bulunmaktadır. Ayrıca bilgi varlıklarının, şirket dışından ve şirket içerisinden gelebilecek saldırılara karşı korunması, işletmeler için, hem maddi hem de manevi kayıplara uğramasının (ticari itibarın zedelenmesi, rekabet edememe, güvenilirliğin zedelenmesi, ticari kayıpları gibi) önlenebilmesi açısından da oldukça önemlidir.

2016-2019 Ulusal Siber Güvenlik Stratejisi Eylem Planı'nda; "*İşletmelerin ticari sırlarını ve bilgi birikimini elde etmeye yönelik hedef odaklı saldırılar sonucunda…bilişim sistemlerindeki güvenlik önlemlerinin eksikliğinden veya kullanıcı hatalarından dolayı kesintiye uğraması, hassas veya ticari değere sahip bilgilerin ele geçirilerek, ifşa edilmesi, değiştirilmesi veya yok edilmesi"* güvenlik riskleri arasında sayılmıştır. Bu riskler sebebiyle de, *"İşletmelerin bilgi güvenliklerini hem saldırganlara karşı, hem de kullanıcı hatalarına karşı korumak için düzenlemelerin yapılması(…)kurum yöneticilerinin farkındalıklarının arttırılması, yetkin personel yetiştirilmesi(…)her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ulaşması"* gerekliliği ifade edilmiştir (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, s. 12-13).

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda;

> Kurumlarda veri güvenliği bilincinin sağlanması…veri güvenliği standartları uygulanmalarının genişletilmesi…üniversitelerde veri ve siber güvenlik programlarının arttırılması… ulaştırma gibi kritik altyapı sektörlerinin güvenli bir dijital ortamda hizmet vermesi gerekliliği(…)dijital dönüşümün etkili ve devam edilebilir olması için dijital güvenliğin çok büyük bir önemi olduğu(…).sağlam yasal zeminler üzerine güçlü bir siber güvenlik altyapısının oluşturulması gerekliliği" ifade edilmiştir (T.C. Ulaştırma ve Altyapı Bakanlığı, 2020a, s. 12,18-19,21,23-24).

İşletmelerin ticari sırlarını korumak için, teknik ve hukuki önlemler alma zorunluluğu bulunmaktadır. Türk Ticaret Kanunu madde 18/2'ye göre, her tacirin, ticari

faaliyetlerinde basiretli bir iş insanı gibi hareket etme sorumluluğu bulunmaktadır. Bu doğrultuda, işletme sahibi yöneticilerin de ticari sırlarını koruması, gerekli tedbirleri alması ve bu konuda dikkatli ve özenli davranması gereklidir (Yüksel, 2018).

Şirketler ayrıca çeşitli tür ve sayıda kişisel veri işlemektedir. 29677 sayı ve 7 Nisan 2016 tarihli Resmi Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun olarak, şirketlerin bu kişisel verileri koruma yükümlülüğü bulunmaktadır. Kişisel verilerin kaydedilmesi, işlenmesi ve saklanması süreçlerinde gerekli güvenlik önlemleri alınmalıdır. Aksi takdirde kanunun 18. maddesi gereğince idari ve 17. maddesi gereğince de cezai yaptırımlarla karşılaşma riski bulunmaktadır.

Tablo 1'de gösterilen Siber Güvenlik İhlalleri Araştırması (Cyber Security Breaches Survey) değişik tarihli anket sonuçlarına göre, her ölçekten firma, verilerinin izinsiz ele geçirilmesi saldırısı ile karşı karşıyadır. Maruz kalınan saldırı yöntemleri çeşitlendiği gibi, büyük ekonomik zararlara sebep olan saldırıların, yıllar içerisinde arttığı görülmektedir. Her geçen gün artan siber riskler karşısında, ulusal eylem planlarında da belirtildiği üzere, işletmelerin verilerini koruyabilmek için bilgi güvenliği önlemlerini alması oldukça önemlidir.

Tablo 1. Siber Güvenlik İhlalleri Araştırması (Yıldırım, 2018) (Gov.uk, 2021) (Gov.uk, 2022) (Gov.uk, 2023)

Cyber Security Breaches Survey 2016 yılı raporuna göre	**Cyber Security Breaches Survey 2021 yılı raporuna göre**	**Cyber Security Breaches Survey 2022 yılı raporuna göre**	**Cyber Security Breaches Survey 2023 yılı raporuna göre**
2015 yılında büyük şirketlerin %65'i siber güvenlik ihlal ve saldırıları ile karşılaşmıştır.	2020 yılında orta ölçekli firmaların % 65'i ve büyük işletmelerin de % 64'i Siber ihlal ve saldırılarılar ile karşılaşmıştır.	Son 12 ayda, Büyük işletmelerin de % 72'si, orta ölçekli işletmelerin %59, küçük ve mikro ölçekli işletmelerin % 84 siber saldırılar ile karşılaşmıştır.	Son 12 ayda orta ölçekli işletmelerin %59'u, büyük işletmelerin % 69'u, küçük işletmelerin %32'si ve mikro işletmelerin %31'i siber saldırılar ile karşılaşmıştır.
Bu işletmelerin %25'i ayda en az bir defa ihlal olayı ile karşılaşmıştır.	Bu işletmelerin %27'si her hafta en az bir defa ihlal olayı ile karşılaşmıştır.	İşletmelerin %31'i her hafta en az bir defa ihlal olayı ile karşılaşmıştır.	İşletmelerin %11'i haftada bir kez siber saldırı tecrübesi yaşamıştır. Büyük işletmelerin çoğu tedarik zinciri risklerini gözden geçirmektedir, ancak bu durum, tüm kuruluşlar arasında hâlâ nispeten seyrek görülmektedir.
2016 yılında işletmelerin Siber Güvenlik ihlal ve saldırılarının %68'inin sebebi casus yazılımlar, virüs, ve kötümcül yazılımlardır.	Siber ihlal ve saldırıların %83'ü kimlik avı saldırılarıdır.	Kimlik avı saldırılarının işletmeler için oranı % 83 dür.	İşletmelerin genel olarak %79'u kimlik avı saldırıları, %31' e-postalarda şirketin kimliğine bürünen siber saldırılara maruz kalmıştır.
%32'si ise farklı kimliklere girmiş kurum içindeki kişilerden kaynaklanmaktadır.	%27'si başka kimliğe bürünmüş kişilerden kaynaklanmaktadır.	Son 12 aydaki tüm siber saldırıların ortalama tahmini maliyetinin sadece orta ve büyük riskli işletmeler için 4.200 £ olmuştur.	Siber suçun işletmeler için ortalama yıllık maliyeti mağdur başına yaklaşık 15.300 £ olduğu tahmin edilmektedir.

Bilgi güvenliği çok boyutlu bir disiplindir, teknik yönler önemlidir ancak yeterli değildir. Kontrol ve gözetim gerekmektedir. Teknoloji, insani, eğitim ve farkındalık, yönetimsel, kanun ve yaptırımlar ile psikolojik, kültürel ve sosyal boyutlarına da önem verilmelidir (Safa, Maple ve Watson, 2017).

Bilgi güvenliği çok yönlü bir disiplin olduğundan kanun ve yaptırımlar kısaca yasal düzenleme yönlerine de önem verilmesi gerekliliği birçok metinde ifade edilmiştir. 2016-

2019 tarihli Ulusal Siber Güvenlik Stratejisi Eylem Planında; ‘’*Paydaşların güvenlik risklerini bilmeleri…teknik boyutlar yanında hukuki, idari, ekonomik, politik ve sosyal boyutlara da’’* önem vermesi gerektiği açıkça belirtilmiştir (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, s. 11).

1.2 Literatür Araştırması

Literatür araştırması için öncelikle anahtar kelimeler, “Bilgi Güvenliği”, “Bilgi Güvenliği Politikaları”, “Bilgi Güvenliği İhlali”, “Bilgi Güvenliği Hukuku”, “Lojistikte Bilgi Güvenliği, “Bilgi Paylaşımı”, “Veri Koruma”, “Tedarik Zincirinde Bilgi Güvenliği” “Ticari Sır”, “Kişisel Verilerin Korunması” ve “Siber Güvenlik” şeklinde belirlenmiştir.

Belirlenen anahtar kelimelerle, Science of Direct, Scopus, Web of Science, Google Scholar ve YÖK Ulusal Tez Merkezi veri tabanlarında, akademik kaynaklar taranmıştır. Çalışma sonucunda tez, makale, rapor ve konferans bildirileri bulunmuştur. Sonrasında, Zhang vd.’nin (2020) “literatür araştırmasına dahil etme ve hariç tutma kriterleri’nden faydalanılarak Tablo 2 oluşturulmuştur (s.6).

Tablo 2. Literatür Araştırmasına Dahil Etme-Hariç Tutma Kriterleri

(Zhang, Duan, Gong, Brown ve Li, 2020)

Dahil Etme Kriterleri	Hariç Tutma Kriterleri
Lojistik veya Tedarik Zinciri Sektörü ile ilgili çalışmalar	Lojistik veya Tedarik Zinciri Sektörü haricinde farklı sektörler ile ilgili çalışmalar
Makale, tezler, ilgili meslek kuruluşları tarafından yayınlanan raporlar, konferans bildirileri	Haberler, teknik odaklı çalışmalar, ilgili meslek kuruluşları tarafından yayınlananlar hariç raporlar
İngilizce veya Türkçe çalışmalar	İngilizce veya Türkçe harici diğer dillerdeki çalışmalar
2005 ve sonrası çalışmalar	2005 öncesi çalışmalar

Literatür çalışması Aralık 2019’da yapılmıştır. Yeni araştırmaları da dahil etmek için çalışma 2020 yılı Temmuz’da tekrarlanmıştır. Araştırma neticesinde Türkçe ve İngilizce olarak toplam 145 çalışmaya erişilmiştir. Lojistik ve Tedarik Zinciri sektörü haricindeki veya teknik odaklı kaynak ile haber ve rapor içerikli kaynaklar kapsam dışı tutulmuştur. Netice itibariyle 2005-2020 yılları arasındaki 57 kaynak literatür çalışmasına dahil edilerek Tablo 3’de listelenmiştir.

Tablo 3. Literatür Araştırması

No	Yazar-Yıl	Başlık	Araştırma Türü	Yöntem
1	Michelberger, Labodi, 2009	Development Of Information Security Management System At The Members Of Supply Chain	Makale	Kavramsal çalışma
2	A.Boiko, Shendryk, O. Boiko, 2019	Information Systems For Supply Chain Management: Uncertainties, Risks And Cyber Security	Makale	Nitel araştırma
3	Safa, Maple, Watson, 2017	The Information Security Landscape in Supply Chain	Makale	Kavramsal çalışma
4	Avci, Karataş, 2017	Lojistik Bilgi Sistemi Güvenliği Kültürü Üzerine Bilgi Sistem Güvenliği Farkındalığı ve Bağlılığının Etkisi: Kargo Lojistik Firmalarından Bulgular	Makale	Anket
5	Małkus, Wawak, 2015	Information Security in Logistics Cooperation	Makale	Kavramsal çalışma
6	Pham, Nguyen, Mcdonald, Tran-Kıeu, 2019	Information Sharing in Logistics Firms: An Exploratory Study of theVietnamese Logistics Sector	Makale	Nitel araştırma
7	Burrell, Bhargava, Swanson, Harmon, Wright, Springs, Dawson, 2020	Supply Chain and Logistics Management and an Open Door Policy Concerning Cyber Security Introduction	Makale	İçerik analizi
8	Roy, Gupta, Deshmukh, 2012	Information Security in Supply Chains – A Process Framework	Konferans bildirisi	Kavramsal çalışma

9	Liu, Sun, Zhao, 2018	A Method of Logistics Information Security Based on Blockchain Technology	Konferans bildirisi	Deneysel araştırma modelleme
10	Fu, Zhu, 2017	Operation Mechanisms for Intelligent Logistics System: A Blockchain Perspective	Makale	Sistem tasarımı
11	Zhang, Li, 2006	Secure Information Sharing in Internet-Based Supply Chain Management Systems	Makale	Literatür taraması
12	Boyar-Sozonovitch, Pitelinskiy, Ermolatiy, 2019	Innovation Economy: Aspects of Economic And Information Security in Logistics Innovation	Makale	Kavramsal çalışma
13	Cheung, Bell, 2019	Attacker–Defender Model Against Quantal Response Adversaries For Cyber Security in Logistics Management: An Introductory Study	Makale	Sistem tasarımı modelleme
14	Tan, Wong, Chung, 2015	Information And Knowledge Leakage in Supply Chain	Makale	Vaka çalışması, Modelleme
15	Di, Libin, 2010	The Study of Security of Network Management Information System Based on Logistics Information Platform	Konferans bildirisi	Model uygulaması
16	Sindhuja, Kunnathur, 2015	Information Security in Supply Chains: A Management Control Perspective	Makale	Literatür taraması
17	Roy, Gupta, Deshmukh, 2013	Information Security Risk Assessment in SCM	Konferans bildirisi	Literatür taraması, kavramsal modelleme

18	Denolf, Trienekens, Vorst, Omta, 2015	The role of governance structures in supply chain information sharing	Makale	Vaka çalışması
19	Zhang, Zeng, Wang, Li, Geng, 2011	Modeling and evaluating information leakage caused by inferences in supply chains	Makale	Kavramsal model, Vaka çalışması
20	Colicchia, Creazza, Menachof, 2019	Managing Cyber and Information Risks in Supply Chains: insights from an Exploratory Analysis	Makale	Vaka çalışması
21	Wolden, Valverde, Talla,2015	The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System	Konferans bildirisi	Anket
22	Khan, Estay, 2015	Supply Chain Cyber-Resilience: Creating an Agenda for Future Research	Makale	Literatür taraması
23	Jianqiang, Shue, Weijun, 2015	Analyzing Information Security Investment in Networked Supply Chains	Konferans bildirisi	Modelleme
24	Smith, Watson, Baker, Pokorski, 2007	A critical balance: collaboration and security in the IT-enabled supply chain	Makale	Kavramsal çalışma (çerçeve)
25	Davis, 2015	Building Cyber-Resilience into Supply Chains	Makale	Kavramsal çalışma
26	Smith, Watson, Baker, 2008	Perception And Reality: An Introspective Study On Supply Chain Information Security Risk	Makale	Literatür taraması, Anket
27	Tuptuk, Hailes, 2018	Security of smart manufacturing systems	Makale	Kavramsal çalışma

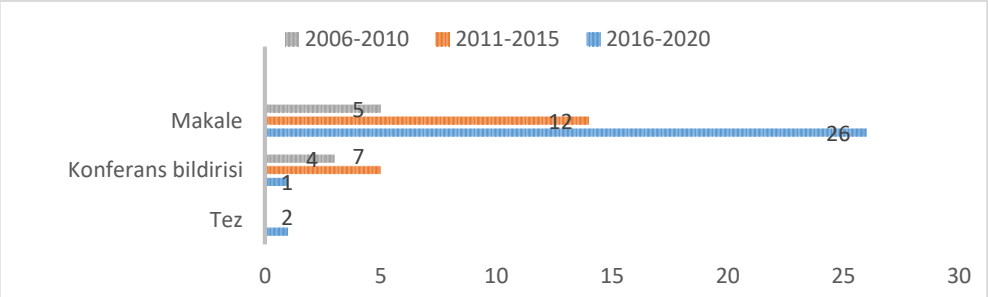
28	Hashem, Hossam, Hanafy, 2017	Impact of Information Security Initiatives on Supply Chain Performance	Makale	Kavramsal model, Yapısal eşitlik modellemeAnket
29	Kunnathur, Vaithianathan, 2008	Information Security Issues In Global Supply Chain	Konferans bildirisi	Literatür taraması, kavramsal çerçeve
30	Babaeinesami, Tohidi, Seyedaliakbar, 2020	A closed loop Stackelberg game in multi-product supply chain considering information security: A case study	Makale	Stackelberg oyun modeli
31	Wadhwa, Prakash, Deshmukh, Wadhwa, 2009	Information Security in Flexible Supply Chain Network: A Decision Information Security (DIS) Model	Makale	Modelleme
32	Durowoju, Chan, Wang, 2022	Investigation of the Effect of e-Platform Information Security Breaches: A Small and Medium Enterprise Supply Chain Perspective	Makale	Modelleme, Simulasyon
33	Wang, 2012	Research on the Construction of Supply Chain Collaboration System Based on Information Sharing	Konferans bildirisi	Modelleme
34	Selvi, 2020	Hızlı Tüketim Ürünlerinin Lojistiğinde Kullanılan Elektronik Sistemler Ve Endüstri 4.0: Balıkesir İli Örneği	Yüksek lisans tezi	Anket
35	Fernando, Chidambaram, Wahyuni, 2018	The Impact of Big Data Analytic and Data Security Practices on Service Supply Chain Performance	Makale	Modelleme, Anket

36	Tran, Childerhouse, Deakins, 2016	Supply Chain Information Sharing: Challenges and Risk Mitigation Strategies	Makale	Keşif nitel araştırma, Vaka çalışması
37	Speier, Whipple, Closs, Voss, 2011	Global supply chain design considerations: Mitigating product safety and security risks	Makale	Çoklu yöntem araştırması
38	Epiphaniou, Pillai, Maple Bottarelli, Al-Khateeb, Hammoudesh, 2020	Electronic Regulation of Data Sharing and Processing Using Smart Ledger Technologies for Supply-Chain Security	Makale	Modelleme
39	Varma, Khan, 2015	Information technology and e-risk of supply chain management	Makale	Kavramsal çalışma
40	Bargshady, Zahraee, Parto, Ahmadi, 2016	The effect of information technology on the agility of the supply chain in the Iranian power plant industry	Makale	Anket
41	Durowoju, Chan, 2012	The Role of Integration in Information Security Breach Incidents	Makale	Simulasyon
42	Ulhag, Kuruvilla, Nkhoma, Vu, Truong, 2016	Information Security Risks In Supply Chain Management: A Review Of Literature For The Developing Country Context	Makale	Literatür taraması
43	Estay,2017	Managing cyber-risk and security in the global supply chain: A systems analysis approach to risk, structure and behaviour	Doktora Tezi	Literatür taraması, Sistem analizi

44	Durowoju, Chan, Wang, Akenroye, 2020	Supply chain redesign implications to information disruption impact	Makale	Simulasyon Anket İstatiksel analiz
45	Sindhuja,2014	Impact of information security initiatives on supply chain performance	Makale	Literatür taraması Kavramsal model, Anket
46	Kattan, Nunu, Saleh, 2009	A stochastic model for improving information security in supply chain systems	Makale	Stokastik güvenlik modeli
47	Ghadge, Weiß, Caldwell, Wilding, 2019	Managing cyber risk in supply chains: A review and research agenda	Makale	Literatür taraması, Veri madenciliği küme analizi, Kavramsal model
48	Roy, Kundu, 2012	Management Of Information Security In Supply Chains – A Process Framework	Konferans bildirisi	Literatür taraması Kavramsal süreç çerçevesi
49	Bolhari, 2009	Electronic-Supply Chain Information Security: A Framework for Information Security in e-SCM (e-SCIS)	Konferans bildirisi	Kavramsal çalışma
50	Zadeh, Ramayah, Hanifah, Kurnia, Mahmud, 2020	Supply chain information integration and its impact on the operational performance of manufacturing firms in Malaysia	Makale	Anket, Modelleme
51	Zhong, Deng, 2010	Model Design of Information Security Monitoring System of	Konferans bildirisi	İstatiksel yöntem, Modelleme

		Nanchang Bonded Logistics Park		
52	Bhargava, Ranchal, Othmane, 2013	Secure Information Sharing in Digital Supply Chains	Konferans bildirisi	Kavramsal çalışma
53	Ried, Carter, Eckerd, Kaufmann 2020	Spillover effects of information leakages in buyer-supplier-supplier triads	Makale	Deneysel tasarım, Modelleme
54	Zhang, Cao, Wang, Zeng, 2012	Mitigating the risk of information leakage in a two-level supply chain through optimal supplier selection	Makale	Modelleme
55	Spiliotopoulou, Donohue,Gürbüz 2016	Information Reliability in Supply Chains: The Case of Multiple Retailers	Makale	Modelleme
56	Dwivedi, Amin, Vollala, 2020	Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism	Makale	Modelleme
57	Liu, Jiang, Feng, Chin, 2020	Information leakage and supply chain contracts	Makale	Modelleme, Analiz

Tablo 3' de gösterilen 57 adet akademik çalışma arasında, en eski tarihli çalışma 2006 yılına ait ve 1 adettir. 2006-2010 arasında 9 adet, 2011-2015 arasında 19 adet, 2016-2020 arasında da 29 adet çalışma yapılmıştır.



Şekil 1. Yıllara Göre Yapılan Akademik Araştırmalar

Şekil 1 verileri, bilgi güvenliği konusunda sektörde yapılmış olan araştırmaların yıllar içerisinde artış eğiliminde olduğunu göstermektedir. Özellikle dijitalleşmenin iş ve sosyal yaşama hızlı şekilde girişi ile birlikte bilgi güvenliği konusu daha da önemli hale gelmiştir.

Akademik çalışmalar, tedarik zinciri ve lojistikte bilgi güvenliği, siber güvenlik, bilgi ihlali, veri güvenliği hakkındadır. Lojistik sektöründe bilgi güvenliğine ilişkin olan blok zincir, büyük veri teknolojilerine odaklanan çalışmalar da incelenmiştir. Kullanılan yöntemler açısından yapılan değerlendirmeye göre, 11 çalışmada Literatür taraması, 10 çalışmada Anket, 22 çalışmada Modelleme/sistem tasarımı/deneysel/ simulasyon, 10 çalışmada Vaka/analiz, 21 çalışmada Kavramsal araştırma/nitel/çerçeve çalışması yürütülmüştür. Tablo 4'de araştırma konu ve yöntemlerine ilişkin bilgilere yer verilmiştir.

Tablo 4. İnceleme Konuları ve Yöntemler

		Yöntemler				
İnceleme Konuları	**Araştırılan Kaynaklar**	Vaka-Analiz	Anket	Literatür Taraması	Kavramsal Çerçeve-Çalışma-Nitel	Sistem Tasarım - Simülasyon - Modelleme
Bilgi güvenliği - Kişisel veri	3				2	1
Siber risk-güvenlik-ihlal	7	4		3	3	2
Bilgi güvenliği çerçeve-politikaları	4		8	1	3	
Bilgi güvenliği-	39	6	1	7	13	15

Sızıntı-paylaşım						
Büyük veri-BZ teknolojisi	4		1			4
TOPLAM	**57**	**10**	**10**	**11**	**21**	**22**

Literatür araştırma çalışmasının bir sonraki aşamasında, seçilen makale özetleri çalışmanın kapsamıyla ilgileri açısından gözden geçirilerek, detaylı olarak incelenecek 20 adet çalışma seçilmiştir. Tablo 5'de 20 adet çalışmanın özeti yer almaktadır.

Tablo 5. Ayrıntılı Literatür İncelemesi

No	Yazar-Yıl	İncelenen Problem	Yöntem	Özet
1	Safa, Maple, Watson, 2017	Tedarik zincirlerinde bilgi varlıklarının kullanılabilirliğini, gizliliğini ve bütünlüğünü etkileyen bilgi güvenliğinin farklı yönleri araştırılmıştır.	Kavramsal çalışma	Çalışmada, TZ'de bilgi varlıklarının kullanılabilirliğini, gizliliğini ve bütünlüğünü etkileyen bilgi güvenliğinin farklı yönleri araştırılmıştır. Bilgi güvenliği için teknik yönlerin önemli olduğu ancak yeterli olmadığı, bilgi güvenliğinin tüm yönlerine dikkat edilmesi gerektiği, çok boyutlu bir disiplin olduğu, kontrol ve gözetim gerektiği, teknolojik, yönetimsel, insani, eğitim ve farkındalık, kanun, yaptırımlar, sosyal, kültürel ve psikolojik boyutlarına da önem verilmesi gerektiği, kurumsal bir yönetim sorumluluğu olduğu, bilgi güvenliği politikalarına uyulması gerektiği vurgulanmıştır.
2	Boyar-Sozonovitch, Pitelinskiy, Ermolatiy, 2019	Lojistik inovasyonu, ekonomik ve bilgi güvenliği yönleri ile ele alınmıştır.	Kavramsal çalışma	Lojistik inovasyonu, ekonomik ve bilgi güvenliği bakımından araştırılmıştır. Sonuç olarak, lojistik uygulamalarda teknoloji değiştikçe artan yenilik sayısı ve kalitesi ile birlikte, iş süreçleri ve lojistik sistemlerin, üretim ve operasyonun her aşamasında hem yeni teknolojiyi hem de bilgi güvenliğini korumak için, teknik, yasal ve bilgi risk yönetimi ve güvenlik önlemlerine ihtiyaç duyulacağı hususu değerlendirilmiştir.
3	Zadeh, Ramayah, Hanifah, Kurnia, Mahmud, 2020	Tedarik Zinciri Bilgi Entegrasyonunun şirketlerin operasyonel verimliliği üzerindeki etkisi, bilgi sızıntısının rolü dikkate alınarak incelenmiştir.	Anket, Modelleme	Makalenin amacı, TZ Bilgi Entegrasyonunun şirketlerin verimliliği üzerindeki etkisini, bilgi sızıntısının rolünü dikkate alarak incelemektir. Sonuç, BG kalitesi ve teknolojisinin, TZ'ni olumlu etkilediğini göstermiştir.

		İşletmelerin, bilgi güvenliğiyle ilgili politikalara uygun hareket etmesi gerektiği belirtilmiştir.		Yasal sistemin, çalışanların sorumluluklarını tkileyebileceği, veri güvenliğinin yalnızca teknik yönü olan bir alan olmadığı, teknolojik, eğitimsel, yönetimsel, kanun ve yaptırıma kadar çeşitli boyutları olan bir disiplin olduğu belirtilmiştir. Çalışanlar sorunun farkındaysa, bilgi güvenliği ihlali olasılığının büyük ölçüde azalacağı vurgulanmıştır.
4	Wolden, Valverde, Talla,2015	TZ yönetim sistemlerinde, siber saldırı riskinin azaltılmasında COBIT 5 Bilgi Güvenliği Çerçevesi uygulamasının etkinliği araştırılmıştır.	Vaka çalışması, Anket	Siber casusluk ve zararlı yazılım saldırıları gibi siber suçlara TZ'leri yabancı değildir. Çalışma da, TZ üzerindeki siber saldırı riskinin azaltılmasında COBIT5 Bilgi Güvenliği Çerçevesi uygulamasının etkinliği anket ile araştırılmıştır. Sonuçlar, COBIT 5'in katı politikalar ve kurumsal uygulama güvenliğini daha da güçlendirdiğini kuruluşların COBIT 5 çerçeve güvenlik önlemlerini uyguladığı görülmüştür.
5	Durowoju, Chan, Wang, Akenroye, 2020	Bilgi güvenliği ihlallerinin risk stratejileri üzerindeki etkisi incelenmiştir.	Simulasyon, Anket, İstatistiksel analiz	Analistlere göre, bilgi güvenliği ihlalleri, işletmeler için büyük maliyetler oluşturan bir risk ve tehlikedir. Çalışmada, bilgi güvenliği ihlallerinin risk stratejileri üzerindeki etkileri araştırılmıştır. Pandeminin getirdiği önemli tedarik zinciri kesintileri, uzun ve karmaşık küresel tedarik zincirinin güvenlik açıklarını ve risklerini de ortaya çıkarmıştır.
6	Avci, Karataş, 2017	Yerleşik bilgi sistem güvenliğine ilişkin kültürel bir yapının mevcudiyeti ve yöneticilerin konuya ilişkin bilgi sahipliği durumu incelenmiştir.	Anket	Çalışmada, bilgi sistem güvenliğinde alınan teknik önlemlerin yanı sıra, örgütsel önlemlere de gereksinim olduğu, bilgi sistem güvenliği için yalnızca teknik konularda çalışan işçilerin yeterli olmadığı diğer tüm çalışanlarında katılımının gerekli olduğu belirtilmiştir. Kargo şirketlerinde mevcut bilgi sistem güvenliği kültürünün varlığı ve yöneticilerin bu konudaki farkındalıklarının incelenmesi üzerine bir çalışma gerçekleştirilmiştir.
7	Michelberger, Labodi, 2009	Lojistik bilgi sistemlerinde, uluslararası standartlar ve önerilere uygun bir bilgi güvenliği oluşturmak için	Kavramsal çalışma	Lojistik bilgi sistemlerinde bilgi güvenliği için, TZ üyesi şirketler için öngörülen gereksinimler araştırılmıştır. Entegre tedarik zinciri bilgi sistemlerinin

		ihtiyaçları belirlemek üzere bir çalışma yapılmıştır.		çalışmasının yalnızca bilgi teknolojisi sorunu olmadığı vurgulanarak gerekli bilgilere kimlerin ne zaman ve nasıl erişebilecekleri veya ne zaman şirket içi veya şirketler arası bir ticari işleme başlayabilecekleri hususunun TZ'deki şirketler için hayati önem taşıdığı belirtilmiştir.
8	A.Boiko, Shendryk, O. Boiko, 2019	Çok bileşenli üretime sahip şirketlerde tedarik zinciri yönetimi için bilgi sistemlerinin kullanım durumu incelenmiştir.	Nitel araştırma	Tedarikçiler ve müşteriler arasında iş akışlarını etkili bir şekilde bütünleştirmek için, üreticilerin karmaşık bilgi güvenliği sorununu çözmesi gerektiği vurgulanmıştır. Gerçek zamanlı izleme ve kaçak yolu tespiti sağlayan çözümlerin sağlanması gerektiği, işletmelerin politikalarını test ederek etkinliğini doğrulamak için sağlam araçlar uygulamaları, ağa bağlı envanter cihaz ve sistemleri almalarının gerekliliği belirtilmiştir.
9	Burrell, Bhargava, Swanson, Harmon, Wright, Springs, Dawson, 2020	Kurumlarda önleyici bilgi güvenliği ve dijital güvenlik risklerini azaltmak için yaklaşımların neler olabileceği araştırılmıştır.	İçerik analizi	Günümüzde TZ ve lojistik kuruluşlarını siber risklerden korumanın artık sadece bir bilgi teknolojisi çalışanı işlevi olmadığı, her kurumsal çalışanın veri koruma sürecinde bir sorumluluğu olduğu belirtilmiştir. Öngörü sahibi işletmelerin, çalışanlarını bilgi ve siber güvenlik sürecinde aktif olarak çalışmaya yönlendiren, politikalar ve yöntemler geliştirebilen firmalar olduğu ifade edilmiştir.
10	Colicchia, Creazza, Menachof, 2019	Tedarik zincirlerinde şirketlerin bilgi sızıntı riskleri yönetimine nasıl yaklaştıkları, hangi girişimleri ve ne ölçüde benimsedikleri araştırılmıştır.	Vaka çalışması	Çalışmada nihai amaç, kuruluşların, tedarik zincirlerindeki siber risk sürecini ve siber dayanıklılığı anlayıp geliştirmelerine yardımcı olmak olarak belirtilmiştir. Sonuçta, şirketlerin bilgi teknolojisi altyapılarını tüm TZ'ne yöneltmelerinin önemli olduğu vurgulanmıştır.
11	Khan, Estay, 2015	Tedarik zinciri siber dayanıklılığı için bir araştırma gündemi oluşturulmuş, akademi ve uygulama için önerilerde bulunulmuştur.	Literatür taraması	TZ'de hayati önemde bilgi paylaşılmakta olup, siber korsanlar için kolay ve kazançlı bir hedef durumuna gelmiştir, bu durum maddi kayıplara, marka itibar ve değerine zarar vermektedir. Şirketlerin, tehditlere karşı korunmak için

				TZ'ni koruyucu yatırımlar yapmaları gerektiği vurgulanmıştır. İş dünyasında bu alana ilişkin ilginin fazlalaştığı ancak akademik çevreler tarafından az çalışma yapıldığı belirtilmiştir. Bu amaçla, TZ siber dayanıklılığı için bir araştırma gündemi oluşturulmuş, akademi ve uygulama için öneriler yapılmıştır.
12	Smith, Watson, Baker, 2008	TZ'de bilgi güvenliği algı ve risk çalışması yapılmıştır. Bu konuya önem veren yöneticilerin, güvenlik maliyetlerinin azaltılmasında veya rekabet konusunda önemli faydalar sağlayabilecekleri belirtilmiştir.	Literatür taraması, Anket	TZ'de firmalar hayatta kalabilmek için daha fazla iş birliğine gitmekte bunun için bilgi teknolojisinden de daha fazla yararlanarak müşteri memnuniyetini arttırmaktadır. Ancak risklere karşı savunmasızlığıda artmaktadır. Çalışmada, TZ'de bilgi güvenliği riski ve algısı çalışması yapılmıştır.
13	Hashem, Hossam, Hanafy, 2017	Tedarik zincirindeki şirketlerin bilgi güvenliğini etkin şekilde uygulamalarının operasyon ve performansa etkileri araştırılmıştır.	Kavramsal model, Anket, Yapısal eşitlik modelleme	Araştırmada, tedarik zincirindeki şirketlerin iç ve dış bilgi güvenliği girişimlerinin etkin bir şekilde uygulanmasının, tedarik zincirinin operasyon ve performansı üzerindeki etkisi incelenmiştir.
14	Durowoju, Chan, Wang, 2022	Çalışmada, bilgi güvenliği ihlallerinin neden olduğu irtibat kesintisinin tedarik zinciri verimliliği üzerindeki etkileri incelenmiştir.	Modelleme, Simulasyon	Değişik büyüklükteki şirket ortakları veya tedarikçileri ve müşteriler, bilişimden de faydalanarak bilgi alışverişinde bulunmaktadır. Bilgi teknolijilerinde, siber saldırıların neden olduğu bilgi güvenliği ihlalleri çok yaygındır. Çalışmada, ayrık olay modelleme yoluyla, bilgi güvenliği ihlallerinin neden olduğu irtibat kesintisinin tedarik zinciri verimliliği üzerindeki sonuçları araştırılmıştır. Ayrıca farklı düzeylerde bilgi paylaşımı ile ihlal kesintisi sıklığının ve bunları düzeltme süresinin tedarik zinciri performansı üzerindeki etkisi incelenmiştir.
15	Bolhari, 2009	E-tedarik zincirleri bilgi güvenliği açısından daha savunmasızdır. Literatür incelemesi ve tedarik ağının idaresinde bilişim	Literatür taraması, Kavramsal çalışma	Küreselleşme ile birlikte elektronik tedarik zincirleri, diğer tedarik zinciri türleri arasında bilgi güvenliği açısından daha savunmasızdır.

		sistemleri çerçevesi araştırılmıştır.		Makale, güvenlik ve tedarik zinciri literatürlerini inceleyerek ardından tedarik zinciri yönetiminde bilgi teknolojisi çerçevesini araştırmıştır. Çalışma, yöneticilere, e-tedarik zinciri ağlarının yeterince güvenli olup olmadığını öğrenmeleri için kılavuz olmaktadır.
16	Roy, Kundu, 2012	Tedarik zincirlerinde bilgi güvenliği ile ilgili konular tartışılarak bilgi güvenliğinin yönetimi için bir süreç çerçevesi önerilmiştir.	Literatür taraması Kavramsal süreç çerçevesi	Bilgi güvenliği, işletme için,itibarı korumak ve tehditleri azaltmak için çok önemlidir. Bilgi güvenliği sadece teknoloji sorunu olarak ele alınamaz yönetişim ve personel sorunları eşit derecede önemlidir. Bu itibarla çalışmada, tedarik zinciri boyunca bilgi güvenliğinin yönetimini sağlamak için tutarlı iş uygulamalarını geliştirmek ve sürdürmek için bilgi güvenliği yönetimi süreç çerçevesi önerilmiştir.
17	Selvi, 2020	Teknoloji tabanlı uygulamalarda güvenlik açıkları ve riskleri bulunmaktadır. Bu sebeple şirketlerin bilişim sistemlerini ve teknik altyapılarını güvenlik tehditlerine karşı korumalarının gerekliliği vurgulanmıştır.	Anket	Çalışmada, endüstri 4.0 ile değişen lojistik sektöründe, etkili ve başarılı bir lojistik 4.0 için, birtakım uygulamaların kullanılmasının öneminden bahsedilmiştir. Bunların içinde bilgi güvenliği de vardır. Firmaların bilişim sistemlerini ve teknik altyapılarını güvenlik tehditlerine karşı savunmaları zorunludur. Anket sonuçlarına göre, firmaların bilgi güvenliği ile ilgili, ek maliyet gibi konularda farklı yaklaşımlarda olduğu belirtilmiştir.
18	Jianqiang, Shue, Weijun, 2015	Bilgi güvenliği riskinin, firmaların bilgi güvenliğine yatırım yapma stratejilerine etkileri araştırılmıştır.	Oyun teorisine dayalı Modelleme	Güvenlik ihlalleri ve saldırılar, tedarik zincirlerindeki çoğu şirket için büyük problem oluşturmuştur. Çalışmada, bilgi güvenliği riskinin, firmaların bilgi güvenliğine yatırım yapma konusunda optimal stratejilerini nasıl etkilediği araştırılmış bunun için de oyun teorisine dayalı model geliştirilmiştir. Sonuç, güven risklerinin, bilgi güvenliğine aşırı yatırım yapılmasına neden olduğunu göstermiştir.

19	Tan, Wp, Chung, 2015	Bilgi ve bilgi sızıntısını tetikleyen faktörler araştırılarak sızıntıların performans üzerindeki etkileri azaltılmaya çalışılmıştır.	Vaka çalışması, Modelleme	Çalışmanın amacı, bilgi ve bilgi sızıntısını tetikleyen faktörleri araştırarak sızıntıların performans üzerindeki etkisini azaltmak üzere çerçeve oluşturmaktır. Araştırmada metodoloji olarak yapılandırılmış bir görüşmeden elde edilen bir vaka çalışması benimsenmiştir. Sonuç olarak, tedarik zinciri yönetimine bilgi ve bilgi sızıntısı yönetimiyle ilgili fikirler eklenmiştir
20	Pham, Nguyen, Mcdonald, Tran-Kıeu, 2019	Lojistik işletmelerinin tedarik zincirindeki firmalarla paylaştığı bilgiler incelenerek, veri paylaşımı güvenlik tehditleri üzerinde durulmuştur.	Nitel araştırma Yarı yapılandırılmış görüşme ve literatür taraması	Bilgi paylaşımı tedarik zinciri verimliliğini artırmak için oldukça önemlidir. Çalışmada, lojistik işletmelerinin tedarik zinciri ortaklarıyla hangi bilgileri paylaştığını, paylaşım yöntemlerini ve paylaşım uygulamasını etkileyen faktörler incelenmiştir. Bilgi paylaşımı güvenlik riskleri, teknik yetenek, organizasyon kuralları ve politikaları üzerinde durulmuştur.

Araştırma konularını içeren Tablo 4 incelendiğinde lojistik sektöründe, bilgi güvenliği ile ilgili araştırmalarda, değişik kapsamlarda çalışmalar yapıldığı görülmektedir. Bilgi güvenliği politikaları konusunda literatürde az sayıda bilimsel çalışmaya rastlanmış, bu çalışmalarda da, gelecekte yapılacak araştırmalar ile doldurulacak birçok boşluk bırakıldığı belirlenmiştir.

Detaylı inceleme yapılan makalelerde;

"Bilgi güvenliği için teknik yönlerin önemli olduğu ancak yeterli olmadığı, bilgi güvenliğinin tüm yönlerine dikkat edilmesi gerektiği, teknolojik, yönetimsel, eğitim ve farkındalık, kanun, yaptırımlar yönlerine de önem verilmesi gerektiği" (Safa, Maple ve Watson, 2017, s. 18-19).

"Teknoloji ve bilgi güvenliğini korumak için teknik, yasal ve bilgi risk yönetimine ihtiyaç olduğu" (Boyar Sozonovitch, Pitelinskiy ve Ermolatiy, 2019, s. 13).

"Yasal sistemin, çalışanların bilgi paylaşımı açısından sorumluluklarını etkileyebileceği, bilgi güvenliği sadece teknik bir konu olmadığı, teknolojik, eğitimsel,

yönetimsel, kanun ***ve*** *yaptırıma kadar çeşitli boyutları olan bir disiplin olduğu"* (Zadeh, Ramayah, Hanifah, Kurnia ve Mahmud, 2020, s. 8).

"Yalnızca bilgi teknolojisi sorunu olmadığı, gerekli bilgilere kimlerin ne zaman ve nasıl erişebilecekleri (yetki sınırlaması) hususunun tedarik zincirindeki örgütlenmiş şirketler için hayati önem taşıdığı" (Michelberger ve Labodi, 2009, s. 78) şeklinde "*Bilgi Güvenliğinde Hukukun Önemini"* anlatan ifadelere yer verildiği görülmektedir. Ancak çok sayıdaki güncel akademik çalışmada hukukun öneminden bahsedildiği halde bilgi güvenliğini hukuki açıdan inceleyen bir çalışmaya rastlanılmamıştır. Bu çalışmada, bilgi güvenliği hukuki boyutu ile ele alınmıştır. Şirket verilerini elde etmeye yönelik saldırılar, ister dışarıdan ister şirket içinden yapılmış olsun, yasal düzenlemeler ile uyumlu prosedür, yetkilendirme ve politikalar oluşturularak koruma tedbiri alınmaz ise, bilgi güvenliğinin tam ve yeterli şekilde sağlanmış olduğundan söz edilemeyecektir.

Temmuz 2020'de yapılan literatür araştırmasında, lojistikte bilgi güvenliği konusunda çalışmaların yıllar içerisinde 2015'den itibaren artış eğiliminde olduğu, özellikle dijitalleşmenin yaygınlaşması ile bu konunun çok daha önemli hale geldiği görüldüğünden, 2021-2024 yılları arasında araştırmaya devam edilmiştir. Literatür araştırması "Siber saldırılar", "Siber suç", "Bilgi güvenliği standartları", "Dijitalleşme", "Bilişim sistemi" ve "Tedarik zinciri risk" ve "Siber risk" anahtar kelimeleri de eklenerek yapılmıştır. Tablo 6'da araştırma sonuçlarına yer verilmiştir.

Tablo 6. Güncel Literatürün Kapsamlı Analizi

No	Yazar-Yıl	İncelenen Problem	Yöntem	Özet
1	Cheung K-F, Bell M.G.H., Bhattacharjya J., 2021	Çalışmada, lojistik ve tedarik ağının idaresinde siber güvenliği artıran önlemler gözden geçirilmektedir. Siber güvenlik araştırmalarıyla ilgili önemli bulgular sunulmaktadır.	Literatür araştırması, sentez yöntemi	İnternet tabanlı teknolojiler lojistikte saldırı yüzeyini artırmıştır. Saldırılar hem lojistik hem de genel TZ performansını olumsuz etkileyebilir. Lojistik ve TZ yönetiminde siber güvenliği artıran önlemler üzerine yapılan çalışmalar incelemektedir. Sonuç, (1) Lojistik, TZ'de önemli bir rol oynamasına rağmen, lojistikte siber güvenliğe odaklanan çalışmalar azdır, (3) Bilgi güvenliği ve dijital adli soruşturma ile ilgili çalışmalar azdır.
2	Latif M.N.A., Aziz N.A.A., Hüseyin N.S.N., Aziz Z.A., 2021	Çalışmada anket sonuçları, bilim adamlarının TZ yönetiminde siber güvenliğin önemine ilişkin görüşlerini sunmaktadır. Geçmiş çalışmaların çoğu ağ güvenliğine odaklanmıştır. Gelecekte siber güvenlikle ilgili birçok çalışmaya ihtiyaç duyulacağı belirtilmiştir.	Anket, Literatür araştırması, Makale analizi	TZ yönetiminin siber terörizm, kötü amaçlı yazılım ve veri hırsızlığı tehdidi altında olma riski yüksektir. Riskleri azaltmak için çalışma yapılmalıdır. Anket sonucu, TZ yönetiminde siber güvenlik araştırmaları artmaktadır. Siber güvenlikte Ağ güvenliği, web uygulaması, nesnelerin interneti ve bilgi güvenliği keşfedilmiştir.
3	Topping C., Dwyer A., Michalec O., Craggs B., Rashid A., 2021	Hükümetler, kritik ulusal altyapılara yönelik saldırılar konusunda endişelidir. Çalışmada, Siber Tedarik Zinciri Risk Yönetimi ile ilgili olarak Birleşik Krallık, ABD ve AB'deki yetkililer tarafından sunulan tavsiye ve rehberlik formları incelenmiştir.	Yaygın kartopu tekniği	Siber tehditler, artan bir şekilde TZ hedefliyerek müşteri-tedarikçi güvenini kötüye kullanmaktadır. Çalışmada, Siber Tedarik Zinciri Risk Yönetimi ile ilgili olarak Birleşik Krallık, ABD ve AB'deki yetkililer tarafından sunulan tavsiye ve rehberlik formları incelenmiştir. Sonuçlar, TZ riskini azaltmak ve kontrollerin uygulanmasını sağlamak için tedarik zinciri risk yönetimi ve sistematik rehberliğe ilişkin bir sınıflandırma ihtiyacını vurgulamaktadır. Daha fazla tartışma ve araştırma çalışmasını teşvik etmek için veri analizine

				dayalı bir anahat şablonu sunulmuştur.
4	Farah M.A.B., Ukwandu E., Hindy H., Brosset D., Bures M., Andonovic I., Bellekens X., 2022	Çalışmada, denizcilik endüstrisinde yaşanan siber saldırılar sınıflandırılmakta ve etkileri sayısallaştırılmaktadır. Güçlü bir siber koruma sağlamanın önemli bir yolunun, topluluk genelinde siber güvenlik bilincinin geliştirilmesi olduğu, farkındalığı desteklemek için de, siber tehditlere yönelik çözümleri daha da fazla güçlendirmek için hukuki bir çerçeve metodolojileri oluşturulması gerektiği ifade edilmiştir.	Literatür taraması	Sektörün, sürekli artan şekilde akıllı liman içi hizmetlere ve otonom gemilere geçişi, yeni siber güvenlik protokollerinin kurulmasını gerektirmiştir. Güçlü bir siber koruma sağlamanın önemli bir yolu, topluluk genelinde siber güvenlik bilincinin geliştirilmesidir. Farkındalığı desteklemek için, siber tehditlere yönelik çözümleri daha da fazla güçlendirmek üzere hukuki bir çerçeve metodolojileri oluşturulmalıdır. Ayrıca, uygulamaların gelişimini hızlandırmak için tüm siber güvenlik sorunları paydaşlar arasında şeffaf hale getirilmelidir; yeni siber saldırıların ayrıntıları ve etkisi, tedarik zinciri boyunca bilgi için iletilmelidir.
5	Li W., Lai Y., Zhong Y., 2024	Bilgi güvenliği ihlali ile ilgili olarak yapılan bu araştırmada, bir firmaya coğrafi olarak daha yakın olan bir tedarikçinin, o firmanın bilgi ifşa ihlalini daha kolay bastırabileceğine ilişkin sonuçlara ulaşılmıştır. Ayrıca sistemli olarak yapılacak bilgi güvenliği denetimlerinin önemi üzerinde durulmuştur.	Eşleştirme ve araçsal değişken yöntemi	Bu çalışma da, tedarikçi coğrafi yakınlığı ile kurumsal bilgilerin ifşa ihlali arasındaki ilişki incelenmektedir. Çin'de 13.775 firma verileri kullanılarak, bir firmaya coğrafi olarak daha yakın olan bir tedarikçinin o firmanın bilgi ifşa ihlalini bastırabileceği sonucuna ulaşılmıştır. Bu ilişki, tedarikçinin daha spesifik yatırımlar sağlaması ve firmanın devlete ait olmayan bir kuruluş olması durumunda daha da belirgindir.
6	Syed N.F., Shah S.W., Rasua R.T., Doss R., 2021	Makale, insanlar ve süreçler sistemin bir parçası haline getirildiğinde tedarik zincirinde güvenli	Modelleme	Dijital teknolojiler, modern TZ'de giderek daha fazla benimsenmektedir. Bu benimseme siber tehditlerin

		izlenebilirliği analiz etmektedir. Analizin amacı, izlenebilirlik için teknik çözümler uygulanırken ilgili paydaşlara olası siber güvenlik risklerini ve güvenlik açıklarını anlamalarında yardımcı olmaktır.		sayısını artırmaktadır. Bunlar, iş verileri, iş operasyonlarının aksaması ve itibar, fikri mülkiyet ve finansal varlıkların kaybı şeklinde olur. Bu sebeple TZ ağı etkili bir siber güvenliğe ihtiyaç duyar.
7	Filho N.G., Rego N., Claro J.,2021	Çalışmada, tedarik zinciri akışları ve stoklarının, siber risklere giriş noktaları olarak nasıl işlev gördüğünü tespit edebilmek üzere düzenli bir kaynak araştırması yapılmıştır.	Sistematik literatür taraması	TZ dijital hale geldikçe, farklı riskler ortaya çıkmaktadır. Siber riskler, TZni doğrudan ve dolaylı olarak etkileyen ve TZ akışları ve stokları (bilgi, malzeme ve finansal) yoluyla yayılan risklerdir. Çalışmada, TZ akışları ve stoklarının, siber risklere giriş noktaları olarak nasıl işlev gördüğünü tespit edebilmek üzere bir kaynak araştırması uygulanmıştır. Araştırma, 1) Potansiyel siber risklerin giriş noktalarının tanımı, yönetsel çabaların nereye odaklanılacağına dair ipuçları verdiğinden ve farkındalık sağladığından yararlıdır. 2) Gelecekteki araştırmalar için faydalı olabilir.
8	Sindhuja P.N, 2021	Bu makalenin amacı, bilgi güvenliği girişimlerinin TZ sağlamlığı ve performansı üzerindeki etkisini incelemek olarak açıklanmıştır.	Yapısal eşitlik modelleme, Anket, Analiz	Bilgi güvenliği, tüm ticari faaliyetlerde önemlidir. Günümüzün küresel TZ bilginin, zincir ortakları arasında hızlı ve sağlam bir şekilde yayılmasına güvenmektedir. Etkili bir bilgi güvenliği yönetiminin tedarik zincirinin sağlamlığını sağladığı kabul edilir. Bilgi güvenliği, insanları, süreçleri, yönetimi ve araçları kapsayan çok boyutlu bir unsur olarak görülmüştür.
9	Kechagias EP.Chatzistelios G., Papadopoulos G.A	Çalışmada, denizcilik siber güvenlik yönlerine ilişkin ayrıntılı bir vaka çalışması analizi sunmaktadır.	Vaka çalışması analizi	Denizcilik alanında siber güvenliğe odaklanılarak bir vaka çalışması sunulmuştur.

	Apostolou P., 2022			Makalenin temel amacı, bir denizcilik şirketinin siber güvenlik yaklaşımını prosedürlere ve politikalara referanslarla sunarak, araştırmayı uygulama ile ilişkilendirmektir. Vaka çalışmasının bulguları şirketin güvenlik açıklarını belirleyebildiğini ve siber riskleri azaltmayı başardığını göstermektedir.
10	Bilgiç E. Türkmenoğlu, M.A. Koçak, A. 2020	Makalede, dijitalleşmenin lojistik sektörünü ne şekilde etkilediği ve gelecekte ne tür etkiler oluşturabileceği, literatür ve firma örneklerinin incelenmesi ile ortaya çıkarılmaya çalışılmıştır.	Nitel araştırma	Dijital dönüşümün lojistik sektöründeki işletmeler üzerindeki etkileri ve potansiyel gelecek etkileri, güncel literatür, kurum raporları ve işletme örneklerinin incelenmesiyle ortaya konulmaya çalışılmıştır.
11	Senarak C., 2021	Çalışmada liman işletmecilerinin siber güvenlik önlemleri geliştirmelerine yardımcı olmak için, liman siber güvenliğinin üç boyutu (insan, altyapı ve prosedür faktörleri) incelenerek siber güvenlik ile siber tehditler arasındaki ilişkiler araştırılmıştır.	Anket, Modelleme	Liman işletmecileri rekabet için siber teknolojiyi liman faaliyetlerine entegre etmektedir. Ancak bu, siber tehditi arttırmaktadır. Liman siber güvenliği ile siber tehditler arasındaki ilişki araştırılmıştır. Sonuçlar konteyner limanlarının insan altyapı ve prosedür faktörleri savunmasız olduğunda bilgisayar korsanlığıyla karşılaşma eğiliminde olduğunu göstermiştir. Bu nedenle tüm liman çalışanlarına eğitim verilmesi gerekliliği ifade edilmiştir.
12	Jbair M., Ahmad B., Maple C., Harrison R., 2022	Kuruluşların siber saldırıları ciddi iş riski olarak görmeleri gerekir. Çalışmada endüstriyel varlıkları potansiyel siber saldırılardan korumak için	Modelleme Literatür taraması	Potansiyel siber tehditleri belirlemek ve etkilerini analiz etmek, iş sürekliliği planlaması için önemlidir. Çalışma, endüstriyel

		siber risklerin tahminini ve analizini sağlayan yapılandırılmış bir tehdit modelleme yaklaşımı önerilmektedir.		varlıkları potansiyel siber saldırılardan korumak için siber risklerin tahminini ve analizini sağlayan yapılandırılmış bir modelleme yaklaşımı önermektedir. Yöntem, varlıkları kritikliğe göre sınıflandırmayı ve ardından siber güvenlik açıklarını, tehditleri, riskleri, etkileri ve karşı önlemleri analiz etmeyi içermektedir.
13	Weaver G.A., Feddersen B., Marla L., Wei D., Rose A., Moer M.V., 2022	Deniz taşımacılığı liman operasyonlarını etkileyen siber saldırıların ekonomik etkisi ele alınarak, liman bilgi teknolojisi ile operasyonel teknoloji sistemleri arasındaki etkileşimlerin risk değerlendirmeleri yapılmaktadır.	Deneysel tasarım	Deniz Taşımacılığı Sistemi, hacim olarak küresel mal ticaretinin %80'inden fazlasını oluşturmaktadır. Nakliye limanlarını etkileyen son siber saldırılardan dolayı, limanların otomasyona ve gelişmiş lojistik teknolojilerine yatırım yaparak artan rekabet gücü ve daha yüksek risk arasındaki dengeleri anlaması gerekmektedir
14	ASELSAN A.Ş. Bilgi Yönetimi Direktörlüğü, 2022	Çalışma, tedarik zinciri saldırılarının hedef ve etkilerini sunmuştur.	Rapor (Döküman) incelemesi	TZ siber saldırılarında, ilk saldırı, bir veya daha fazla tedarikçiyi hedeflerken ikinci saldırı, müşterilerin varlıklarını hedef alır. Müşterilerin tedarikçilere güvenmesi sebebiyle bu tür saldırıların tespit edilmesi zordur. Tek bir tedarikçiye yapılan saldırının tetiklediği zincirleme reaksiyon bütün bir sağlayıcı ağını tehlikeye atmaktadır. TZ saldırı örneği; Kaseya saldırısı: Kaseya şirketi, bilişim hizmetiyle uğraşan firmalara yazılım tedarik etmektedir. Şirketin yazılımlarına yetkisiz erişim sağlayan saldırganlar, müşterilerin bilgisayarlarına fidye yazılımı yüklemek için bu erişimden yararlanmıştır.

15	Sayın A.A., 2017	Çalışmada, lojistik tehditlerinin kontrolü ve faydalanılan bilişim sistemleri irdelenmiştir. Perakende sektöründe hizmet veren bir işletmede, lojistikte kullanılan bilişim sistemleri bu çerçevede değerlendirilmiştir.	Nitel araştırma	Çalışmada, lojistik sistemlerin etkili şekilde idare edilebilmesi için yönetim bilgi sistemlerine önem verilmesi ve risk yönetimi kavramına yoğunlaşılması gerektiği belirtilmiştir. Lojistik tehditlerinin kontrolü kavramı ve faydalanılan bilişim teknolojileri irdelenmiştir. Perakende iş alanında çalışan büyük ölçekli bir firmada lojistikte kullanılan bilişim sistemleri incelenmiştir.
16	Azimli M., 2013	Çalışmada, firmaların rekabet edebilmeleri için tedarik zincirlerinde bilişim sistemlerine ve bilgi güvenliklerini güçlendirmeleri gerektiği ifade edilmiştir.	Nitel araştırma	Firmaların rekabet için tedarik zincirlerini güçlendirmeleri gerektiği belirtilerek, bilişim sistemleri irdelenmiştir. Gelişme için firmaların TZ de bilişim sistemleri yanında iş süreçlerini ve bilgi güvenliğini de güçlendirmeleri gerektiği belirtilmiştir.
17	Elhabashy A.E., WellsJaime L.J., Camelio A., 2019	Çalışma, imalatta siber-fiziksel güvenlik çalışmalarına ilişkin bir literatür taraması sunmaktadır.	Literatür araştırması	İnternet teknolojisindeki en son gelişmelerle birlikte, siber-fiziksel saldırılar, üretim de içinde olmak üzere değişik sanayi alanlarında sıkça gerçekleşir hale gelmiştir. İmalattaki bu nitelikteki saldırılar, ekipmanın tahrip edilmesini, ürün tasarımlarının veya imalat süreçlerinin değiştirilmesini içerebilir. Makalede, siber-fiziksel saldırıların farklı alanlarda yaygınlığını ve imalatta etkilerinin tespit edilmesinin önemini irdeleyerek, siber-fiziksel güvenlik çalışmalarına ilişkin literatür taraması sunulmaktadır. Bu literatür taramasının, bu alandaki araştırmaların mevcut durumunu belirlemeye ve gelecekteki araştırma alanlarını vurgulamaya olanak tanıyacağı belirtilmiştir.

Tablo 6 incelendiğinde, güncel akademik çalışmalarda, dijitalleşmenin etkisi ile, tedarik zincirlerinde bilgi güvenliğinin ciddi bir problem olarak devam ettiğinin ifade edildiği görülmektedir.

> Kritik bilgi sistemleri gerekli olduğu şekilde korunmaz ise, her liman veya geminin siber saldırı riski taşıdığına ilişkin net kanıtlar bulunmaktadır. Güçlü bir siber koruma sağlamanın önemli bir yolu, farkındalığı desteklemek, siber tehditlere yönelik çözümleri daha da güçlü hale getirmek için hukuki bir çerçeve metodolijisi oluşturmaktır. Ayrıca, yeni siber saldırıların ayrıntıları ve etkisi, tedarik zinciri boyunca bilgi için iletilmelidir (Farah, Ukwandu,Hindy, Brosset, Bures, Andonovic, ve Bellekens, 2022, s. 26).

Kaspersky, merkezi Rusya'da olan bir güvenlik firmasıdır. Kaspersky'nin araştırmacıları, 2023 yılı siber saldırı öngörülerinde; "*Tarım, ulaştırma ve lojistik sektörleri, ilaç ve sağlık malzeme tedarikçileri, alternatif enerji iş alanları ve yüksek teknoloji üreticilerinin, 2023 senesinde daha fazla siber saldırıya uğramasının beklendiğini"* ifade etmişlerdir (Yılmaz, 2022). Lojistik sektörünün saldırılardan daha fazla etkilenecek sektörler arasında sayılmış olması oldukça önemli ve endişe vericidir. Çünkü yaşam için gereksinim duyulan ihtiyaçların giderilmesi lojistik faaliyetler ile mümkündür. Zincirde yaşanacak bir kopukluk mal ve hizmet tedarikinde büyük sorunlar yaşanmasına sebep olacaktır.

> İnternet tabanlı teknolojilerin benimsenmesi, lojistik ortamındaki saldırı yüzeyini artırmıştır. Makale, lojistik ve tedarik ağının idaresinde siber güvenliği artıran önlemler üzerine yapılan çalışmaları gözden geçirmektedir. Bulgular şunlardır: (1) Lojistik, tedarik zincirlerinde önemli bir rol oynamasına rağmen, lojistikte siber güvenliğe odaklanan çalışmalar azdır;…(3) Veri güvenliği ve dijital adli araştırma ile ilgili çalışmalar azdır (Cheung, Bell ve Bhattacharjya, 2021, s. 1).

1.3 Amaç

Bilgiler, günümüzde farklı nedenlerle ve bazı durumlarda yasal düzenlemeler gereği, örneğin e-fatura gibi, çoğunlukla dijital ortamlarda saklanmaktadır. Ticari sırlar ve kişisel

verilerin saklanmasında teknoloji büyük bir kolaylık sağlamaktadır. Ancak bu kolaylık, yetkisiz kişiler tarafından izinsiz olarak verilere erişim riskini de beraberinde getirmektedir. Bu nedenle, işletmeler için büyük ekonomik değer ve öneme sahip olan verilerin tüm yönleri ile korunması gerekir.

Lojistik sektöründe bilişim sistemlerinden yoğun olarak faydalanılmaktadır. Mal sevkiyatı, teslimat, mal hareketlerinin planlanması, tahsilat ve fatura işlemleri, müşteri ilişkileri gibi işlemler bilişim sistemlerinden faydanılarak yapılmaktadır. Lojistik hizmetlerin hızlı ve doğru şekilde yapılabilmesi için bilgi akışının kesintisiz sürdürülmesi gerekir. Süreç içinde bu akışın korunması, bilginin doğru kaynaktan, doğru şekilde, doğru maliyetle ve zamanında temin edilmesi önemlidir. Ufak bir aksaklık dahi tüm sistemi etkileyerek zarara sebep olabilecektir. Sistemdeki aksaklık yanlış bilgi verme, yanlış kayıt açma şeklinde olabileceği gibi dışarıdan ya da şirket içinden verilere yapılacak müdahale ile de olabilir. İşte bu noktada verilerin korunması konusunda gerekli tedbirlerin tüm yönleri ile alınıp alınmadığı sorusu oluşacaktır.

Lojistik sektörüne ilişkin olarak yapılan literatür araştırmasında, bilgi güvenliği ile ilgili olarak değişik kapsamlarda akademik çalışma yapıldığı görülmüştür. Ancak, bilgi güvenliği politikaları üzerine literatürde sınırlı sayıda bilimsel çalışmaya ulaşılmıştır. Diğer taraftan çalışmalarda, bilgi güvenliğinin sadece teknik bir konu olmadığı teknolojik, eğitimsel, yönetimsel, kanun ve yaptırımlar gibi çeşitli boyutları bulunan bir disiplin olduğu da ifade edilmiştir. Bilgi güvenliği için yasal düzenlemeler ve hukukun öneminden bahsedilmiştir. Ancak önemine rağmen bilgi güvenliği konusunu hukuki açıdan ele alan bir çalışmaya rastlanılmamıştır.

O sebeple bu çalışmada, bilgi güvenliği hukuki boyutu ile ele alınarak, bilgilerin korunmasına yönelik yasal düzenlemeler kapsamında değerlendirilmek suretiyle literatüre katkı sağlanması hedeflenmiştir. Bilişim sistemlerinin yoğun olarak kullanıldığı, verinin değişik türde ve şekilde kayıt altına alındığı ve doğru bilginin zamanında ve kesintisiz ulaştırılmasının son derece önemli olduğu lojistik sektöründe yapılan bu çalışmanın diğer kuruluşlar için de yol gösterici katkılar sağlayacağı düşünülmektedir.

Bu temel amaçtan hareketle çalışmada;

1- Kişisel veriler ile tüzel kişi verilerinin korunmasına dair ulusal ve uluslararası yasal düzenlemeler ile Yargıtay kararları ve Kişisel Verileri Koruma Kurulu kararlarının incelenmesi ve verilerin güvenliği çerçevesinde değerlendirilmesi ile ayrıca, bilgi güvenliğine ilişkin uluslararası ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardları, Kişisel Verilerin Korunması Kanunu düzenlemeleri ve lojistik işletmelere uygulanan anket sonuçlarından yararlanılarak, lojistik işletmeler için öneri olarak, bir model münferit bilgi güvenliği politikası oluşturulması,

2- Ayrıca, araştırma kapsamında, Türkiye Ulaştırma Politika Belgesinin "Veri (Bilgi)" başlıklı bölümünde yer alan siber güvenliğin sağlanmasına yönelik düzenlemelerin Lojistik Sektörü için uygun ve yeterli olup olmadığı hususunun değerlendirilmesi amaçlanmıştır.

Anket çalışması ile, lojistik işletmelerde bilgi güvenliği uygulamalarının tespiti amaçlandığından bu doğrultuda hazırlanan 9 adet hipotez aşağıda sunulmuştur.

Araştırma hipotezleri;

H1: Mali Durum, ISO 27001 Belgesi Sahibi Olunmasında Etkilidir.

H2: ISO 27001 Belgesi Sahibi Firmalar, Tedarikçi ve Müşterilerinin de ISO 27001 Belgesine Sahip Olmasının Öneminin Farkındadırlar.

H3: Eğitim, Veri İhlalleri Konusunda Farkındalık Oluşumunda Etkilidir.

H4: Bilgi Güvenliğine Harcama Yapan Firmalar, Veri İhlali Etkilerinin Farkındadırlar.

H5: Mali Durum, Bilgi Güvenliğine Yönelik Harcama Yapılmasında Etkilidir.

H6: Veri Güvenliğinden Yasal Sorumlu Olunduğunun Farkında Olunması, Veri Güvenliğinin Korunmasına Yönelik Önlem Alınmasında Etkilidir.

H7: Veri Güvenliğinden Yasal Sorumlu Olunduğunun Farkında Olunması, Bilgi Güvenliğine Bütçe Ayrılmasında Etkilidir.

H8: Bilgi Güvenliğinden Sorumlu Komisyon Kurulmuş Olması, Verilere İlişkin Prosedür ve Politikaların Oluşturulmasında Etkilidir.

H9: Şirket Personeline Bilgi Güvenliğine İlişkin Eğitim Veren Firmalar, Personel Sözleşmelerine Bilgi Güvenliği, Sır Saklama Yükümlülüğüne İlişkin Hüküm Koyulması Gerektiğinin Farkındadırlar.

1.4 Önem

Devletler, şirketler, bireyler ve kurumlar faaliyetlerini devam ettirebilmek, varlığını sürdürebilmek için bilgiye ihtiyaç duyarlar. Bilgiye gerekli olduğu anda ulaşılabilmesi için bilgi sistemlerine gereksinim vardır. Bu sistemlerin güvenliği, uluslararası boyutta tüm kuruluşların önemle üzerinde durduğu ciddi ve kritik bir konudur (Avci ve Karataş, 2017).

Bilgi güvenliği, fiziksel ya da dijital ortamlarda işlenen tüm verilerin izinsiz kullanımı, ifşası, değiştirilmesi ve yetkisiz erişimlerin önlenmesi amacıyla geliştirilmiş ve sürekli güncellenen bir koruma sistemidir. Verilerin izinsiz kullanımını önlemek için güvenlik tedbirlerini almak hem gerekli hem de zorunludur.

Türk Ticaret Kanunu 18/2'nci maddesi;

"Her tacirin, ticaretine ait bütün faaliyetlerinde basiretli bir iş adamı gibi hareket etmesi gerekir" (Türk Ticaret Kanunu, 2011, s. 10979)*'* düzenlemesine ve 6698 sayılı Kişisel Verilerin Korunması Kanunu 12/1-a,b,c'inci maddesinde; "*Veri sorumlusu (tüzel ya da gerçek kişi) kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemek, muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır*" (Kişisel Verilerin Korunması Kanunu, 2016, s. 12305) düzenlemesine yer verilerek, veri sorumlularının işledikleri verileri korumakla yükümlü oldukları, tedbir almalarının zorunlu olduğu açıkça belirtilmiştir.

Bilgi teknolojileri lojistik şirketlere birçok açıdan fayda sağlar. Rekabet ve maliyet üstünlüğü yanında şirketlerin performansını da arttıran bir yönü bulunmaktadır. Firmalara sağladığı avantajlar ile birlikte güvenlik sorunlarına da sebep olmaktadır. Lojistik bilgi sistemlerine bağlı işlemlerde ve sistemlere yönelik siber saldırılar, veri ihlalleri, hırsızlık, veriyi silme ve başkaca türdeki saldırılar bilgi kaynaklarının kaybı ile sonuçlandığından bilgi sistemlerinin güvenliği sorunu öne çıkmaktadır (Avci ve Karataş, 2017).

Dünyada yaşanan siber saldırı örneklerinde çok sayıda üretici ve lojistik işletme saldırıya maruz kalarak zarara uğramıştır: Fransa tren taşımacılığı şirketi SNCF, Hollanda merkezli kargo şirketi TNT, Danimarka taşımacılık şirketi Moller-Maersk, İspanyol yiyecek şirketi Mondelez ve ABD'den ilaç şirketi Merck sayılmıştır (Lojiport Teknoloji , 2017).

Değişik tarihlerde bazı ülkelerin hava limanları siber saldırılara maruz kalmıştır. 2023 yılında Almanya'nın Dortmund, Nürnberg ve Düsseldorf havalimanları web siteleri siber saldırıya uğramıştır. Siteye erişim sağlanamamış ve olayla ilgili inceleme başlatılmıştır (Airway Post, 2023). Yaşanan olay havayolu taşımacılığını engelleme saldırısıdır. Saldırı süresince sistemlere ve bilgiye zamanında erişim imkanı olmadığından iş süreçleri aksamıştır.

Bir ülkenin kalkınmışlık düzeyini anlamaya yardımcı olan en önemli ölçüt kriteri ekonomik göstergelerdir. Ekonomik göstergelerin değişiminde lojistik önemli rol oynayan araçlardan birisidir. Ülkelerin dış ticarete yönelimlerinin artmış olması ve bu işlemlerin karmaşık bir hal alması lojistiğin önemini arttırmıştır (Duran ve Türkoğlu, 2019).

Lojistik, taşımacılık ve depolama dışında birçok farklı işlevi barındıran bir sektördür. Ürünlerin taşınma ve depolama süreçlerini tedarik zinciri boyunca etkili bir şekilde yönetmek, işin özünü oluşturur. Bu da ancak bilginin elde edilmesi, işlenerek bir karara bağlanması ile mümkündür. Bundan dolayı, lojistik sürecinde, bilginin doğru zamanda, doğru kaynaktan, doğru şekilde, doğru bilgi olarak ve uygun maliyetle elde edilmesi büyük önem taşır. Bilgi, değerli bir varlık olarak kabul edildiğinden korunması gereklidir (Yıldıztekin, 2012).

2020 yılında başlayan pandemi, üretim, ticaret, iş şekilleri, sosyal yaşam gibi her alanda büyük bir değişim yaratmıştır. Salgın, ülkeleri ve sektörleri olumsuz yönde etkilemiş, ilk defa ülke sınırları kapatılmıştır. Salgın ile birlikte, kalabalıklardan uzak, mesafeli yaşam şekilleri oluşmuştur. Bu durum, hayatın içindeki pek çok uygulamanın değişmesine sebep olmuştur. Kalabalıklardan uzak durmak amacıyla, uzaktan eğitim, uzaktan çalışma, uzaktan alışveriş gibi yeni yaşam tarzları oluşmuştur. Lojistik sektörü de bu yeni durumdan fazlasıyla etkilenmiştir.

Pandemi süreci, bir kez daha lojistiğin önemini göstermiştir. Sağlık sektöründe tedarik zincirinin sürdürülebilirliğinden, insanın beslenme, hijyen gibi temel ihtiyaçlarının karşılanmasına kadar lojistik fonksiyonların önemi net bir şekilde anlaşılmıştır (Tanyaş, 2020).

Pandemi döneminde yaşanan değişimlerle birlikte, üreticiler, tedarikçiler ve taşıyıcılar tarafından dijitalleşmenin önemi daha net anlaşılmıştır. Lojistikçiler açısından da, dijital platformlar üzerinden yöneterek taşımak daha da önemli hale gelmiştir (Girgin, 2020).

Diğer taraftan, teknolojik cihaz kullanımının artması, güvenlik önlemi almayan işletmeler için risk oluşturmakta iken, bu duruma bir de küresel salgının eklenmesi ile değişen iş ve yaşam şekilleri ile yeni güvenlik riskleri ortaya çıkmıştır.

Lojistik faaliyetlerin yürütülmesinde yoğun bir veri girişi ve paylaşımı yapılmaktadır. Bilgiler, hem fiziki (manuel) hem de dijital ortamda kayıt altına alınmaktadır. Bilgilerin eksik şekilde paylaşılması örneğin; "gönderim bilgileri eksik verilmiş olursa, sevkiyat zorlaşabileceği gibi, doğru olmayan bir taşıma modu tercih edilebilecektir" bu durum iş süreçlerini aksatacaktır. Kayıt altına alınarak muhafaza edilen bilgilere izinsiz şekilde ulaşılması, izinsiz kullanımı ve paylaşılması da firma itibarını zedeleyerek zarara sebep olacaktır. Ayrıca bu halde, verileri kayıt edilmiş olan üçüncü kişilere karşı hukuki sorumluluk söz konusu olacaktır.

STM teknolojik düşünce merkezinin 2022 Siber Tehdit Durum Raporuna göre;

> Siber suçlar son birkaç yıldır yükseliştedir ve 2025 senesine kadar dünyaya maliyetinin senede 10,5 trilyon dolar olacağı tahmin edilmektedir. Fidye yazılım saldırıları dünya çapında %62 artmıştır(...)Denizciliğin güvenliği ve deniz alanlarının korunması için kritik olan çok sayıda sistemin işletilmesi ve yönetimi için siber güvenlik çok önemli hale gelmiştir.

Tablo 7'de raporun, en çok saldırı gelen ülkeler ve saldırı sayılarına ilişkin sonucu gösterilmektedir. Toplanan veriler incelendiğinde, en çok saldırı gelen ülkenin Almanya olduğu, sonrasında onu, Hindistan, Rusya, ABD ve Türkiye'nin takip ettiği görülmektedir (STM Mühendislik , 2022, s. 5,10,23).

Tablo 7. Saldırı Gelen Ülkeler ve Saldırı Sayıları (STM Mühendislik , 2022)

Saldırının Geldiği Ülke	Saldırı Sayısı
Almanya	451.319
Hindistan	423.026
Rusya	345.961
ABD	322.576
Türkiye	278.855
Çin	271.227
Hollanda	174.696
Vietnam	145.992
Moldova	84.079
Tayland	57.000

STM teknolojik düşünce merkezinin 2023 tarihli Siber Tehdit Durum Raporunda da, "*Organizasyonlar, tedarik zinciri süreçlerindeki siber risklere karşı önlemler alarak, siber güvenliklerini güçlendirmeye ve iş sürekliliğini sağlamaya odaklanmalıdır… Günümüzde her organizasyon başka organizasyonların hizmetlerine ihtiyaç duymaktadır(…).Yaşayabilecekleri zafiyetler doğrudan hizmet verdikleri organizasyonu etkileyecektir, gerekli tedbirleri almaları elzemdir"* şeklindeki tespitlere yer verilmiştir (STM Mühendislik , 2023, s. 5). Raporlar siber risklerin artarak devam edeceğini, büyük zararlar oluşturacağını ortaya koymaktadır. Ayrıca, günümüzde her bir organizasyon diğer firmaların hizmetine ihtiyaç duymaktadır. Bir firmada ki güvenlik zaafiyeti diğer firmayı da etkileyebileceğinden, alınacak bilgi güvenliği tedbirleri karşılıklı bilgi paylaşımında bulunan firmaların tamamı için fayda sağlayacaktır.

Bilgi güvenliği doğası gereği, varlıkları ortaya koymak, riskleri ve tehditleri tespit etmek, gerekli önlemleri hem gerçek ortamlarında almak hem de yazılı belgeler ile bunları somutlaştırmak durumundadır. Doğal olarak bu süreçlerin tamamının yürürlükteki yasal düzenlemeler ile de uyumlu olması gereklidir. Bunun sağlanması için de dengeli bir politika hazırlanmalı ve tüm çalışanlar ile paylaşılmalıdır. Yeni kanunlar ve yönetmelikler çıkarıldıkça bilgi güvenliğinin de buna uyum sağlaması gerekecektir (Evrin ve Demirer, 2011). Saldırının hedefi ve çeşidi ne olursa olsun mevzuat ile de

uyumlu yeterli koruma tedbiri alınmadığı sürece kayıt edilen bilgiler risk altında olacaktır.

Günümüzde, tedarik zinciri ve lojistiği siber ve veri güvenliği risklerinden korumak artık sadece bir bilgi teknolojisi çalışanı işlevi değildir. Her kurumsal çalışanın veri koruma sürecinde bir sorumluluğu vardır. İleriyi görebilen işletmeler, çalışanlarını, bilgi ve siber güvenlik sürecinde etkin bir görev üstlenmeye yönlendiren yöntem, politika ve yaklaşımlar oluşturabilen kuruluşlardır (Burrell, Bhargava, Swanson, Harmon, Wrigh, Springs ve Dawson, 2020).

Veri ihlali yalnızca dışarıdan gelen siber saldırılardan kaynaklanmamaktadır. Çoğu zaman tehdit şirket içinden gelmektedir. Bilgi güvenliğinin ihlali ile ilgili bilgi sızdırma, rekabet ihlali, rakip firma çalışanları ile bilgi paylaşımı gibi çeşitli ihtilaflar mevcuttur. Bazen de şirketler çeşitli sebeplerle sorunu mahkemeye intikal ettirmeksizin şirket içinde çözme yolunu tercih etmektedir.

Tüm bu hususlar gereğince, lojistik sektöründe kayıt altına alınan ve paylaşılan veri tür ve sayısı ile çalışan kişi sayısının fazlalığı, veri paylaşımı yapılan aktörlerin fazla sayı ve çeşitte olması (müşteri, tedarikçi, üçüncü kişiler, personel gibi) dolayısı ile verilen hizmetin devamı için, bilgi paylaşımının kesintisiz sürdürülmesi önemlidir. Bu sebeple, bilginin korunması ve güvenliğinin sağlanmasına ihtiyaç vardır.

Anayasa Mahkemesi'nin 2017/16 Esas 2019/64 Karar numaralı, 24 Temmuz 2019 tarihli kararında, günümüzde bilgi ve iletişim konularında gelişmeler yaşandığı, bu ilerleme ile birlikte tehdit ve siber saldırıların arttığı ve bundan dolayı siber güvenlik gereksiminin oluştuğu belirtilmiştir. Devletin, bireylerin güven içinde yaşamasını sağlamak görevi karşısında siber güvenliğin sağlanmasının da bu görevlerden birisi olduğu ifade edilmiştir. Dolayısı ile siber saldırılara karşı güvenliğin sağlanmasının, kamunun güvenliğinin korunmasına yönelik olacağı belirtilmiştir (Anayasa Mahkemesi Kararı, 2019).

2020 tarihli, Ulaştırma ve Altyapı Bakanlığı'nca hazırlanan 'Türkiye Ulaştırma Politika Belgesi'nin 'Veri (Bilgi)' başlıklı bölümünde siber güvenlik konularına yer verilerek belgede:

> Siber güvenliğin sağlanması ve riskler ile mücadele için…farkındalığın artırılacağı, konuya ilişkin eğitimler düzenlenerek bu eğitimlerin teknik bilgiler ile birlikte olayı bir bütün olarak görülmesini sağlayan politik, ekonomik, idari, hukuki ve sosyal kısımları da içerek şekilde oluşturulmasının sağlanacağı…Ülkemizde üretilen ulaştırma ve haberleşme verilerinin, uluslararası arenada kabul görmüş güvenlik standardları ve gereksinimlerini karşılayacak şekilde üretimi, iletimi, saklanması, ve paylaşımının yapılacağı belirtilmiştir (T.C. Ulaştırma ve Altyapı Bakanlığı, 2020b, s. 10-11).

Ulusal Eylem Planları hazırlık toplantılarına Üniversite temsilcileri de davet edilmiş ve görüşleri alınarak eylem planlarında birlikte çalışma esasları belirlenmiştir. Eylem Plan'larında, "*Üniversitelerde siber güvenlik eğitimlerinin yaygınlaştırılması, siber güvenlik alanında, Türkçe kitap, makale, dergi kaynaklarının çoğaltılması"* ifade edilmiştir(T.C.Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013, s. 38), (T.C.Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, s. 6).

Yapılan araştırmalar, tüm kuruluşların bilgi güvenliğini sağlamak için harekete geçmesi gerektiğini ortaya koymaktadır. Şirketlerin kayıt altına alarak sakladıkları verilerin korunabilmesi için bilgi güvenliğinin tüm boyutları ile ele alınarak prosedür ve politikalar oluşturulması, tüm şirket nezdinde uygulanması, denetlenmesi, gerekli hallerde güncellenerek sürecin devam ettirilmesi gerekmektedir. Bu çalışmanın sonucunda;

- Kişisel ve tüzel kişi verilerinin korunmasına ilişkin ulusal ve uluslararası yasal düzenlemeler ile yargı ve kurul kararlarının incelenmesi ve değerlendirilmesi ile bilgi güvenliği konusu hukuki boyutu ile incelenecektir.

-Bilgi güvenliğine ilişkin uluslararası ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardları ile Kişisel Verilerin Korunması Kanunu düzenlemelerinin karşılaştırması ve analizi yapılacaktır.

-Lojistik işletmelerin bilgi güvenliği uygulama ve farkındalıklarının belirlenmesi için anket çalışması yapılarak sonuçlar değerlendirilecektir.

-Tüm bu inceleme ve lojistik işletmelere uygulanacak anket sonuçlarından yararlanılarak, lojistik işletmeler için öneri olarak, bir model münferit bilgi güvenliği politikası oluşturulacaktır.

-Araştırma kapsamında, Türkiye Ulaştırma Politika Belgesinin "Veri (Bilgi)" başlıklı bölümünde yer alan siber güvenliğin sağlanmasına yönelik düzenlemelerin Lojistik Sektörü için uygun ve yeterli olup olmadığı hususu değerlendirilecektir.

-Bu akademik çalışma ile, firmalar nezdinde bilgi güvenliği konusunda hukuki farkındalık ve yetkinlik oluşturulması mümkün olabilecektir. Çalışmanın konusu ile ilgili sonuç ve öneriler, diğer araştırmacıların konuyla ilgili olarak daha fazla araştırma yapmak üzere bulgulardan faydalanmasına yardımcı olabilecektir.

1.5 Varsayımlar

Literatür çalışmasında, Science Direct, Scopus, Google Scholar, Web of Science ve YÖK Ulusal Tez Merkezi veri tabanlarında 2005-2020 yılları arasındaki kaynaklar taranmıştır. Literatür taraması ilk olarak Aralık 2019'da yapılmıştır. Temmuz 2020'de yeni araştırmalar dahil edilmek üzere tekrarlanmıştır. Dijitalleşme ile birlikte bilgi güvenliği konusunun daha da önemli hale geldiği, sektörde araştırmaların artış eğiliminde olduğu görülmüştür. Literatür araştırması tez izlemeler sürecinde de (2021-2024) tekrarlanmıştır. Ancak buna karşın, bazı yeni araştırma çalışmalarının gözden kaçırılmış olması mümkündür.

Araştırma kapsamında lojistik işletmeler ile yapılan anket çalışmasında katılımcıların bütün sorulara samimiyetle, doğru bir şekilde ve eksiksiz olarak cevap verdikleri ve yapılacak araştırmayla aydınlatılması gereken konular tespit edilirken de, elde edilen çalışmaların bu alandaki çalışmaları kapsadığı varsayılmıştır.

1.6 Sınırlılıklar

Ülkemizde, lojistik sektöründeki şirketlerin sayısı yetki belgesi almamış olanlar sebebiyle net olarak bilinmemektedir. Ülkemiz genelindeki dağılıma bakıldığında sektör Marmara bölgesinde yoğunlaşmıştır. Kayıtlı yaklaşık 4.700 civarında uluslararası karayolu taşımacılık yetki belgesi bulunan firmanın yaklaşık 1.000 tanesi İstanbul ve

çevresindedir. Yurtiçi taşımacılık yetki belgeli yaklaşık 313 bin firmanın 105 bin tanesi İstanbul bölgesindedir. Uluslararası Nakliyeciler Derneği'ne kayıtlı 1.079 adet üyenin 306 tanesi İstanbul'da, Uluslararası Taşımacılık ve Lojistik Hizmet Üretenleri Derneğine bağlı 447 adet lojistik firmanın 363 tanesinin merkezi İstanbul'da bulunmaktadır (T.C.Kalkınma Bakanlığı, 2018). Diğer taraftan, söz konusu lojistik derneklerine üye firmalar incelendiğinde, aynı firmaların birden fazla lojistik derneğine üye oldukları belirlenmiştir. Bu durumda dernek üye sayıları dikkate alınarak tam bir sayı belirlemek mümkün olmamaktadır. Bu da çalışma başlangıcında bir sınırlılık oluşturmuştur.

Lojistik işletmelerine uygulanacak anket çalışmasında firmalara ulaşmak ve ankete yanıt almak zor olabilir, kısıtlı sayıda katılımcı ile anket uygulaması yapma zorunluluğu olabilir. Anket çalışmasının bitirilmesi zaman alabilir, beklenmedik sorunlarla karşılaşılabilir.

Araştırma, yasal düzenlemeler, literatür araştırması, yargı ve kurul kararları, ISO 27001 bilgi güvenliği standardları ve lojistik işletmelerin bilgi güvenliği uygulama ve farkındalıklarını belirlemek üzere yapılan anket aracılığıyla toplanan veriler ile sınırlıdır.

Anket bulgularında, 'Fikrim Yok' cevapları, yanıtlayan kişinin konuyla ilgili bilgisi olmadığını ifade etmektedir. Bu cevap, ne evet ne de hayır olarak kabul edilmiştir. Dolayısıyla ilgili sorunun yanıtı normalde lojistik şirket bazında olumlu veya olumsuz olmasına rağmen kişinin bu durumu bilmemesinden kaynaklanan bir yanıt verdiği kabul edilmiştir.

Yargıtay kararları incelemesinde ticari davalara ilişkin yargı kararları (ticari sırrın ifşası hariç) kapsam dışı bırakılmıştır.

Veri sahibi olarak, veri üzerinde hak sahibi olan devlet gibi diğer unsurlar çalışma kapsamı dışında tutulmuştur.

Araştırmaya ayrılan zaman ve bütçe kısıtlıdır. Araştırmacı araştırmayı tek başına yürütecektir.

1.7 Tanımlar

Bilgi Güvenliği: Bilgi güvenliği, bir varlık olarak ele alındığında bilginin, oluşabilecek zararlardan korunması, doğru teknolojinin, doğru amaçlarla ve doğru bir şekilde kullanılarak bilgiye yetkisiz kişiler tarafından her ortamda ulaşılmasının önlenmesi olarak tanımlanır (Aktaş, 2020)

Ticari Sır: Bir şirketin rakiplerine karşı ekonomik avantaj elde etmesini sağlayan bilgi bütünüdür. Formül, tasarım, yasal araç ya da örüntü biçiminde olabilir. Ticari sırlar bazı hukuk sistemlerinde "gizli bilgi" ya da "sınıflandırılmış bilgi" olarak adlandırılmaktadır (Vikipedi, 2020a).

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi (Kişisel Verilerin Korunması Kanunu, 2016).

Veri Sorumluları Sicili (VERBİS): Kişisel verileri işleyen gerçek ve tüzel kişilerin kayıt yaptırdığı ve veri işleme faaliyetleri ile ilgili bilgileri beyan ettikleri bir kayıt sistemidir.

Lojistik: Tedarik Zinciri Yönetimi Profesyonelleri Konseyi (CSCMP,Counsul of supply chain management professionals) tarafından yapılan tanım; "Müşteri gereksinimlerini karşılamak üzere, üretim ve tüketim yerleri arasındaki hizmet, eşya ve ilgili bilgilerin ileri ve geri yöndeki akışları ile depolanmalarının etkin ve verimli bir şekilde plânlanması, uygulanması ve kontrolünü içeren tedârik zinciri süreci aşamasıdır" şeklindedir (Tanyaş, t.y.).

Genel Veri Koruma Tüzüğü (GDPR): AB hukuk sisteminde, Avrupa Ekonomik Alanı ve Avrupa Birliği içerisindeki bireylerin bilgilerini koruma ve gizliliğini düzenleyen bir tüzüktür. Düzenleme öncelikli olarak, bireylerin kendi kişisel verilerini kontrol etmelerini sağlamak ve AB içindeki firmaların bu düzenlemelerle uyumlu olmasını hedeflemektedir (Vikipedi, 2020b).

Siber Saldırı: Bir birey veya kuruluşun "bilgileri çalmak, ifşa etmek, değiştirmek, devre dışı bırakmak veya ortadan kaldırmak ya da bilgisayar bilgi sistemlerine, bilgisayar ağlarına ve bilgisayar altyapılarına sızmak için bir veya daha fazla bilgisayar ve bilgisayar sistemi kullanma" girişimidir (Vikipedi, 2020c).

Bilgi Güvenliği Standardları: ISO/IEC 27001 bilgi güvenliği alanında dünya genelinde yaygın olarak kullanılan uluslararası standartlardan biridir. Söz konusu standart, kuruluşların, bilgi güvenliğinin en temel gereksinimleri olan “gizlilik”, “bütünlük” ve “erişilebilirlik” ilkelerini sağlamasını amaçlamaktadır (BTK, 2020).

2. GENEL BİLGİLER

2.1 Veri, Enformasyon ve Bilgi

Bilgi, insan aklının kavrayabileceği gerçekler, olgular ve ilkeler bütünü olarak tanımlanır. Ayrıca bilgi, belirli bir konu veya iş hakkında edinilen veya aktarılanlar olarak da açıklanabilir. Bilişim sistemlerinde, bilgi işlenir, depolanarak iletilebilir, değiştirilebileceği gibi, silinme ya da anonimleştirme yapılabilir, o sebeple bilişim sistemleri en önemli yerdir. Veriler birleşerek bilgiyi meydana getirir. Bilgi, verinin işlenmiş halidir (Çek, 2017). Verilerin işlenmesiyle enformasyon oluşur. Bu sebeple enformasyon, bireylerin zihinsel yapısında fark yaratabilecek veri olarak da tanımlanmaktadır (Henkoğlu, 2015).

2.2 Bilgi Güvenliği

Bilgi güvenliği geniş kapsamlı bir konudur. Fiziksel koşulların oluşturulması, haberleşme ortamlarının korunması, şirket kültürünün oluşturulması gibi, tümü bu kapsam içindedir. Bu geniş yelpazede en önemli ve değişmeyen unsur korunacak olan bilgidir (Henkoğlu, 2015).

TS ISO/IEC 27001:2005; "*Bilgi, bir kurumun en önemli değerlerinden birisidir ve sürekli korunması gerekir."* Günümüz koşullarında, veri güvenliğinin sağlanması ihtiyacı gün geçtikçe artmaktadır. Değişen çalışma ortamları, bilginin biçimini değiştirdiği gibi bilginin çeşitli zayıflıklardan ve tehditlerden etkilenmesi olasılığını da artırmıştır. Bilgi, saklanma biçimlerine göre aşağıdaki gibi sınıflandırılabilir;

- Yazılı olarak (sözleşmeler, faturalar, kıymetli belgeler vb) tüm belgelerde
- Elektronik ortamlarda (sunucularda, ortak alanlarda, bilgisayarlarda, usb belleklerde vb)
- Sözlü olarak (telefon konuşmalarında vb.), e-posta veya posta olarak taşınabilir ortamlarda
- Çalışanların hafızalarında (şifreler, ticari bilgiler vb). Hızla değişen teknolojiyle bu biçimlerden bazıları sonlanabileceği gibi aralarına yenileri de eklenebilir. Sürekli

devam eden değişim ve gelişimden dolayı bilgi güvenliğinin tekrar ve tekrar sorgulanması ve kontrol edilmesi gerekmektedir (Can, 2012).

Saklama ve depolama biçimleri farklılık göstersede, şirketlerin, bilgi varlıklarını koruma gerekliliği hem bir ihtiyaçtır hem de yasal bir yükümlülüktür. Ayrıca, şirketlerin müşterilerine güven sağlama, rakipleriyle rekabet edebilme ve piyasada ticari itibarlarını koruma gereklilikleri bulunmaktadır.

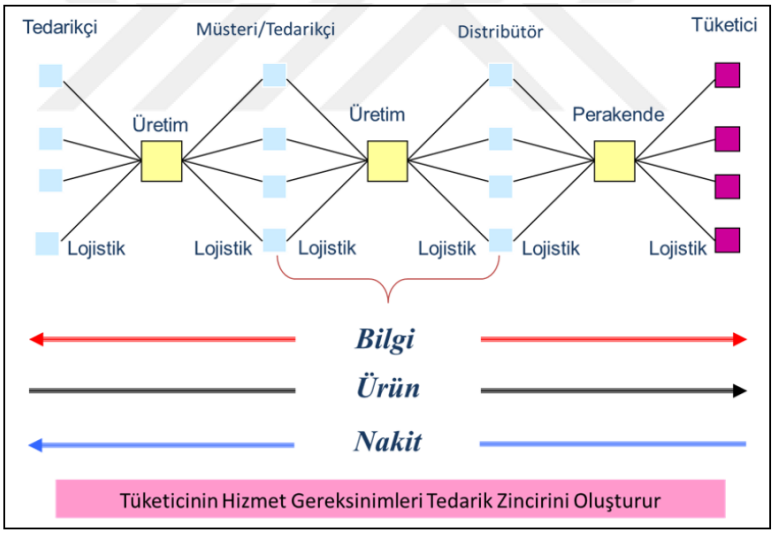
2.3 Tedarik Zinciri, Lojistik ve Lojistik Bilgi Sistemleri

2.3.1 Tedarik zinciri ve lojistik

Lojistik terimi için Yunanca "logistikos" (hesaplama yeteneği) ve Fransızca "logistique" (sunmak, askeri alan-konaklama yeri) sözcükleri tarihsel referans terim olarak belirtilmektedir. Lojistik, esas olarak ''logic'' ve ''statistics'' kelimelerinin bir araya gelmesinden ortaya çıkmıştır. Bu sözcükler "istatistiksel mantık"ı belirtmektedir. Böylelikle, askerlerin konaklama yeri, mantık ve hesap sözcüklerinin birleşmesi ile lojistik kelimesi elde edilmiştir. İlk kullanım yeri Silahlı Kuvvetlerdir. 1905 senesinde, "malzeme ve personelin taşıma, tedarik, bakım ve yenilenmesi" olarak askeri bir faaliyeti anlatmak amacıyla, Albay Chauncey B. Baker tarafından kullanıldığı bilinmektedir. Askeri manada lojistik kelimesi, "muharip unsurlara strateji ve taktiğine uygun ve gerekli olan ikmal maddeleri ile hizmet desteğini sağlamak için yapılan faaliyetler" anlamına gelmektedir. Bu kapsamda "orduların erzak ve mühimmat desteğinin düşünülerek hareket ettirilmesi sanatı" olarak öngörülmektedir (Gülenç ve Karagöz, 2008).

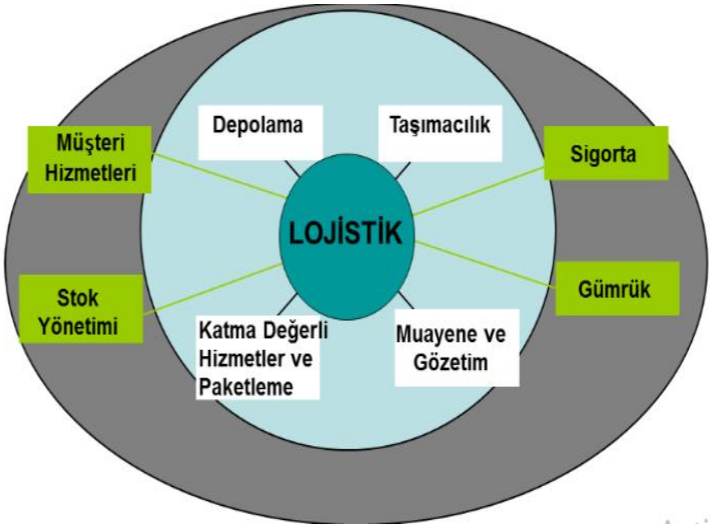
Lojistiğin tanımı konusunda farklı görüşler bulunmaktadır. Tedarik Zinciri Yönetimi Profesyonelleri Konseyi lojistik yönetimini şu şekilde tanımlamaktadır: "*Müşteri gereksinimlerini karşılamak üzere, üretim ve tüketim yerleri arasındaki eşya, hizmet ve ilgili bilgilerin ileri ve geri yöndeki akışları ile depolanmalarının etkin ve verimli bir şekilde planlanması, uygulanması ve kontrolünü içeren tedarik zinciri süreci aşamasıdır"* (T.C. Milli Eğitim Bakanlığı, 2011, s. 7).

Tedarik ise, işletmelerin ihtiyacı olan hammadde ve malzeme, makine teçhizat veya nihai mamullerin sağlanmasıyla ilgili süreç, faaliyet ya da sorumlulukları ifade eder. Tedarik zinciri; "Hammaddelerin temin edilmesinden üretilen nihai ürünün son kullanıcıya ulaştırılması ve tamir, bakım veya ürünün içerdiği zararlı maddelerin yok edilmesine kadar tüm faaliyetlerin, sistemlerin ve kişilerin oluşturduğu bir şebekedir." Tedarik zinciri, dağıtım ve üretim merkezlerinden, tedarikçilerden, perakendecilerden, hammadde ve sistem içerisinde nakledilen son ürünlerden meydana gelir. Tüm bu aktivitelerin bilişim sistemlerinde biçimlendirilerek ekrana aktarılması önemlidir. Bu şekilde tedarik ağının bütün olarak kontrol edilmesi daha kolay olacaktır (Deniz, 2017). Tanımlara göre, lojistik, tedarik zinciri sürecinin bir aşamasıdır. Bu iki kavram arasındaki ilişki Şekil 2'de gösterilmektedir.



Şekil 2. Tedarik Zinciri ve Lojistik İlişkisi (Tanyaş, 2013)

Lojistik ana faaliyetleri nakliye ve depolamadır. Bunlar yanında, gümrük, sigorta, stok idaresi, paketleme, sipariş yönetimi, muayene ve gözetim ile katma değerli hizmetlerden oluşmaktadır. Tedarik zinciri ise, malların sadece bir yerden başka yere taşınması değil, asıl kaynağından tüketildiği yere kadar olan hareketidir (Long, 2016). Temel lojistik faaliyetler Şekil 3'de gösterilmektedir.



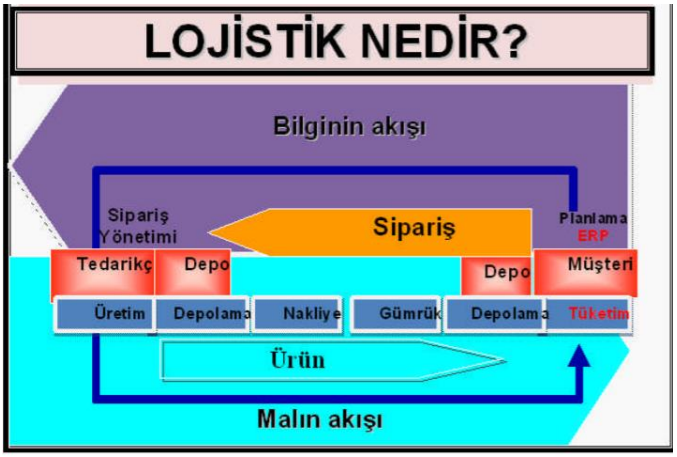
Şekil 3. Temel Lojistik Faaliyetler (Tanyaş, 2013)

Lojistik hizmeti verenler, tedarik zinciri içerisinde bilgi, malzeme ve hizmet akışı sağlayarak, tedarikçi ve müşteri arasında köprü benzeri bir işlev görür.

Ekonomik faaliyetlerin devamı açısından üretim ve ticaret sistemlerinin mutlaka etkin lojistik sistemlerle desteklenmesi gerekir. Bu kapsamda, lojistik hizmetlerin etkinliğinin arttırılması, lojistik maliyetin azaltılması, ticari hayatın geliştirilmesi ve rekabet edebilme kapasitesinin artırılması için özel sektörün desteklenmesi temel amaçtır. Ülkemizin sahip olduğu lojistik güç ve kapasite ile birlikte; bölgenin potansiyeli birlikte değerlendirildiğinde, ayrıca doğu ve batı arasında değişen ticari değişimler ile İpek Yolu' da lojistik pazar gücüne dahil edildiğinde, tüm bunlar, ülkemizin sahip olduğu avantajların büyüklüğünü açıkça ortaya koymaktadır (T.C. Kalkınma Bakanlığı, 2018).

2.3.2 Lojistikte doğru bilginin önemi ve dijitalleşme

Lojistik süreç içinde bilginin, doğru şekilde ve doğru zamanda, geçerli kaynaktan temin edilmesi önemlidir. Şekil 4'de lojistik uygulamalarda bilgi ve mal akışı gösterilmiştir. Sürdürülen her bir işlemde, zincir içerisinde yer alan birimler arasında yoğun bir bilgi paylaşımı söz konusudur. Lojistik işlemler, hammaddenin tedarikçiden temini ile üretim alanına getirilmesi anında başlamakta ve ürünün son kullanıcıya teslimi ve sonrasında da iadeler, geri dönüşüm gibi hareketlerle devam etmektedir. Yoğun hareket, mal, para ve yoğun bir bilgi akışı sözkonusudur.



Şekil 4. Lojistikte Malzeme, Hizmet ve Bilgi Akışı (T.C. Milli Eğitim Bakanlığı, 2011)

Lojistik işlemlerde, hızlı yanıt verme (sipariş ve teslimat arasındaki sürenin kısa tutulması), hizmetin kaliteli şekilde verilmesi önemlidir. Hızlı yanıt için de, doğru bilginin doğru şekilde kesintisiz akışı gerekir.

Pandemi, her ülkeyi ve bir çok sektörü kötü yönde etkilemiştir. Lojistik sektörü de bu süreçten etkilenen iş alanları arasındadır. Bu dönemde sınırların kapatılması ile, devletler arasındaki eşya ve hizmet sunumu yavaşlayarak durma noktasına gelmiştir. Yasaklar sebebi ile sokağa çıkamayanların ihtiyaçlarının karşılanması gerektiğinden, hizmetlerin sunulmasında lojistiğin ne kadar önemli olduğu görülmüştür. En temel ihtiyaçlar dahi internet üzerinden, dijital platform kullanılarak tedarik edilmeye başlanmıştır. Bu durum, geniş çapta veri kaydedilmesi anlamına gelmektedir. Oluşan yeni yaşam şekli ile verilere yönelik risk seviyesi arttığından verilerin korunmasını sağlamak daha da büyük bir önem kazanmaya başlamıştır.

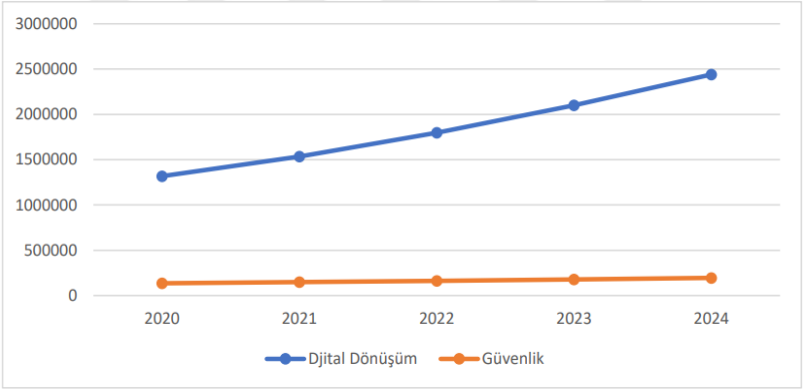
Teknolojinin değişimi ile birlikte şirketler de bu alanda değişimler yaşamaktadır. Dijital dönüşüm, şirketlerin geçirdiği bu değişimlere etkisi olan başlıca unsurlardan birisidir. Androit tarafından 2018 yılında, lojistik ve ulaştırmada dijitalleşme ve tahminler raporu yayınlanmıştır. Raporda, 2018 yılında ulaştırma ve lojistik alanında hizmet veren şirketlerin, 54,92 milyar $ düzeyinde dijital dönüşüme mali kaynak ayırdığı, 2025 yılında bu rakamın 145,28 milyar $ seviyesine yükseleceğinin tahmin edildiği belirtilmiştir. Ayrıca dijitalleşme araçlarının, depo idaresi, akıllı tedarik ve otonom lojistik gibi alanların ilerlemesine önemli katkılar sağlayacağı ifade edilmiştir. Dijitalleşme, tedarik zincirleri için önemlidir, ayrıca müşterilerin talepleri ve beklentilerinin yerine getirilmesi

bakımından gereklidir. Müşteriler, lojistik işletmelerinden hızlı teslimat yapılmasını beklemektedir. Tedarik zincirinde dijital dönüşümü sağlayan şirketler, lojistik hizmetlerin yönetilmesinde hız kazandığı gibi yapılan işleri de kolaylıkla başarma kazanımı elde etmektedir. Böylece müşteri memnuniyeti artarak şirket karı da yükselmektedir (Bilgiç, Türkmenoğlu, ve Koçak, 2020).

Dijital dönüşümün gerekliliği ve zorunluluğu kaçınılmaz bir gerçektir. Yenilikler, bazı sorunları da beraberinde getirmektedir. Müşteri yaşamını ve firmaların hizmet sunumlarını kolaylaştırarak, giderleri azaltan, işleri hızlandıran dijital kullanım sırasında paylaşılan bilgilerin koruma altına alınması gerektiği ortadadır. Aksi takdirde, bilgi olmadan süreçlerin devam ettirilmesi mümkün değildir.

Dünya Ekonomik Forumu 2019 raporunda, önümüzdeki on yıl süresince, lojistik sektöründe dijital dönüşümün odak noktasında beş konu olacağı belirtilmektedir. Bunlar, büyük verinin kullanımı, sürücüsüz tır ve kamyonlar, insansız hava araçları ile teslimat şekilleri gibi konulardır (Bilgiç, Türkmenoğlu ve Koçak, 2020).

Siber güvenliğe yapılan harcamalar ile dijitalleşmeye yapılan harcamalara bakıldığında, dijitalleşme projelerine olan yatırımların yıllar içinde (5 yılda) büyük oranda artacağı, bunun yanında, aynı zaman süresinde, güvenlik harcamalarında ise daha düşük seviyede artış olacağı düşünülmektedir (Zaralı, 2022). Dijital değişim ve güvenlik giderleri arasındaki tahmin durumu Şekil 5'de görülmektedir.



Şekil 5. Dijital dönüşüm ve güvenlik harcamaları 2020 – 2024 tahmini (Zaralı, 2022)

Siber güvenlik harcamalarının dijitalleşmeye yapılan harcamaya oranının artması beklenirken Tablo 8'deki verilerde ise, yıl geçtikçe daha fazla oranda azalacağının öngörüldüğü görülmektedir.

Tablo 8. Dijital Dönüşüm ile Siber Güvenlik Harcamalarının Yüzdesel Oranları (Zaralı, 2022)

Yatırım/Yıl	2020	2021	2022	2023	2024
Dijital Dönüşüm	$1,317,540	$1,533,959	$1,796,831	$2,099,149	$2,440,097
Güvenlik	$134,860	$148,330	$162,712	$178,063	$194,463
DD/G % Oranı	10.24	9.67	9.06	8.48	7.97

Küreselleşme ve teknolojide yaşanan yenilikler, dünya genelinde pek çok sistemi birbirine entegre etmiştir. Veriye ilişkin kaynakların birbiri ile entegre olması ve çok sayıda ülkede hizmetlerin dijital platformlarda sunulması, güvenlik algısı ve anlayışında değişimlere yol açmıştır. Bu değişimin etkisi ile siber risk ve tehditler artmıştır. Ülkeler ve işletmeler günümüzde dijital ortamlarda da tehdit edilebilmektedir (Atakan, 2021). Bu nedenle, güvenlik için ayrılacak bütçenin artırılması büyük önem taşımaktadır.

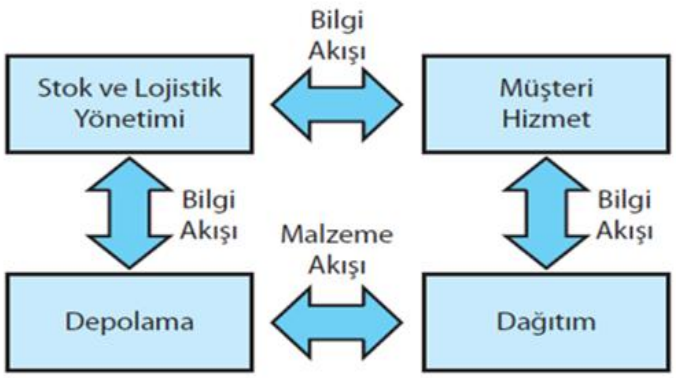
2.3.3 Lojistikte bilgi paylaşımı ve bilişim sistemleri

Lojistik faaliyetler gerçekleştirilirken dikkat edilmesi gereken hususlar arasında müşteriye sunulan hizmetin az maliyet ve yüksek kalite ile gerçekleştiriliyor olması ilk sırada yer almalıdır. Küreselleşme ile birlikte, hizmet beklentilerinin değişmesi, üretim zamanının azalması ve etkin dağıtım, işletmeler açısından öncelikli ve önemli meseleler durumuna gelmiştir. Bundan dolayı, firmaların rekabet edebilmeleri için dinamik ve verimli lojistik sistemleri oluşturması gerekmektedir (Sayın, 2017)

Tedarik zinciri içerisinde, veri aktarımının niteliği ve seviyesi arttıkça, tedarik zinciri etkinliği de artmaktadır. Çünkü, zincir içerisindeki halkalar, tek bir vücutmuş gibi hareket edebilmelidir. Ancak bu şekilde, değişen tüketici taleplerine karşı zamanında ve doğru tepkiler verebilirler. Firmalar arasındaki yoğun rekabet ve ayakta kalma mücadelesinde en kritik silah "bilgi", "bilginin doğru kullanımı", "bilginin yönetilmesi", haline gelmiştir. Sürekli bir rekabet içerisinde olan, hep daha "iyinin" peşinde olan iş dünyasının, yeni teknolojilere kayıtsız kalması beklenemez (Azimli, 2013).

Lojistik süreçlerin iyileştirilmesinde kullanılacak en temel enstrümanlardan birisi bilişim sistemleridir. Veriler bilişim sistemleri vasıtasıyla bilgiye dönüşmektedir. Kararların verilmesinde bilgiden faydalanılırken lojistik hizmet akışlarının verimliliğini, esnekliğini ve etkinliğini de sağlamaktadır. Bilgi, lojistik sistemin yaşam kaynağıdır ve bu sebeple, lojistik işleyişin verimliliği ve doğruluğu bilgi transfer ve yönetimine bağlıdır. Veri aktarımının planlanarak iyi koordine edilmesi ile karar vericiler güncel, geçerli ve doğru bilgiye ulaşabileceklerdir (Saatçıoğlu, Görçün, Görçün, Aydınocak ve Saatçıoğlu, 2019). Lojistik süreçlerin kesintisiz devamı için bilgi paylaşımı zorunlu olduğu gibi her bir sürecin birbiri ile entegre edilmesi de önemlidir.

Lojistik bilişim sistemlerinin niteliği, alt yapıların birbirine ve genel yapıya uyumlu şekilde bağlanması (entegre olması) ile artmaktadır (Adıgüzel, 2005).

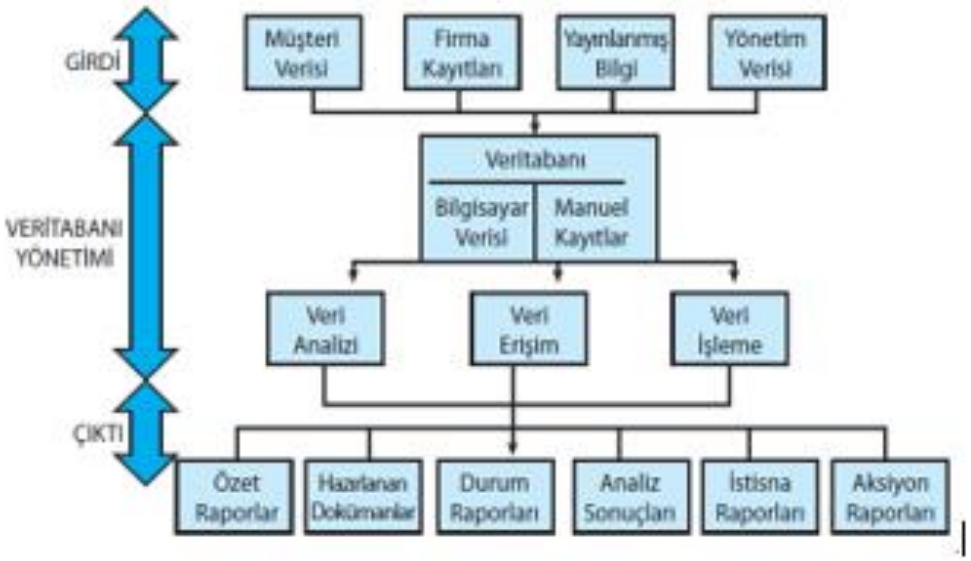


Şekil 6. Lojistik Fonksiyonlarda Bilgi Akışı (Saatçıoğlu vd., 2019)

Lojistik hizmetlerin sunulmasında çeşitli paydaşlar yer alır ve bu paydaşların hepsi birbirine zincirleme bağlıdır. İletişim ve bilgi iletimi, işletmeler, tedarikçiler ve müşteriler arasında ilerlemektedir. Zamanında ve doğru bir iletişim, lojistik yönetiminin etkili olmasını sağlar. Halkada meydana gelen bir kopukluk, sürecin aksamasına neden olur. Bilgi akışının sürekliliğine ve güvenliğinin sağlanmasına ihtiyaç bulunmaktadır. Bilgi paylaşımının düzenlenmesi karar vericilerin doğru bilgiye ulaşmasını da kolaylaştırır. Şekil 6'da lojistik faaliyetlerde bilgi akışı gösterilmektedir.

Lojistik bilgi teknolojisi sistemleri; üç ana unsurdan oluşmaktadır; Girdiler, Bilgi arşivi, Çıktılar. Lojistik bilgi teknolojisi sistemleri; 1- Lojistikle ilgili olan bilgilerin toplanmasını, işlenmesini ve depolanmasını mümkün hale getirmektedir. 2-Aynı

zamanda coğrafi olarak farklı konumlarda gerçekleşen lojistik faaliyetlerin entegrasyonunu sağlar. 3- İdarecilere, lojistikle ilgili en yeni, doğru ve geçerli olan bilgiyi vermektedir (Saatçıoğlu, Görçün, Görçün, Aydınocak ve Saatçıoğlu, 2019). Şekil 7'de lojistik bilişim sistemi bileşenleri görülmektedir.



Şekil 7. Lojistik Bilişim Sistemi Bileşenleri (Saatçıoğlu vd., 2019)

Lojistik faaliyetler kapsamlı olduğundan, bu faaliyetlerin yürütülmesi ve planlanmasında, uygulamada tek bir yazılım yeterli olmamaktadır, kullanılan farklı yazılımlar bulunmaktadır. Kurumsal Kaynak Planlama (Enterprise Resource Planning-ERP), Müşteri İlişkileri Yönetimi (Customer Relationship Management-CRM), Tedarikçi İlişkileri Yönetimi (Supplier Relationship Management-SRM), Depo Yönetim Sistemleri (Warehouse Management Systems-WMS), Taşıma Yönetim Sistemleri (Transportation Management Systems-TMS) gibi.

Bilgi teknolojilerinden yararlanmanın faydaları yanında bazı riskleri de bulunmaktadır. Lojistik bilgi teknolojileri kullanımında bilgi güvenliğini ilgilendiren bazı zorluk ve riskler;

- Müşteri bilgilerinin başka kişilerin eline geçmesi,
- Yazılım sistem güvenlik açıkları,
- Bilgilere sorumlu olmayan kişiler tarafından erişilmesi,

- Bilgisayar virüslerinin yarattığı sorunlar,
- Bilgi teknolojisinin altyapı yetersizliklerinden kaynaklanan sorunlar,
- Bilgilerin hatalı kullanımı, şeklinde sıralanabilir (Sayın, 2017).

Veriye izinsiz erişim günümüzde her büyüklükteki işletme için sözkonusudur. Diğer taraftan siber saldırganlar yoğun olarak tedarik zincirlerini hedef almaktadır. İşletmeler şirket içi bilgi güvenliklerini sağlamış olsa da, veri paylaşımı yapılan iş ortaklarının kendi bilgi güvenliklerini sağlamamış olmalarından dolayı güvenlik riski devam edecektir.

2.3.4 Risk ve lojistikte bilgi güvenliği

Zayi, hasar ve gecikmeye neden olabilecek bir olayın gerçekleşme ihtimali risk olarak tanımlanabilir. Risk, bir tehlikenin, bir zaafın yani zayıflığın ve bir sonucun bileşimidir (Kılıç, 2019). Lojistik operasyonların yürütülmesinde de çeşitli riskler bulunur; bu risklerin zamanında tespit edilip gerekli önlemlerin alınması önemlidir.

Dünya Ekonomik Forumu'nun Küresel Riskler Raporu (2023), son 17 yıldan bu yana birbirine sıkı sıkıya bağlı küresel risklerle ilgili ikazlarda bulunmaktadır. İsviçre'nin Cenevre şehrinde 11 Ocak 2023' de yapılan toplantı sonuç raporuna göre, ilerleyen 10 yıl içerisinde, teknoloji eşitsizlikleri şiddetlenirken siber güvenlikten kaynaklanan riskler sürekli bir endişe olmaya devam edecektir. Yeni teknolojilerin hızlı gelişimi ve devreye alınması, kendi risklerini de beraberinde getirmektedir. Siber suçlardaki artışın yanı sıra, tarıma ve suya, finansal sistemlere, kamu güvenliğine, ulaşıma, enerjiye ve evsel, uzaya dayalı ve deniz altı iletişim altyapısına yönelik beklenen saldırılarla, kritik teknoloji destekli kaynakları ve hizmetleri bozma girişimleri daha yaygın hale gelecektir. Teknolojik riskler yalnızca bununla sınırlı olmayıp, kişisel bilgilerin meşru yasal mekanizmalar aracılığıyla kötüye kullanılması söz konusu olacaktır (Werthmuller ve Angajman, 2023).

Dünya Ekonomik Forumu'nun hazırladığı 2024 tarihli Küresel Riskler Raporu'na göre, dezenformasyon ve yanlış bilgilendirme önümüzdeki 2 yıl içinde en büyük küresel risk olarak değerlendirilirken, aynı süreçte diğer küresel riskler arasında siber güvenlik riski de yer almaktadır. 10 yıllık perspektifte ise aşırı hava olayları öncelikli risk olarak

değerlendirilirken, diğer riskler dezenformasyon ve yanlış bilgilendirme, yapay zekânın yaratabileceği olumsuz sonuçlar, siber güvenlik şeklinde sıralanmaktadır (İSO Yeşil Blog, 2024). Raporlar, önümüzdeki yıllarda siber suçlar ve siber güvenlik risklerinin artmaya devam edeceğini göstermektedir.

Lojistik ve nakliye işlemlerindeki riskler, ürünlerin depolanması, hazırlanarak paketlenmesi ve teslimatı ile ilgili riskleri kapsar. Bilgi kaynaklı riskler, bilgi ve iletişim sistemleri ile teknolojiyle ilgili yenilikleri kapsamaktadır. Bilgi sistemleri için başlıca risk konuları, bilgiye erişilememesi, bilgiyi zamanında elde edememek, gecikmesi, bilgi altyapısının bozulması, bilgi paylaşımı sorunları, yönetimsel sorunlar, bilgi sisteminin güvenliği, gizlilik riski, siber saldırılar şeklinde sayılabilir (Küçükoğlu, 2020).

Tedarik zinciri faaliyetlerinde riskin yönetilmesi, risk değerlendirmelerinin yapılması ile muhtemel risklerin tespit edilerek, bu risklere karşı nasıl tedbir alınacağına karar verilmesidir (Sayın, 2017). Bilgi güvenliği için de en önemli husus risk analizinin yapılmasıdır. İşletmeler tarafından yapılacak öncelikli iş oluşabilecek riskleri tespit etmektir. Risklerin hangi kaynaklardan gelebileceği, hangi tür bilgilerin işlendiği ve hangi bilgilerin korunması gerektiği gibi hususların belirlenmesi gerekeceğinden veri envanterinin oluşturulması gereklidir. Kaydedilen verilerin türü, işlenme ve kullanım yeri ile işleme türü belirlenip sıralanmalıdır. Varlıkların yanı sıra tehdit ve güvenlik açıkları da tanımlanarak riskler belirlenmelidir.

Uluslararası standard ve yasal düzenlemelerden faydanılarak oluşturulacak bilgi güvenliği politikaları ile şirket verilerine yönelik risk seviyesinin düşürülmesi, oluşabilecek muhtemel zararların azaltılması ve hatta önlenmesi mümkündür. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, bütün süreçlerin emniyetini sağlamayı hedefleyen bir bilgi güvenliği standardıdır. Risk yönetimi süreçlerini uygulayarak verilerin mahremiyeti, tamlığı ve ulaşılabilirliğini korur. Risklerin doğru bir şekilde idare edildiğine ilişkin olarak ilgililere güvence verir. Bu standard ile sadece dijital ortamda işlenen ve saklanan veri ve sistemlerin güvenliği değil aynı zamanda, fiziki olarak kayıt edilen verilerin de güvenliği sağlanabilmektedir. ISO bilgi güvenliği standardı ile oluşturulacak bilgi güvenliği politikaları, prosedürler, teknik ve idari tedbirler ihtiyaca

göre güncellenmekte ve denetlenmektedir. Bu şekilde, değişen risklere karşı zamanında önlem alınması da mümkün olmaktadır.

Lojistikte verilen hizmetlerin amacı, müşterilerin gereksinimi olan malların temin edilmesi ve bu yapılırkende yedi beklentisinin karşılanmasıdır. Buna "Lojistiğin 7 Doğrusu" adı verilir. Bunlar Doğru malın, Doğru zamanda, Doğru yolla, Doğru miktarda, Doğru kaynaktan, Doğru biçimde, Doğru fiyata sağlanmasıdır (Yıldıztekin, 2009). Bu işlemlerin düzenli bir şekilde yürütülebilmesi için sürekli ve kesintisiz bilgiye ihtiyaç bulunmaktadır. Yasal düzenlemelere uyumlu ve standartlardan faydalanılarak oluşturulacak politikalar ve alınacak teknik ve idari tedbirler ile sağlanacak bilgi güvenliği ortamında bilgiye kesintisiz erişim mümkün hale gelecektir. Hukuki düzenlemelere uyumlu politikaların bir diğer faydası, çalışanların yasal düzenlemelere dair farkındalıklarının oluşması ve sorumluluklarının bilincinde hareket etmelerine yardımcı olmaktır.

2.4 Hukukumuzda Kişiler ve Veriler

2.4.1 Gerçek ve tüzel kişi

4721 sayılı Medeni Kanunun birinci kitabı Kişiler Hukuku olarak düzenlenmiştir. Kişiler hukukunun temel kavramı kişidir ve hukukta kişi, hak ve borçlara sahip olan varlık' tır. Hukukta iki tür kişi bulunmaktadır, Gerçek ve Tüzel Kişiler. Medeni Kanun 8'nci maddeye göre; "*Her insanın hak ehliyeti vardır. Buna göre bütün insanlar, hukuk düzeninin sınırları içinde, haklara ve borçlara ehil olmada eşittirler*" (Türk Medeni Kanunu, 2001, s. 8050). Toplum hayatının gereği olarak, belirli nitelikteki kişi ya da mal toplulukları da hak ehliyetine sahiptir. Buna göre kanun koyucu, toplumun gerçekleri ve ihtiyaçlarını göz önünde bulundurarak insanın (gerçek kişi) yanında, belirli nitelikteki kişi ya da mal topluluklarını da kişi (tüzel kişi) olarak kabul etmiştir.

Tüzel kişiler, kendilerine başlı başına kişilik tanınmış, belli bir amaca yönelmiş kişi ya da mal topluluklarıdır. Medeni Kanun'un 47 ila 48'nci maddelerinde tüzel kişilere ilişkin düzenlemelere yer verilmiştir;

A. Tüzel kişilik

MADDE 47- Başlıbaşına bir varlığı olmak üzere örgütlenmiş kişi toplulukları ve belli bir amaca özgülenmiş olan bağımsız mal toplulukları, kendileri ile ilgili özel hükümler uyarınca tüzel kişilik kazanırlar.

B. Hak ehliyeti

MADDE 48- Tüzel kişiler, cins, yaş, hısımlık gibi yaradılış gereği insana özgü niteliklere bağlı olanlar dışındaki bütün haklara ve borçlara ehildirler.

Tüzel kişiler ve gerçek kişiler hak süjesi olma yönünden eşittir; yalnızca hak edinme ve borç yükü altına girme bakımından aralarında kapsam ve nicelik açılarından farklar bulunmaktadır (Arslan, 2018)

2.4.2 Veri

2.4.2.1 Kişisel veriler

Anayasanın 'Temel Hak ve Hürriyetlerin Niteliği' başlıklı 12'nci maddesine göre; "*Herkes, kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir"* (T.C. Anayasası, 1982, s. 4). Kişisel veri ise, bireylerin kimliklerini belirli hale getirmeye elverişli her türlü bilgi olarak tanımlanabilir. Bu bağlamda kişinin kimlik, iletişim, sağlık ve mali bilgileri ile özel hayatına, dini inancına ve siyasi görüşüne ilişkin bilgiler, kişisel veri olarak nitelendirilmektedir (Türkiye Büyük Millet Meclisi, 2016).

Anayasanın Özel Hayatın Gizliliği başlıklı 20'nci maddesine göre;

> Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. 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 (T.C. Anayasası, 1982, s. 7).

Anayasanın 20'nci maddesi, 2010 yılında yapılan düzenlemeyle yeni halini almıştır. Böylelikle, kişisel verilerin korunması, temel bir hak olarak teminat altına alınmıştır.

Anayasanın 20'nci maddesinde, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtildiğinden bu doğrultuda hazırlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarihinde 29677 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Kanunun 3/d maddesinde kişisel veri; "*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmıştır (Kişisel Verilerin Korunması Kanunu, 2016, s. 12301). Bu tanıma göre, bireylerin ismi, soy ismi, doğum yeri ve tarihi gibi kimliğini belirleyen bilgiler yanında ayrıca bireyin ailevi, ekonomik, fiziki, kültürel, sosyal, psikolojik kimliğini de ifade edecek veriler ile kimlik, sosyal güvenlik numarası, telefon numarası gibi kişileri belirlenebilir kılacak verilerin tümü kişisel veri olacaktır.

Kanunun 6/1'nci maddesinde Özel Nitelikli Kişisel Veriler'den sözedilerek;

> Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veri olarak belirtilmiştir (Kişisel Verilerin Korunması Kanunu, 2016, s. 12302).

Bu verilerin yetkisiz kişiler tarafından elde edilmesi, kullanılması ve ifşa edilmesi gerek taraf olduğumuz sözleşmeler ve gerekse Anayasamızda koruma altına alınan temel hakların ihlali olarak karşımıza çıkmaktadır (Türkiye Büyük Millet Meclisi, 2016).

2.4.2.2 Tüzel kişi verileri

Doktrinde, Hatemi (1979) ve Çağlayan (2018), tüzel kişi tanımlaması, gerçek kişilerden farklı olarak hukuki bir kişiliğe sahip olan, hukuki varlıklar şeklinde yapılmıştır. Hak ehliyetine sahip olmak tüzel kişiler bakımından da en önemli niteliklerden birisidir. Medeni kanun gereğince, "*Tüzel kişiler, cins, yaş, hısımlık gibi yaradılış gereği insana özgü niteliklere bağlı olanlar dışındaki bütün haklara ve borçlara ehildirler."* Tüzel kişi verilerinin korunması konusunun temelinde, verilerinin korunmasında hukuki menfaati

bulunan tüzel kişilerin bu taleplerini destekleyen Anayasal hakları yer almaktadır (Küpeli, 2019).

Anayasa'nın 12'nci maddesinde, herkesin kişiliğine bağlı olarak dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlerinin bulunduğu, 17'nci maddesinde de, herkesin; yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahip olduğu hükme bağlanmıştır. Buna göre, tüzel kişiler kendileri için uygun olan ve Anayasamızda belirtilen hak ve borçlardan faydalanabileceklerdir. Tüzel kişilerin incitilecek duyguları yoktur, ancak itibarları zarara uğrayabilir. Bu nedenle, tüzel kişiliğe ait bilgilerin nasıl ve ne ölçüde paylaşılacağına tüzel kişiliklerin kendilerinin karar vermesi gereken mahremiyet hakkı ve özel yaşama saygı duyulması haklarının tüzel kişilikler açısından da kabul edilmesi gerekmektedir. Keza, tüzel kişilikler acı çekip üzüntü duyamazlar, ancak tüzel kişiliğe olan güven azalabilir, piyasadaki itibarları sarsılabilir (Küpeli, 2019).

Buna göre, yetersiz önlemler veya önlem alınmaması nedeniyle veri ihlali yaşanması halinde, şirketin tüzel kişiliğinin müşteri ve paydaşlar nezdindeki itibarı zarar görecektir. Aynı zamanda piyasadaki rekabet gücü de olumsuz etkilenecektir. Şirket tüzel kişiliği, riske karşı gerekli önlemi almaması sebebiyle maddi ve manevi zarara uğrayacaktır.

Tüzel kişilerin, bireylere has olan haklar haricinde, isim, kredi bilgileri, ticari sır, şeref ve saygınlıkları gibi kişilik değer ve haklarının mevcut olduğu kabul edilmektedir. Doktrinde, Özsunay (t.y.) ve Köprülü (1967), tüzel kişilerin gizlilik alanı, tüzel kişiler tarafından dışarıya açıklanmak istenmeyen ve tüzel kişilerin iç işleyişleriyle ilgili bilgiler olarak tanımlanmıştır. Tüzel kişilerin ticari faaliyet bilgilerinin paylaşılması konusunda da bu alanın sınırlarının belirlenmesi önemlidir. Örneğin, tüzel kişinin finansal durumu ile ilgili bilgilerinin kredi talebinde bulunduğu banka tarafından öğrenilmesi kişilik hakkının ihlali olarak değerlendirilmez. Ancak bu bilgilerin ilgisiz kişiler ile paylaşılmış olması halinde kişilik hakkı ihlal edilmiş olacaktır. Tüzel kişiliğe özgü tüm bilgiler tüzel kişi verileridir. Ticari sırlar ve analizleri, finansal bilgiler, kuruluş bilgileri, müşteri dataları gibi örneklendirilebilir (Küpeli, 2019).

Tüzel kişilerin işlediği veriler, tüzel kişiliğin ticari sır niteliğindeki verileri, diğer veriler, müşteriler ile ilgili veriler, gerçek kişiler ile ilgili kayıt altına aldığı (personel verileri gibi) kişisel veriler şeklinde sayılabilir.

2.4.2.2.1 Ticari sır

İnsanlar arasındaki iş ilişkileri rekabet olgusunu ortaya çıkarmıştır. Bu durum, kaynakların ve pazarın paylaşımıyla ilgili çeşitli aktörler arasında avantaj arayışı ile performansın artırılmasına yol açmıştır. Ticaretle uğraşanlar, kendi rekabet avantajlarını devam ettirebilmek ve rakiplerine karşı güçlü durabilmek için, kendilerine piyasada ticari ve ekonomik açıdan üstünlük sağlayan verilerin diğer tacirler tarafından öğrenilmesini istememişlerdir. Yaklaşık 4000 yıl önce hazırlanan Hammurabi Kanunları, bilinen ilk ticari sır düzenlemesini içermektedir. Hammurabi Kanunları'na göre, bir ticari sırrı hukuk kurallarına aykırı şekilde açıklayan kişi ağır bir ceza alır, bir gözü kör edilirdi. Sanayi devrimi ile birlikte fabrikalar kurulmuş ve üretim şekli değişerek seri üretime geçilmiştir. Bundan dolayı çalışan sayısı da artmıştır. Bu aşamada ticari sırların korunması gerekliliği daha da önemli hale gelmiştir. Çünkü çalışan sayısının artışı ile işyerinin ticari sırları daha fazla işçi tarafından bilinir hale gelmiştir. Bu dönemden sonra ticari sırların hukuki olarak korunması için adli makamlara başvurular başlamıştır (Sulu, 2020).

Türk Ceza Kanunu'nun 239'nci maddesinde "*Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi"* (Türk Ceza Kanunu, 2004, s. 9023) denilerek ticari sırdan bahsedilmiş ancak bu madde de olduğu gibi, ticari sır ile ilgili hükümlere kanunlarda yer verildiği halde tanımı yapılmamıştır.

Türk Ticaret Kanunu'nu Haksız Rekabetin düzenlendiği 55/b-3 fıkrasında "*İşçileri, vekilleri veya diğer yardımcı kişileri, işverenlerinin veya müvekkillerinin üretim ve iş sırlarını ifşa etmeye veya ele geçirmeye yöneltmek"* denilerek üretim ve iş sırlarından sözedilmiş, ancak yine tanım yapılmamıştır (Türk Ticaret Kanunu, 2011, s. 10987).

Yargıtay 23.Hukuk Dairesinin 21.10.2019 tarihli ve 2016/6958 E., 2019/4349 K. Sayılı kararında Ticari sır dar anlamda, "*Ticari sır, gerçek ya da tüzel kişi tacire, rakiplerine karşı ekonomik anlamda menfaat sağlayan, sır olarak saklanan ve gizli kalması için gerekli önlemlerin sahibi tarafından alındığı bilgi*" olarak açıklanmıştır (Yargıtay 23. HD, 2019).

Fikri Mülkiyet Haklarının Ticari Niteliklerine İlişkin Anlaşma da (TRIPS) ticari sırlar, ulaşılması kolay olmayan veya kamu ve iş çevrelerinin bilmediği, gizli tutmak üzere güvenlik tedbirleri alınan ve gizli olduğu için de ticari ve ekonomik değere sahip olan bilgiler olarak tanımlanmıştır. Bu bilgiler özel kanunlar ve haksız rekabet hükümleri ile korunmaktadır (Baylan, 2020). Kanun koyucu ilk kez ticari sır tanımına, tasarı halinde olan, Ticari Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısı' nda yer vermiştir.

"Ticari sır, bir ticarî işletme veya şirketin faaliyet alanı ile ilgili yalnızca belirli sayıdaki mensupları ve diğer görevlileri tarafından bilinen, elde edilebilen, özellikle rakipleri tarafından öğrenilmesi halinde zarar görme ihtimali bulunan ve üçüncü kişilere ve kamuya açıklanmaması gereken, işletme ve şirketin ekonomik hayattaki başarı ve verimliliği için büyük önemi bulunan; iç kuruluş yapısı ve organizasyonu, malî, iktisadî, kredi ve nakit durumu, araştırma ve geliştirme çalışmaları, faaliyet stratejisi, hammadde kaynakları, imalatının teknik özellikleri, fıyatlandırma politikaları, pazarlama taktikleri ve masrafları, pazar payları, toptancı ve perakendeci müşteri potansiyeli ve ağları, izne tâbi veya tâbi olmayan sözleşme bağlantılarına ilişkin veya bu gibi bilgi ve belgelerdir" (Türkiye Büyük Millet Meclisi, 2011).

Hukuki literatürde ticari sır, ekonomik değer taşıyan ya da rekabet avantajı sağlayan, henüz genel olarak bilinmeyen ya da rakip olan şirketler tarafından bilinmeyen ve sahibi tarafından gizli tutulmak istenen bilgi şeklinde tarif edilmektedir (Küpeli, 2019).

Ticaret ile ilgili verilerin ticari sır olarak kabul edilmesinin bazı şartları bulunmaktadır. Gizli olan bilginin ilgili sektör veya kamu tarafından bilinmemesi veya kolaylıkla ulaşılmasının mümkün olmaması, gizli tutulabilmesi için bu bilgiyi korumak üzere kabul edilebilir önlemlerin alınmış olması, bilginin gizli tutulması sebebiyle ekonomik bir değerinin bulunması gerekmektedir. Bu bilgilerin gizliliğinin korunabilmesi için önlemler alınmasının gerekliliğine ilişkin Coca-Cola örneği verilebilir. Firmanın üst düzey yetkilisi ve hukuk müşavirinin davada vermiş olduğu şahit beyanlarında; "*İçeceğin formülünün gizli olduğunu ve formülün yazılı metninin Atlanta Trust Company Bankası'nda kasada korunduğunu, kasanın da ancak şirket Yönetim Kurulu'nun alacağı karar ile açılmasının mümkün olduğunu ifade etmişlerdir. Ayrıca, firmada herhangi bir zamanda aynı anda yalnızca 2 kişinin formülü bildiğini ve sadece bu 2 kişinin formülün*

fiili hazırlık aşamasını denetleyebileceğini" belirtmişlerdir (Baylan, 2020). Bu örnek göstermektedir ki, firma, ürün formülünü, yazılı politikaları ile belirlediği bir ortamda korumaktadır. Çünkü formülün korunduğu kasa yönetim kurulu kararı ile açılabilmekte, şirkette aynı anda sadece iki kişi formülü bilmektedir, tüm bunların firma içi politikalar ile belirlendiği, kurallaştırıldığı anlaşılmaktadır. Firma, tüzel kişiliğin menfaatleri için çok önemli olan üretim formülünü korumak üzere, yüksek seviyede özen göstererek basiretli bir tacir olarak üst düzeyde güvenlik tedbiri almıştır.

Şirketler için ticari değeri olan, gizli ve şirketlere rekabet edebilme olanağı veren ticari sır örnekleri, iş raporları, fiyat oluşum bilgileri, stok verileri, üretime ilişkin teknik ve formüller, tedarik listeleri, ücret stratejileri, hammadde kaynakları, aleni olmayan finansal veriler şeklinde sayılabilir (Küpeli, 2019).

2.4.2.2.2 Müşteri verileri

Şirketlerin ticari faaliyetleri dolayısı ile elde ettiği ve finansal ve kişisel olmak üzere çeşitli türlerden oluşan gizli kalması gereken veriler şeklinde tanımlanır. Ticarî Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısı'nın 2' nci maddesinde müşteri sırrı; "*Müşterilerin şahsi, iktisadi, mal, nakit ve kredi durumlarına ilişkin doğrudan veya dolaylı bilgi ve belgeler"* olarak tanımlanmıştır. Şirketler tarafından işlenen müşteri verileri Türk Ceza Kanunu (239.md.) ile korumaya alınmıştır. Özel hukuk tüzel kişilerinin müşteri bilgileri, bu koruma kapsamındadır (Küpeli, 2019).

Tüzel kişiler tarafından kayda alınan ticari sırlar ve müşteri sırları niteliğindeki verilerin izinsiz ele geçirilerek ifşası ve kullanılması, iş gereği izinli olarak elde edildiği halde sonrasında bu verilerin izinsiz olarak ifşa edilerek kullanılması, güven zedeleyici bir durum olmasından ötürü, şirketin piyasada itibar kaybı yaşamasına, maddi kayıplara ve hukuki sorumluluklarının doğmasına sebep olacaktır.

Ticari işletmelerin sahip olduğu veriler, korunması gereken değerli ticari varlıklardır. Bilgi güvenliği, işletme yönetimi için hem itibarı korumak hem de işletmeye yönelik tehdidi azaltmak için çok önemlidir (Roy ve Kundu, 2012).

2.4.2.2.3 Kişisel veriler

Tüzel kişiler tarafından işlenen, gerçek kişilere ilişkin verilerdir. Örneğin; Personele ilişkin bilgiler, iş başvurusunda alınan bilgiler gibi. Bu türden veriler, Kişisel Verilerin Korunması Kanunu kapsamında korunmaktadır.

2.4.2.2.4 Diğer veriler

Tüzel kişiler tarafından işlenen ticari sır niteliğinde olmayan, tüzel kişiliğe ilişkin diğer türden verilerdir. Genellikle kamuya açıktır, şirketlerin web sitelerinde yer alan bilgiler, bilgi toplumu hizmeti içeriğinde yer verilen bilgiler gibi.

2.5 Yasal Düzenlemeler

2.5.1 Kişisel verilerin korunmasına ilişkin yasal düzenlemeler

2.5.1.1 Ulusal düzenlemeler

Kişisel verilerin korunması ile ilgili ulusal düzenlemelerin kronolojik sıralaması Tablo 9'da gösterilmiştir.

Tablo 9. Kişisel Verilerin Korunması ile İlgili Ulusal Yasal Düzenlemeler (Kişisel Verileri Koruma Kurumu, t.y.)

TARİH	YASAL DÜZENLEME
18 Ekim 1982	Türkiye Cumhuriyeti Anayasası
22 Kasım 2001	4721 Sayılı Türk Medeni Kanunu
12 Ekim 2004	5237 Sayılı Türk Ceza Kanunu
4 Mayıs 2007	5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
12 Eylül 2010	Kişisel Verilerin Korunması İle İlgili Hükmün Anayasaya Dahil Edilmesi
11 Ocak 2011	6098 Sayılı Türk Borçlar Kanunu
17 Mart 2016	108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Türk Hukukuna Dahil Edilmesi
07 Nisan 2016	6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun 29677 Sayılı Resmi Gazetede Yayımlanarak Yürürlüğe Girmesi
05 Mayıs 2016	181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokolün Türk Hukukuna Dahil Edilmesi

2.5.1.1.1 1982 Anayasası

Teknolojideki yenilik ve gelişmeler temel hak ve özgürlüklere müdahale etmeyi kolaylaştırdığından, bu durum hukuki bir mesele halini almıştır. Bu sebeple, konuya ilişkin hukuki düzenlemelerin yapılması ihtiyacı doğmuştur. Kişilerin temel hak ve görevleri Anayasa'nın ikinci bölümünde düzenlenmiştir.

Temel haklardan birisi de özel hayatın gizliliğidir. 5982 sayılı Kanun ile 2010 yılında yapılmış olan Anayasa değişikliğiyle, "Özel hayatın gizliliği ve korunması" başlığı altındaki 20'nci maddeye bir fıkra eklenerek kişisel verilerin korunması ile ilgili hükümlere yer verilmiştir (Kişisel Verileri Koruma Kurumu, t.y.).

A. Özel hayatın gizliliği

MADDE 20 – 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.

2.5.1.1.2 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Ülkemizde kişisel verilerin korunması konusunda yasa çıkarılması için 1989 yılında bir komisyon kurulmuştur. Ancak komisyon çalışmalarını bitiremeden dağılmıştır. İlerleyen yıllarda da komisyonlar kurulmuş ancak tasarılar kanunlaşamamıştır (Kişisel Verileri Koruma Kurumu, t.y.).

Anayasa'nın 20. maddesine eklenen, kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir, şeklindeki hüküm ile kişisel verileri korumaya ilişkin düzenlemelerin kanunla yapılacağı düzenlenmiştir.

AB üyesi devletlerde kişisel verilerin benzer standartlarda korunması ve birlik sınırları dışında da bilgi paylaşım kurallarının belirlenmesi için, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme" hazırlanmıştır ve 28 Ocak 1981 tarihinde imzaya açılmıştır. Bu sözleşme ülkemiz tarafından da imzalanarak 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazete'de yayımlanmış ve iç hukuka dahil edilmiştir. Sözleşmenin 4. maddesi gereğince, iç hukukumuzda kişisel verilerin korunmasına yönelik hukuki düzenleme yapılması gerekliliği oluşmuştur (BG Hukuk, 2021).

Nitekim, Anayasa Mahkemesinin 9 Nisan 2014 tarihli ve E:2013/122, K:2014/74 sayılı kararında da; *"Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı […]" amaçladığı tespit edilerek, "kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara*

ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler" nedeni ile kişisel verilerin çok daha fazla korunmaya ihtiyacı olduğu belirtilmiştir (BG Hukuk, 2021).

Tüm bu gelişmeler gereğince hazırlanan Kişisel Verilerin Korunması Kanunu Tasarısı 18 Ocak 2016'da Türkiye Büyük Millet Meclisi Başkanlığına gönderilmiştir. Tasarı metni, 24 Mart 2016 tarihinde TBMM Genel Kurulu'nda kabul edilerek yasalaşmıştır. 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir (Kişisel Verileri Koruma Kurumu, 2019a)

Amaç

MADDE 1- (1) 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.

Kanunun amacı, madde gerekçesinde de belirtildiği üzere, 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. Ayrıca, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların da düzenlenmesi Kanunun amaçları arasında yer almaktadır (Türkiye Büyük Millet Meclisi, 2016).

Tanımlar

MADDE 3- (1) Bu Kanunun uygulanmasında;

d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, ifade eder.

Kanunun tanımına göre;

- Gerçek kişilerin isim, soy isim, doğum tarihi ve yeri gibi bireyin kesin olarak teşhisini sağlayan bilgiler yanında, bireyin ailevi, fiziki, ekonomik, sosyal vb. özelliklerine ilişkin veriler de kişisel veri olarak kabul edilmektedir.

- Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesidir. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi ile kişinin belirlenmesini sağlayan tüm durumları kapsamaktadır.

- Sosyal güvenlik numarası, araç plakası, pasaport ve telefon numarası, mülakat sonuçları, kullandığı elektronik cihazların IP adresleri, Cv'si, fotoğraf, görüntü ve ses kayıtları, adli sicil kaydı, kredi kartı ekstreleri, sosyal medya beğenileri, parmak izleri, genetik bilgiler gibi veriler de kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel veridir (Kişisel Verileri Koruma Kurumu, t.y.).

- Diğer taraftan, bir firmanın ticaret unvanı ya da adresi gibi tüzel kişiliğe ilişkin bilgiler (gerçek bir kişiyle ilişkilendirileceği durumlar hariç) kişisel veri sayılmamaktadır (Nitelikli Veri, t.y.).

ı) Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ğ) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi, ifade eder.

Bu tanımlamalara göre, veri sorumlusu kişiler, gerçek kişiler olabileceği gibi, şirket, dernek, vakıflar veya kamu kurumları gibi tüzel kişiler de olabilecektir. Veri işleyenler de, kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen çalışanlar olabileceği gibi, veri sorumlusunun hizmet satın almak suretiyle belirlediği ayrı bir gerçek veya tüzel kişi de olabilir. Herhangi bir gerçek veya tüzel kişi aynı zamanda hem veri sorumlusu, hem de veri işleyen olabilir. Örneğin;

- Bir muhasebe şirketi kendi personeliyle ilgili tuttuğu verilere ilişkin olarak veri sorumlusu sayılırken, müşterisi olan şirketlere ilişkin tuttuğu veriler bakımından ise veri işleyen olarak kabul edilecektir.

- Bir özel şirket, topladığı kişisel verilerin saklanması için bir bulut hizmeti sağlayıcısı ile sözleşme yapar ise, bulut hizmeti sağlayıcısı veri işleyen durumundadır. Çünkü taraflar arasındaki sözleşme gereği bulut hizmeti sağlayıcısının verileri kendi amaçları için kullanması mümkün değildir. Ayrıca, bulut hizmeti sağlayıcısının kendisi de veri toplamamaktadır. Tek faaliyeti şirketten gelen kişisel verileri yine özel şirketin talimatlarına uygun olarak saklamaktır (Kişisel Verileri Koruma Kurumu, t.y.) (Kişisel Verileri Koruma Kurumu, 2019b).

MADDE 3- (1) Bu Kanunun uygulanmasında;

a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı, ifade eder.

Bu düzenlemelere göre açık rıza, ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüte yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır (Kişisel Verileri Koruma Kurumu, 2019c). Firmalarca yapılacak kişisel veri kayıtlarında kanunun bu hükmüne uygun hareket edilmesi gerekmektedir.

Kişisel verilerin işlenme şartları

MADDE 5- (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

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

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

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

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

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

Buna göre, kural olarak kişisel verilerin ilgili kişinin açık rızası olmaksızın veya madde de sayılan istisnalar dışında işlenmesi yasaktır.

Bu düzenleme gereğince:

Örneğin; Taraflar arasında sözleşme yapılarak para yatırılabilmesi için karşı tarafın hesap bilgilerinin alınması mümkündür. Aynı şekilde bankadan kredi talebinde bulunan kişiden tapu kayıt bilgileri, maaş bordrosu gibi bilgi ve belgelerin istenmesi bu kapsamda değerlendirilecektir. (c fıkrası gereği)

Örneğin; Bir firmanın, işçilerine maaşlarını yatırabilmesi için hesap numarası bilgilerini istemesi, medeni durumuna, bakmakla yükümlü olduğu kişilere, sosyal sigorta numarası gibi verilerini işliyor olması yine maddenin verdiği yetki ile mümkün olacaktır.(d fıkrası gereği)

Örneğin; Bir kargo firmasının, teslimat yapabilmek için alıcının adres ve iletişim bilgilerini kaydetmesi. Veri sorumlusunun, bu kayıtların hepsini hukuki yükümlülüğünü yerine getirebilmesi için gerekli ve bu amaçla sınırlı olarak gerçekleştiriyor olmalıdır. (ç fıkrası gereği)

Örneğin; Bir şirket sahibi, şirketinin yapılandırılması kapsamında görev ve sorumlulukları belirlerken esas alınmak üzere işçilerinin kişisel verilerini işleyebilir. Bu noktada belirleyici olan, şirketin yeniden yapılandırılması veri sorumlusu firma sahibinin menfaatidir. Önemli olan verilerin korunmasına ilişkin ilkelere uyulması ve veri sorumlusu ile verisi kaydedilen kişinin menfaat dengelerinin gözetilmesidir. (f fıkrası gereği). (Kişisel Verileri Koruma Kurumu, 2019d) (Türkiye Büyük Millet Meclisi, 2016) (Kişisel Verileri Koruma Kurumu, t.y.).

Özel nitelikli kişisel verilerin işlenme şartları

MADDE 6- (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) (Mülga:2/3/2024-7499/33 md.)

(3) (Değişik:2/3/2024-7499/33 md.) Özel nitelikli kişisel verilerin işlenmesi yasaktır. Ancak bu verilerin işlenmesi;

a) İlgili kişinin açık rızasının olması,

b) Kanunlarda açıkça öngörülmesi,

c) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,

ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,

d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,

e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,

f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,

g) Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla;

mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması, halinde mümkündür.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

Bu düzenlemelerin tümü, işlenen kişisel verilerin niteliği ve işlenme şartlarına ilişkindir. Diğer taraftan işlenen verilerin tümü bilgi güvenliği kapsamında korunması gereken varlıklardır ve bu verilerin korunması yasal olarak da bir zorunluluktur.

Veri güvenliğine ilişkin yükümlülükler

MADDE 12- (1) Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

(4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul,

gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

Bu düzenleme ile, veri sorumlularının kaydettikleri kişisel verileri korumaya yönelik uymak zorunda oldukları yükümlülükler ile ihlal halinde yapılması gereken hususlar açık ve net olarak belirlenmiştir. Maddenin 2'nci fıkra düzenlemesine göre, veri sorumlusu, firmasına ait kayıtların tutulması işlemini bir muhasebe şirketine yaptırıyorsa, verilerin kayıt edilmesi ile ilgili maddenin birinci fıkrasında açıklanan önlemlerin alınması konusunda muhasebe şirketi ile birlikte müştereken sorumlu olacaktır. Yine 5'nci fıkra düzenlemesi gereğince, işlenen verilerin yasal olmayan yollarla izinsiz ele geçirilmesi durumunda, veri sorumlusunun bu vaziyeti ilgili kişilere (kişisel verileri işlenmiş olan kişiler gibi) ve Kurula bildirmesi gerekliliği düzenlenmiştir (Kişisel Verileri Koruma Kurumu, 2019b).

Örneğin, yemek tedariki ile lojistik hizmeti sağlayan firmaya siber saldırı düzenlenmiştir. Saldırı sonrasında şirket kamuoyuna açıklama yaparak, müşterilerin bir kısmının ad-soyad, mail adresleri, telefon numaraları ve adres bilgilerinin çalındığını, saldırıdan 21 milyon 504 bin 83 kişinin etkilendiğini ifade etmiştir. Saldırıda kredi kartı ya da finansal verilerin etkilenmediğini, kredi kartı saklama hizmetinin veri sorumlusundan bağımsız Mastercard tarafından sağlandığını ifade etmiştir. Şirket, kanunun 12/5 fıkrasına uygun olarak, siber saldırıyı Kişisel Verileri Koruma Kurulu'na bildirmiştir (Kişisel Verileri Koruma Kurulu Kararı, 2021).

Kişisel Verilerin Korunması Kanunu içeriğinde, yükümlülüklerin yerine getirilmemesi halinde uygulanacak cezai ve idari müeyyidelere de yer verilmiştir. Düzenleme, suçlar ve kabahatler şeklindedir.

Suçlar

MADDE 17- (1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140 ıncı madde hükümleri uygulanır.

(2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.

Kabahatler

MADDE 18- (1) Bu Kanunun;

a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,

b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,

c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,

ç) 16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar,

d) **(Ek:2/3/2024-7499/35 md.)** 9 uncu maddenin beşinci fıkrasında öngörülen bildirim yükümlülüğünü yerine getirmeyenler hakkında 50.000 Türk lirasından 1.000.000 Türk lirasına kadar, idari para cezası verilir.

(2) **(Değişik:2/3/2024-7499/35 md.)** Birinci fıkranın (a), (b), (c) ve (ç) bentlerinde öngörülen idari para cezaları veri sorumlusu, (d) bendinde öngörülen idari para cezası veri sorumlusu veya veri işleyen gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır.

(3) **(Ek:2/3/2024-7499/35 md.)** Kurulca verilen idari para cezalarına karşı, idare mahkemelerinde dava açılabilir.

(4) Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu kurula bildirilir.

Kanun metni bu şekilde düzenlenmiş olmakla birlikte, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 18'inci maddesinde düzenlenen İdari Para Cezaları, 5326 sayılı Kabahatler Kanunu'nun 17'nci maddesinin yedinci fıkrasına göre her takvim yılı başından geçerli olmak üzere o yıl için 213 sayılı Vergi Usul Kanunu'nun mükerrer 298'inci maddesi hükümleri uyarınca revize edilmektedir. 2024 yılı için tespit ve ilan edilen yeniden değerleme oranında arttırılmış tutarlar Tablo 11'de gösterilmiştir. İlgili düzenleme gereğince bu oranlar her sene yenilenmektedir. Suçlara ilişkin cezai düzenlemeler Tablo 10' da özetlenmiştir.

Tablo 10. Türk Ceza Kanunu Hürriyeti Bağlayıcı Cezalar (Türk Ceza Kanunu, 2004)

Suç	Ceza
Kişisel verileri hukuka aykırı olarak kaydetmek (TCK 135/1)	1-3 Yıl Hapis
Kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek (TCK 136/1)	2-4 Yıl Hapis
Özel nitelikli kişisel verileri hukuka aykırı olarak kaydetmek (TCK 135/2)	1 Yıl 6 Ay – 4 Yıl 6 Ay Hapis
Verileri yok etmeme (TCK 138/1)	1 – 2 Yıl Hapis

Tablo 11. İdari Para Cezaları 2024 Oranları (Kişisel Verilerin Korunması Kanunu, 2016) (Kişisel Verileri Koruma Kurumu, 2024a) (T.C. Resmi Gazete, 2023)

İhlal	Müeyyide
Aydınlatma yükümlülüğünün ihlali-10. madde	47.303 TL. – 946.308 TL.
Veri güvenliğinin ihlali- 12. madde	141.934 TL. – 9.463.213 TL.
KVKK kurul kararlarına uymama- 15. madde	236.557 TL. – 9.463.213 TL.
Sicile kayıt ve bildirim yükümlülüğünün ihlali-16.madde	189.245 TL. – 9.463.213 TL.
Standart sözleşmenin Kurula bildirim yükümlülüğünün ihlali- 9. Madde 5.fıkra	50.000 TL. – 1.000.000 TL.

İdari para cezaları, belirtilen kanun maddelerine uyulmaması halinde, kurul tarafından verilen cezalardır. Diğer taraftan, veri ihlalinden etkilenen ilgili kişiler tarafından, yeterli korumayı sağlamayarak zarara uğramalarına sebep olanlar hakkında adli yargıda ceza ve hukuk davaları açılması mümkündür. Yeni değişiklik ile, kurul tarafından karar verilen idari para cezalarına karşı idare mahkemesinde dava açılabileceği belirtilmiştir.

Kişisel verilerin yurt dışına aktarılması

MADDE 9- (Değişik:2/3/2024-7499/34 md.)

(1) Kişisel veriler, 5 inci ve 6 ncı maddelerde belirtilen şartlardan birinin varlığı ve aktarımın yapılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar hakkında yeterlilik kararı bulunması halinde, veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabilir.

(2) Yeterlilik kararı, Kurul tarafından verilir ve Resmî Gazete'de yayımlanır. Kurul, ihtiyaç duyması halinde ilgili kurum ve kuruluşların görüşünü alır. Yeterlilik kararı, en geç dört yılda bir değerlendirilir. Kurul, değerlendirme sonucunda veya gerekli gördüğü diğer hallerde, yeterlilik kararını ileriye etkili olmak üzere değiştirebilir, askıya alabilir veya kaldırabilir.

(3) Yeterlilik kararı verilirken öncelikle aşağıdaki hususlar dikkate alınır:

a) Kişisel verilerin aktarılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar ile Türkiye arasında kişisel veri aktarımına ilişkin karşılıklılık durumu.

b) Kişisel verilerin aktarılacağı ülkenin ilgili mevzuatı ve uygulaması ile kişisel verilerin aktarılacağı uluslararası kuruluşun tâbi olduğu kurallar.

c) Kişisel verilerin aktarılacağı ülkede veya uluslararası kuruluşun tâbi olduğu bağımsız ve etkin bir veri koruma kurumunun varlığı ile idari ve adli başvuru yollarının bulunması.

ç) Kişisel verilerin aktarılacağı ülkenin veya uluslararası kuruluşun, kişisel verilerin korunmasıyla ilgili uluslararası sözleşmelere taraf veya uluslararası kuruluşlara üye olma durumu.

d) Kişisel verilerin aktarılacağı ülkenin veya uluslararası kuruluşun, Türkiye'nin üye olduğu küresel veya bölgesel kuruluşlara üye olma durumu.

e) Türkiye'nin taraf olduğu uluslararası sözleşmeler.

(4) Kişisel veriler, yeterlilik kararının bulunmaması durumunda, 5 inci ve 6 ncı maddelerde belirtilen şartlardan birinin varlığı, ilgili kişinin aktarımın yapılacağı ülkede

de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla, aşağıda belirtilen uygun güvencelerden birinin taraflarca sağlanması halinde veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabilir:

a) Yurt dışındaki kamu kurum ve kuruluşları veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşları arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı ve Kurul tarafından aktarıma izin verilmesi.

b) Ortak ekonomik faaliyette bulunan teşebbüs grubu bünyesindeki şirketlerin uymakla yükümlü oldukları, kişisel verilerin korunmasına ilişkin hükümler ihtiva eden ve Kurul tarafından onaylanan bağlayıcı şirket kurallarının varlığı.

c) Kurul tarafından ilan edilen, veri kategorileri, veri aktarımının amaçları, alıcı ve alıcı grupları, veri alıcısı tarafından alınacak teknik ve idari tedbirler, özel nitelikli kişisel veriler için alınan ek önlemler gibi hususları ihtiva eden standart sözleşmenin varlığı.

ç) Yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı ve Kurul tarafından aktarıma izin verilmesi.

(5) Standart sözleşme, imzalanmasından itibaren beş iş günü içinde veri sorumlusu veya veri işleyen tarafından Kuruma bildirilir.

(6) Veri sorumluları ve veri işleyenler, yeterlilik kararının bulunmaması ve dördüncü fıkrada öngörülen uygun güvencelerden herhangi birinin sağlanamaması durumunda, arızi olmak kaydıyla sadece aşağıdaki hallerden birinin varlığı halinde yurt dışına kişisel veri aktarabilir:

a) İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermesi.

b) Aktarımın, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması.

c) Aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması.

ç) Aktarımın üstün bir kamu yararı için zorunlu olması.

d) Bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması.

e) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması.

f) Kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati olan kişinin talep etmesi kaydıyla aktarım yapılması.

(7) Altıncı fıkranın (a), (b) ve (c) bentleri, kamu kurum ve kuruluşlarının kamu hukukuna tâbi faaliyetlerine uygulanmaz.

(8) Veri sorumlusu ve veri işleyenler tarafından, yurt dışına aktarılan kişisel verilerin sonraki aktarımları ve uluslararası kuruluşlara aktarımlar bakımından da bu Kanunda yer alan güvenceler sağlanır ve bu madde hükümleri uygulanır.

(9) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.

(10) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

(11) Bu maddenin uygulanmasına ilişkin usul ve esaslar yönetmelikle düzenlenir.

Maddenin 11. fıkrası gereğince usul ve esasları belirlemek üzere hazırlanacak olan Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkındaki Yönetmelik 10 Temmuz 2024 tarih ve 32598 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir (Kişisel Verileri Koruma Kurumu, 2024b).

Kişisel Verilerin Korunması Kanunu'nun bazı maddelerinde (Madde 6,9,18), 7499 sayılı Kanunun 35' inci maddesiyle ve 1/6/2024 tarihinde yürürlüğe girmek üzere yapılan

değişiklikler, 12/3/2024 tarihli ve 32487 sayılı Resmî Gazete yayınlanmıştır. Yeni düzenlemelere tez içerisinde madde kapsamlarında yer verilmiştir. Buna göre, özel nitelikli kişisel verilerin işlenmesi, kişisel verilerin yurtdışına aktarımı konusunda bazı değişiklikler ile kabahatlerden sorumluluk ile kurulun vermiş olduğu idari para cezalarına karşı, idare mahkemelerinde dava açılabilmesi gibi yeni düzenlemeler getirilmiştir. Ayrıca kanuna Geçici 3. madde eklenmiştir.

GEÇİCİ MADDE 3- (Ek:2/3/2024-7499/36 md.)

(1) 9 uncu maddenin bu maddeyi ihdas eden Kanunla değiştirilmeden önceki birinci fıkrası, maddenin yürürlüğe giren değişik haliyle birlikte 1/9/2024 tarihine kadar uygulanmaya devam olunur.

Şeklinde düzenlemeye yer verilmiştir. Buna göre, kişisel verilerin yurt dışına aktarımı ile ilgili 9. Maddenin değişiklikten önceki 1. fıkra düzenlemesi, "(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz", yürürlüğe giren bu yeni haliyle birlikte 1/9/2024 tarihine kadar uygulanmaya devam edecektir.

Veri Sorumluları Sicili

MADDE 16- (1) Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili (Verbis) tutulur.

(2) Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.

(3) Veri Sorumluları Siciline kayıt başvurusu aşağıdaki hususları içeren bir bildirimle yapılır:

a) Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri.

b) Kişisel verilerin hangi amaçla işleneceği.

c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar.

ç) Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları.

d) Yabancı ülkelere aktarımı öngörülen kişisel veriler.

e) Kişisel veri güvenliğine ilişkin alınan tedbirler.

f) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

(4) Üçüncü fıkra uyarınca verilen bilgilerde meydana gelen değişiklikler derhâl Başkanlığa bildirilir.

(5) Veri Sorumluları Siciline ilişkin diğer usul ve esaslar yönetmelikle düzenlenir.

Maddenin 3/e fıkrasında, kişisel veri güvenliğine ilişkin alınan tedbirlerin, sicile kayıt başvurusunda açıklanması gerektiği açıkça belirtilmiştir. Kanun koyucu sadece hangi türden verilerin işlendiği ile ilgilenmemekte aynı zamanda bu verilerin korunması ile ilgili yeterli tedbir alınıp alınmadığı konusunu da önemsemektedir.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi

MADDE 7- (1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

(2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.

(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.

Örneğin; Personeline ait özlük verilerini sunucuda tutmakta olan bir şirket, çalışanlarından birinin işten ayrılması halinde, bu verinin bulunduğu sunucuyu tamamen yok edemeyeceği için veriye silme işlemi uygulayacaktır. Bu veri, bazı teknikler uygulanarak veri tabanı yöneticisi tarafından geri getirilebilecek durumda olmakla

birlikte diğer çalışanlar tarafından hiçbir şekilde erişilemez hale gelmiş olacaktır (Kişisel Verileri Koruma Kurumu, 2019d).

Böylece, işten ayrılmış olan eski çalışanın verileri silinerek yasanın amir hükmü yerine getirilmekte diğer taraftan veriye izinsiz girişler önlenerek bilgi güvenliği sağlanmış olmaktadır. Şirket açısından teknik, idari ve hukuki önlemler alınmış olmaktadır. Firma tarafından hazırlanacak bilgi güvenliği politikaları ile verilere kimlerin, ne zaman, ne şekilde ulaşabileceği konusunda yazılı düzenleme yapılması mümkündür. Bu örnek, bilgi güvenliğinin çok boyutluluğunu (teknik, hukuki, eğitim, farkındalık gibi) göstermesi açısından önemlidir.

Yasanın 7/3 fıkrasında usul ve esasların yönetmelik ile düzenleneceği belirtilmiştir. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, 28.10.2017 tarih ve 30224 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir (Kişisel Verileri Koruma Kurumu, 2017). Buna göre;

MADDE 5 – (1) Kanunun 16 ncı maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumluları, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlüdür.

(2) Kişisel veri saklama ve imha politikası hazırlanmış olması; kişisel verilerin Kanuna ve Yönetmeliğe uygun biçimde saklandığı, silindiği, yok edildiği veya anonim hale getirildiği anlamına gelmez.

(3) Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü altında bulunmayan veri sorumlularının, Kanun ve bu Yönetmelik uyarınca kişisel verileri saklama, silme, yok etme veya anonim hale getirme yükümlülükleri devam eder.

Düzenlemeden anlaşılacağı üzere, sicile kayıt sorumluluğu bulunan veri sorumluları, verilerin saklanması ve imhasına ilişkin politika hazırlamak zorundadır. Yalnız politika hazırlanmış olması kanun ve yönetmelikten kaynaklanan yükümlülüklerini ortadan kaldırmamayacaktır.

2.5.1.1.3 5237 Sayılı Türk Ceza Kanunu

25611 sayı ve 12 Ekim 2004 tarihli Resmi Gazete'de yayımlanan 5237 sayılı Türk Ceza Kanunu'nun "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı bölümü, 135 ila 140'ncı maddelerinde, kişisel verilerin korunmasına ilişkin hükümlere yer verilmiştir.

Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar

Kişisel verilerin kaydedilmesi

MADDE 135- (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

(2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.

Verileri hukuka aykırı olarak verme veya ele geçirme

MADDE 136- (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Verileri yok etmeme

MADDE 138- (1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

(2) (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması

MADDE 140- (1) Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Kişilere ilişkin verilerin yasalara aykırı şekilde kayıt edilmesi kanunda suç olarak düzenlenmiştir. Burada suç konusu, kişisel verilerdir ve bireylere ait olan her türlü bilgi kişisel veri olarak kabul edilmelidir. Bu verilerin, dijital ortamda veya fiziki ortamda kayıt edilmesi arasında da bir fark bulunmamaktadır (Baltacı Hukuk, 2016).

Türk Ceza Kanunu'nda Bilişim Alanındaki Suçlara ilişkin düzenlemelere de yer verilmiştir. Bu düzenlemeler Tablo 12'de yer almaktadır.

Tablo 12. Bilişim Suçları Düzenlemesi (Türk Ceza Kanunu, 2004)

Suç	Ceza
Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden (TCK 243/1)	1 Yıl Hapis veya Adli Para Cezası
Bir bilişim sisteminin işleyişini engelleyen veya bozan (TCK 244/1)	1-5 Yıl Hapis
Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen (TCK 244/2)	6 Ay – 3 Yıl Hapis

2.5.1.1.4 4721 Sayılı Türk Medeni Kanunu

24607 sayılı ve 8 Aralık 2001 tarihli Resmi Gazete'de yayımlanan 4721 sayılı Kanun'un, 23 ila 26'ncı maddelerinde kişilik hakları ve korunmasına ilişkin düzenlemelere yer verilmiştir.

B. Kişiliğin Korunması

I. Vazgeçme ve aşırı sınırlamaya karşı

MADDE 23- Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez.

Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlâka aykırı olarak sınırlayamaz.

II. Saldırıya karşı

1. İlke

MADDE 24- Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

2. Davalar

MADDE 25- Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.

Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir.

Davacının, maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır.

III. Ad üzerindeki hak

1. Adın korunması

MADDE 26- Adının kullanılması çekişmeli olan kişi, hakkının tespitini dava edebilir.

Adı haksız olarak kullanılan kişi buna son verilmesini; haksız kullanan kusurlu ise ayrıca maddî zararının giderilmesini ve uğradığı haksızlığın niteliği gerektiriyorsa manevî tazminat ödenmesini isteyebilir.

2.5.1.1.5 6098 Sayılı Türk Borçlar Kanunu

27836 sayılı ve 4 Şubat 2011 tarihli Resmi Gazete'de yayımlanan 6098 sayılı Kanunun 419'ncu maddesinde işveren tarafından işçiye ait kişisel verilerin kullanılmasına ilişkin düzenlemelere yer verilmiştir.

MADDE 419- İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. Özel kanun hükümleri saklıdır.

Bu yasal düzenleme, işçiye ilişkin kişisel verilerin işlenmesi ile ilgili olduğundan, 6698 sayılı Kişisel Verilerin Korunması Kanun'u özel kanun niteliğindedir. İlgili kanun'un, 'Kişisel Verilerin İşlenmesi' başlığını taşıyan ikinci bölümünde, verilerin hangi ilkelere göre işlenebileceği ayrıntılı şekilde düzenlenmiştir.

2.5.1.1.6 Diğer ulusal düzenlemeler

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

İçeriğin yayından çıkarılması ve erişimin engellenmesi

MADDE 9- (1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğin çıkarılmasını ve/veya erişimin engellenmesini de isteyebilir.

2.5.1.2 Uluslararası düzenlemeler

Kişisel verilerin korunması ile ilgili olarak devletler nezdinde yapılan ilk hukuki düzenleme, 1970'de Almanya'nın Hessen eyaletinde kabul edilmiştir. Bu yasal düzenlemeden sonra 1973 yılında İsveç Veri Koruma Kanunu, 1974 yılında ABD Özel Yaşamın Gizliliği Kanunu, 1977 yılında Federal Almanya Veri Koruma Kanunu ve 1978 yılında Fransa Elektronik Veri İşlemesi, Veriler ve Özgürlük Haklarına İlişkin Kanun çıkarılmıştır (Uslan ve Değirmenci, 2023).

Kişisel verilerin korunmasına ilişkin Uluslararası yasal düzenlemeler kronolojik olarak Tablo 13'de gösterilmiştir.

Tablo 13. Kişisel Verilerin Korunması ile İlgili Uluslararası Yasal Düzenlemeler (Kişisel Verileri Koruma Kurumu, t.y.) (Nitelikli Veri, t.y.) (Başar, 2020) (Dülger, 2019)

TARİH	YASAL DÜZENLEME
10 Aralık 1948	İnsan Hakları Evrensel Beyannamesi, Birleşmiş Milletler Genel Kurulu
3 Eylül 1953	İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi
23 Mart 1976	Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme, Birleşmiş Milletler Genel Kurulu
23 Eylül 1980	OECD'nin Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri
28 Ocak 1981	108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
14 Aralık 1990	Birleşmiş Milletler'in Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri
25 Ekim 1998	95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlemantosu ve Avrupa Konseyi Direktifi
7 Aralik 2000	Avrupa Birliği Temel Haklar Şartı
08 Kasım 2001	181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol
12 Temmuz 2002	2002/58/EC Sayılı Elektronik Haberleşme ve Gizlilik Direktifi
15 Mart 2006	2006/24/EC Sayılı İletişim Trafik Verilerinin Saklanması Direktifi
18 Mayıs 2018	Kişisel Verilerin İşlenmesine İlişkin Bireylerin Korunmasına İlişkin Sözleşmede Değişiklik Yapılmasına Dair Protokol'ün (108+)
25 Mayıs 2018	2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

Bu düzenlemeler, Avrupa Konseyi Düzenlemeleri, Avrupa Birliği Düzenlemeleri ve diğer düzenlemeler olarak sınıflandırılabilir.

2.5.1.2.1 Avrupa Konseyi düzenlemeleri

- 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

1970'den itibaren Avrupa Konseyi tarafından, kişisel verilerin korunması konusunda çalışmalar yapılmıştır. Çalışmalar sonucunda, Strazburg'da imzaya açılan *"Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"* 1 Ekim 1985 tarihinde yürürlüğe girmiştir. Türkiye, 28 Ocak 1981'de bu sözleşmeyi imzalayan ilk ülkelerden birisi olmuştur. Sözleşme iç hukukumuza, 17 Mart 2016 tarih ve 29656 sayılı Resmi Gazete'de yayımlanarak dâhil edilmiştir. Sözleşmenin ana amacı; her üye ülkede, yerleşim yeri veya uyruğu ne olursa olsun, bireylerin temel haklarını ve özgürlüklerini ve kişisel nitelikteki bilgilerinin otomatik şekilde işleme tabi tutulması karşısında özel yaşamlarını güvenceye almaktır (Kişisel Verileri Koruma Kurumu, t.y.).

- Kişisel Verilerin İşlenmesine İlişkin Bireylerin Korunmasına İlişkin Sözleşmede Değişiklik Yapılmasına Dair Protokol (108+)

Protokol 18 Mayıs 2018 tarihinde kabul edilmiştir. Protokolün imzalanması ile, 108 No'lu Sözleşme güncellenmiş ve bilişim teknolojilerindeki yeniliklere uyum sağlanması, dijital gizliliği koruma süreçlerinin güçlendirilmesi ve sözleşmenin izleme mekanizmalarının güçlendirilmesi, iyileştirilmesi amaçlanmıştır (Dülger, 2019).

- 181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol

Bu protokol ile, taraf devletler, ülkelerinde denetleyici bir makam kurma sözü vermişlerdir. Bu makam, üye ülkelerde kişisel verilerin korunması konusunda görevlerini bağımsız bir şekilde ifa edecektir. Protokol ülkemizde 8 Kasım 2001 tarihinde imzalanmıştır ve 5 Mayıs 2016 tarihli 29703 sayılı Resmi Gazete'de yayımlanarak iç hukuka dâhil edilmiştir (Kişisel Verileri Koruma Kurumu, t.y.).

- Avrupa İnsan Hakları Sözleşmesinin İlgili Hükümleri

İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi'nde, kişisel verilerin işlenmesi konusunda direkt bir düzenleme bulunmamakla birlikte Avrupa İnsan Hakları Mahkemesi, içtihatlarıyla kişisel verileri koruma altına almıştır. Sözleşme, Avrupa Konseyi tarafından hazırlanmış, 4 Kasım 1950'de Roma'da imzalanıp 3 Eylül 1953'te yürürlüğe girmiştir. Sözleşme'nin *"Özel ve Aile Hayatına Saygı Hakkı"* başlıklı

8’nci maddesi.. ile kişisel verilerin korunmasına doğrudan bir yöneltme yapılmamakla birlikte, aile hayatına ve özel hayata saygı hakkı kapsamında yer alan kişisel veriler hukuken koruma altına alınmıştır (Kişisel Verileri Koruma Kurumu, t.y.).

- 2002/58/EC Sayılı Elektronik Haberleşme ve Gizlilik Direktifi

Elektronik haberleşme alanında mobil teknolojiler gibi pek çok yeniliğin giderek artan oranlarda kullanılması bu sektöre ilişkin özel düzenlemelerin yapılmasını kaçınılmaz hale getirmiştir. Bu çerçevede Avrupa Birliği (AB)’nde elektronik haberleşme sektörüne ilişkin olarak kişisel verilerin işlenmesi ve gizliliğinin korunması hususunda ilk özel düzenlemeyi, Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Avrupa Parlamentosu ve Konseyi‟nin 15 Aralık 1997 tarih ve 97/66/EC sayılı Direktifi oluşturmuştur. Direktifin piyasalar ve elektronik haberleşme hizmetleri teknolojilerindeki ilerlemelere uyumlu hale getirilmesi amacıyla 2002 yılındaki düzenleyici paket içerisinde elektronik haberleşme sektörüne ilişkin Elektronik Haberleşme Sektöründe Gizliliğin Korunması ve Kişisel Bilgilerin İşlenmesine ilişkin 12 Temmuz 2002 tarihli Avrupa Parlamentosu ve Konseyi‟nin 2002/58/EC sayılı Direktifi yayımlanmış (Veri Gizliliği Direktifi) ve 97/66/EC sayılı Direktif yürürlükten kaldırılmıştır (Koca ve Tözer, 2012).

2.5.1.2.2 Avrupa Birliği düzenlemeleri

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

Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif, 1995’de Avrupa Parlamentosu ve Avrupa Konseyi tarafından kabul edilmiştir. Direktif, Avrupa Birliği'nde kişisel verilerin korunmasını sağlamak ve buna ilişkin düzenlemelerin uyumlu hale getirilmesi bakımından önemlidir. Birlik üyesi devletler, kişisel verilerin korunmasına ilişkin yasal düzenlemelerini bu düzenlemeyi temel alarak yapmışlardır. Ülkemizde kişisel verilerin korunması kanunu da bu direktif esas alarak hazırlanmıştır (Nitelikli Veri, t.y.).

- 2006/24/EC Sayılı İletişim Trafik Verilerinin Saklanması Direktifi

7 Temmuz 2005 tarihinde Londra Metrosu'ndaki bombalı saldırının ardından ve saldırının da etkisi ile, 2006/24/EC sayılı İletişim Trafik Verilerinin Saklanması Direktifi 15 Mart 2006 tarihinde kabul edilmiştir. Direktifte, trafik iletişim ve yer bilgileri düzenlenmiştir. Buna göre, iletişim hizmetlerini kullanan kişilerin iletişim içeriği dışındaki bilgileri sadece ciddi suç şüphesi durumunda saklanabilecektir (Dülger, 2019).

- Avrupa Birliği Temel Haklar Şartı

Avrupa Birliği Temel Haklar Şartı, 1 Aralık 2009 tarihli Lizbon Anlaşması'nın kabulü ile bağlayıcı hale gelmiştir. Bu düzenleme, kişisel verilerin korunması hakkını bağımsız ve ayrı bir hak olarak tanımlamıştır. Böylelikle, kişisel verilerin korunması hakkı, insan hakları ile temel hak ve özgürlükler kapsamında kabul edilerek özel hayatın gizliliğinden ayrı tutulmuş ve önemi ortaya konulmuştur (Dülger, 2019).

- 2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

Avrupa Birliği, 2012 yılında yeni bir tüzük çalışması başlatmıştır. Buradaki amaç, kişisel verilerin korunması konusunda oluşan gereksinimleri karşılamaktır. Tüzük 25 Mayıs 2018'de yürürlüğe girmiştir (Nitelikli Veri, t.y.). Bu tüzük ile birlikte, Avrupa Birliği üyesi devletlerin iç hukuk düzenlemelerindeki kişisel verilerin korunmasına ilişkin farklı uygulamaları ortadan kaldırılmıştır.

6698 sayılı Kişisel Verilerin Korunması Kanunu, 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi esas alınarak hazırlanmıştır. Bu direktif, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesi ile birlikte ilga olmuştur. Bu durumda, GDPR ile KVKK düzenlemesi arasında bazı farklılıklar ortaya çıkmıştır. Ülkemizin tüzük ile uygun bir yasal çerçeveye sahip olması önemlidir (Uslan ve Değirmenci, 2023).

GDPR, AB üyesi ülkelerde yürürlüğe girmiş bir düzenleme olmak ile birlikte, belirli koşullar altında, AB üyesi ülkelerde ikamet etmeyen veri sorumlularına da uygulanabilmektedir. Özellikle AB üyesi devletlerle iş ilişkisinde bulunan lojistik işletmelerinin dikkate alması gereken bir düzenlemedir.

2.5.1.2.3 Diğer uluslararası düzenlemeler

Kişisel verilerin korunmasına ilişkin olarak uluslararası düzeyde, Uluslararası Çalışma Örgütü'nün (OECD) 23 Eylül 1980 de kabul edilen "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri" ile Birleşmiş Milletler'in 14 Aralık 1990 da kabul edilen "Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri" bulunmaktadır (Kişisel Verileri Koruma Kurumu, 2019e).

Kişisel verilerin korunması hakkı, Birleşmiş Milletler tarafından özel hayatın gizliliği kapsamında ele alınmaktadır. Ancak, teknolojideki ilerlemeler ve bilgisayar kullanımının artması, Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler'in (BM Rehber İlkeleri) yayımlanmasını zorunlu kılmıştır. Bu ilkeler, doğrudan kişisel verilerin korunması hakkına dair ilk Birleşmiş Milletler düzenlemesidir (Dülger, 2019).

Birleşmiş Milletler Genel Kurulu 10 Aralık 1948'de aldığı karar ile, İnsan Hakları Evrensel Beyannamesi'ni ilan etmiştir. Ülkemizde 27.05.1949 tarihinde Resmi Gazete'de yayınlanmıştır. Bu düzenleme, ülkelerin iç hukuklarında doğrudan doğruya uygulanmasa da, insan haklarının yerel hukuka aktarılmasında rehberlik eden bir rol oynamıştır. Düzenlemeye göre, kişilerin özel hayatları ile aile, konut ve haberleşme hakkına keyfi müdahale edilemeyeceği, isim ve şerefine saldırılamayacağı belirtilerek, aksine davranışlara karşı yasalarca korunma hakkının bulunduğu belirtilmiştir. Birleşmiş Milletler Genel Kurulu'nun aldığı karar ile, Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme 23 Mart 1976 tarihinde yürürlüğe girmiştir. Türkiye sözleşmeyi imzalayarak 18.06.2003 tarihli Resmi Gazete'de yayımlanmıştır. Danıştayın kişisel veriler ile ilgili davalarda, davaya konu işlemin uluslararası sözleşmelerde belirtilen temel düzenlemelere uygun olup olmadığını araştırdığı ve Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'ne atıfta bulunduğu görülmektedir (Başar, 2020).

Kaliforniya Tüketici Gizliliği Yasası, Haziran 2018'de yürürlüğe girmiştir ve Avrupa Birliği Genel Veri Koruma Tüzüğü'nünkilere benzer hükümler içermektedir. Bu düzenlemelerin coğrafik alanı sınırlı görünüyor olsa da, Avrupa Birliği veya Kaliforniya ile ticaret faaliyet yürüten tüm pazarları etkilemektedir (Hürriyet Gazetesi , 2020).

Lojistik işletmeleri, hizmetlerini ulusal ve uluslararası alanda sunan sektörlerden birisidir. Özellikle verilerin işlenmesi bakımından yerel mevzuat yanında hizmet sunulan ve veri işlenen diğer ülke mevzuatlarına uyumun önemi büyüktür.

Avrupa Birliğinde, ülkelerin bilgi güvenliği politikaları, yasal düzenlemelerle ifade edilir. Hukuki düzenlemeler, üye ülkelerin üzerinde anlaşmış oldukları politikaların hayata geçirilmesi anlamına gelmektedir. Diğer taraftan üye ülkeler birlik direktifleri ve sözleşmelere uygun olarak iç hukuklarını düzenlemektedir. Böylece, Avrupa Birliği ülkeleri bilgi güvenliği konusunda yasal düzenlemeler yoluyla ortak bir yaklaşım benimsemekte ve bu sayede bilgi güvenliğini korumaya çalışmaktadır. Avrupa Birliğinde bilgi güvenliği politikalarının tanzim edilmesinde, tehdit ve riskler temel alınmaktadır. İncelemeler sonrasında, teknolojiye bağlı olan çeşitli tehdit (zararlı kodlar, gizlilik ihlalleri, servis ve yer sağlayıcı güvenilirliği gibi) belirlenmekte ve belirlenen politikalar yasalaştırılarak uygulanmaktadır. Birlik içinde iş yapan şirketler yasal yükümlülüklere uymak mecburiyetindedir (Henkoğlu ve Yılmaz, 2013).

Hızla gelişen teknoloji karşısında, yasal düzenlemelerin, gelişmelerin gerisinde kalmadan ivedilikle gözden geçirilerek ihtiyaca uygun olarak revize edilmesi önemlidir. Zararlı saldırıların ortaya çıkması halinde söz konusu fiillerin nasıl değerlendirileceği, oluşturulacak yasal düzenlemeler ile mümkün olacaktır.

Bilgi güvenliği politikalarının hazırlanması ve geliştirilmesinde faydalanılan uluslararası standartlar, şirketlerin kendi idare sistemleri ve hukuki şartlarına bağlı şekilde uygulandığında veri güvenliğine ciddi katkı sağlamaktadır (Henkoğlu, 2015).

2.5.1.3 Kişisel Verilerin Korunması Kanunu ve Genel Veri Koruma Tüzüğü (GDPR) değerlendirme

Genel Veri Koruma Tüzüğü ile, Avrupa Birliği'nin verileri koruma sistemi yenilenerek güncellenmiştir. Verileri işlenen bireyler bakımından yeni güvenceler ve koruma sistemi getiren bu araç, veri kayıt eden firmalar bakımından ise yeni sorumluluklar getirmektedir. GDPR'ın uygulama alanı genişletilmiştir. Bu sebeple sorumlu olacak firmalar sadece Avrupa Birliğinde yerleşik olanlar değil, AB dışında ki firmalarda belli koşullar ile yeni düzenlemeye uyum sağlama zorunluluğundadır (Dülger, 2019).

Tüzüğün getirdiği bazı değişiklikler;

- Yeni düzenleme ile ihlallere karşı uygulanacak para cezaları ağırlaştırılmıştır. İhlallerde yirmi milyon Euro'ya ulaşabilen ağır yaptırımlar düzenlenmiştir. Kişisel Verilerin Korunması Kanunu'nda idari para ceza miktarları en fazla bir milyon Türk Lirası olarak düzenlenmiştir. Bu cezaların her yıl yeniden değerleme oranları gereğince artışı yapılacak olsa da, bu oranlar GDPR kadar ağır bir yaptırım özelliği taşımamaktadır.

- Tüzük'te yer verilen bir diğer düzenleme, veri kayıt etmenin riskli olduğu hallerde "veri koruma etki değerlendirmesi" yapılacak olmasıdır. 6698 sayılı Kanun'da, kişisel veri işlemenin yaratabileceği risklerin değerlendirilmesi ve bu değerlendirmeden sonra işleme faaliyetiyle ilgili bir denetim otoritesine başvurulması uygulaması bulunmamaktadır (Uslan ve Değirmenci, 2023).

GDPR'ın bölgesel kapsamı genişletilmiştir. Belirlenen bazı durumlarda tüzüğün AB dışındaki ülkelere de uygulanabileceği belirtilmiştir. Hukuki bir işleme faaliyetinden sözedebilmek için gereken şartlar sıkılaştırılmış, verileri işlenen kişilere yeni haklar tanınmış ve var olan hakları genişletilmiştir. Bu kapsamda Tüzük ile birlikte "unutulma hakkı" ve "veri taşınabilirliği hakkı" ilk kez yasal bir zeminde düzenlenmiştir. Veri sorumluları ve veri işleyenlerin yükümlülükleri arttırılmış ve somut hale getirilmiştir. Onlara bilgi ve tavsiye vermek üzere veri koruma görevlileri atanması gerekliliği açıkça düzenlenmiştir. Veri ihlali halinde durumu denetim makamı ve ilgililere bildirme sorumluluğu veri sorumlusu ve veri işleyen için öngörülmüştür. Birlik üyesi ülkeler, Tüzüğün ihlal edilmesi durumunda idari cezalar uygulamaları konusunda denetim makamlarını yetkilendirmiştir. GDPR'ın ağır para cezaları getirmesi nedeniyle, veri işleyenlerin, bilhassa firmaların GDPR'a uyum sağlamalarının önemi daha belirgin hale gelmiştir (Dülger, 2019).

Tüzüğün uygulanabilirlik kapsamına bakıldığında, Genel Veri Koruma Tüzüğü hükümleri, Avrupa birliği ile iş ilişkisi içinde bulunan işletmeler için önemlidir. GDPR uygulama kapsamı belgenin 3.maddesinde şöyle belirtilmiştir;

MADDE 3

Bölgesel kapsam

1. Bu Tüzük, işlemenin Birlik içinde gerçekleşip gerçekleşmediğine bakılmaksızın, kişisel verilerin, Birlik içindeki bir veri kontrolör veya veri işleyenin kuruluşunun faaliyetleri bağlamında işlenmesine uygulanır.

2. Bu Tüzük, işleme faaliyetlerinin aşağıdaki hususlarla ilgili olması halinde, Birlik içinde bulunan veri sahiplerinin kişisel verilerinin Birlik içinde kurulu olmayan bir veri kontrolör veya veri işleyen tarafından işlenmesine uygulanır: (a) Veri sahibinin ödeme yapmasına gerek olup olmadığına bakılmaksızın, Birlik içindeki söz konusu veri sahiplerine mal veya hizmetlerin sunulması veya (b) Davranışları Birlik içinde gerçekleştiği ölçüde, davranışlarının izlenmesi.

3.Bu Tüzük kişisel verilerin, Birlik içinde kurulu bulunmayan, ancak Üye Devlet hukukunun uluslararası kamu hukuku vasıtasıyla uygulandığı bir yerde bir veri kontrolör tarafından işlenmesine uygulanır (T.C. Dışişleri Bakanlığı, 2023).

Bu düzenlemeler ile GDPR'a, KVKK'ndan farklı olarak daha geniş bir yetki alanı sağlanmıştır. Şöyleki, AB üyesi ülkelerde yaşayan veri sahibinin kişisel verilerini işleyen tüm firmalar, bulundukları konum önemli olmaksızın GDPR'a uyum ile yükümlü olacaklardır (Güden ve Girinti, t.y.).

Bu itibarla, mukim olmak (lojistik işletme açısından AB'de deposunun bulunması, irtibat ofisi olması gibi) ve veri işleniyor ise, Avrupa Birliğinde bulunan kişilere mal, hizmet sunuluyor ise (dijital ortam üzerinden sunulması da dahil) ve yine bir ürünü pazarlamak için Avrupa Birliği mukimlerine yönelik profil araştırması, Ip adresleri, isim bilgileri, anket vb, işlemler yapılıyor ise kısaca kişiler izlemeye alındı ise yine GDPR' a tabi olunması durumu söz konusudur. Yurtdışına lojistik hizmet sunan, veri sorumlusu lojistik işletmeler açısından önemli bir düzenlemedir.

Avrupa Birliği üyesi ülkeler GDPR'e tabidir. Birlik üyesi olmayan birçok ülke de bu düzenlemeye benzer nitelikte, veri güvenliğini sağlamaya ilişkin hukuki düzenlemeler hazırlamaktadır. Bu açıdan GDPR, model bir çerçeve oluşturmaktadır. Birlik üyesi

ülkelerde bulunan veri sahiplerine ilişkin bilgileri işleyen, saklayan veya bulunduran firmalar bakımından geçerli bir düzenlemedir. AB üyesi devletlerde faaliyette bulunan, Avrupa Birliği vatandaşlarına eşya veya hizmet satan, veri sahiplerinin hareketlerini takip eden firmalar GDPR'ye uyma yükümlülüğündedir. Belirli hassas nitelikli veri kategorileri için ayrı bir koruma söz konusudur (Selvan, 2023).

GDPR'ın yürürlüğe girdiği tarihten itibaren müşteri verilerini korumakta başarısız olan şirketlere yüksek GDPR cezaları kesilmiştir. Örneğin; Amazon.com Inc.'e 746 milyon Euro, WhatsApp İrlanda'ya 225 milyon Euro, Hennes & Mauritz-H&M'ye 35,3 Euro, Meta'nın sahibi olduğu Instagram'a 405 milyon Euro, İngiliz Havayolları British Airways'e 204 milyon Euro, Marriot Oteller Zincirine 111 milyon Euro ceza kesilmiştir (Göktaş, 2022) (ICT Media, 2019).

Genel Veri Koruma Tüzüğü ile getirilmiş olan tüm bu yeni düzenlemeler ve uygulama sınırlarının genişletilmiş olması, düzenlemelere uymayanlara kesilen yüksek para cezaları karşısında yasal düzenlemelerin yeniden gözden geçirilmesi ihtiyacı oluşmuştur. Kişisel Verilerin Korunması Kanunu'nun GDPR ile uyumlu duruma getirilmesi ihtiyacı bulunmaktadır.

Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı 11. Kalkınma Planı'nda (2019-2023), "*Sanayi işletmelerinin siber güvenlik konusunda farkındalık ve yetkinlikleri artırılarak, tedarik zincirlerinde güvenlik önlemleri alınacağı….Kişisel Verilerin Korunması Kanunu'nun Avrupa Birliği Genel Veri Koruma Tüzüğü dikkate alınarak güncelleneceği"* ifade edilmiştir (T.C. Cumhurbaşkanlığı, 2019, s. 75,110). Bu ihtiyaç ve planlamalar aynı şekilde Kişisel Verileri Koruma Kurumu'nun 2024-2028 Stratejik Plan'ında tekrar edilmiştir; "*6698 sayılı Kişisel Verilerin Korunması Kanunu AB'nin Genel Veri Koruma Tüzüğü dikkate alınarak güncellenecektir"* şeklindedir (Kişisel Verileri Koruma Kurumu, t.y., s. 35).

Diğer taraftan, lojistik işletmeleri ilgilendirmesi açısından, Ticaret Bakanlığı tarafından ihracatçıların desteklenmesi yönünde çalışmalar yapılmaktadır. Onların, uluslararası tedarik zincirlerinde hızlı ve rekabetçi fiyatlarla ilerlemelerini sağlamak ve kritik piyasalardaki ihracat verimliliğini sürekli hale getirecek ortam ve olanakları sağlamak için yurt dışı lojistik ağlarının kurulması ve/veya işletilmesi ile desteklenmesi çalışmaları

yürütülmektedir. Konuya ilişkin olarak "Yurt Dışı Lojistik Dağıtım Ağlarının Desteklenmesi Hakkında Karar" 20 Nisan 2022 tarihinde 31815 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir (T.C. Resmi Gazete, 2022). Alınan karar ile yurtdışında lojistik dağıtım ağlarının kurulması, işletilmesi desteklenecektir. Bu itibarla, Bakanlık tarafından, Yurt Dışı Lojistik Dağıtım Ağları (YLDA) Projesi kapsamında Avrupa'da 4, ABD'de 2 merkeze onay verilmiştir. Tedarik zincirlerinin yeniden kurulduğu, ticaret rotalarının baştan kurgulandığı bu dönemde (İstanbul Ticaret, 2024) yaşanan değişiklikler karşısında, lojistik işletmelerin işlediği verilerin ulusal yasal düzenlemeler ile birlikte aynı zamanda uluslararası yasal düzenlemeler gereğince de korunması gerekliliği bulunmaktadır.

2.5.2 Tüzel kişi verilerinin korunmasına ilişkin yasal düzenlemeler

Yasal düzenlemelerimizde, tüzel kişilere ait verilerin korunması gerekliliği; bu verilerin tanımlanması suretiyle düzenlenmiştir. Hukuk doktrinde, tüzel kişilerin veri koruma haklarına dayanak teşkil eden temel haklar olarak tüzel kişinin kişilik hakları, mülkiyet hakkı, sözleşme ilişkileri ve haksız fiil koruması şeklinde bir ayırıma gidilmektedir (Küpeli, 2019). Tüzel kişinin ticari sırlarının korunmasını düzenleyen özel bir kanun bulunmamaktadır. Bu tür bilgiler, Ticaret Kanunu haksız rekabet hükümleri ile korunmakta olup ayrıca, Bankacılık Kanunu ve Elektronik Haberleşme Kanunu ile Rekabetin Korunması Hakkında Kanun gibi özel kanunlar kapsamında korunur (Baylan, 2020).

Elektronik haberleşme kanunu ile; "*Bilgi Teknolojileri ve İletişim Kurumunun, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır"* şeklinde ki sorumluluğuna yer verilmiştir (Elektronik Haberleşme Kanunu, 2008).

2.5.2.1 Ulusal düzenlemeler

2.5.2.1.1 1982 Anayasası

Anayasa'nın 17/1'nci maddesi ile korumaya alınan, "Herkesin yaşama ve maddi manevi varlığını koruma geliştirme hakkı", tüzel kişiler açısından ticari sırların gayri maddi mal olmaları sebebiyle tüzel kişiye ait varlıkların korunması yönünden kabul göreceği

doktrinde belirtilmiştir. Benzer şekilde, Anayasa'nın 20/1'nci maddesinde belirtilen "Herkesin özel ve aile hayatına saygı gösterilmesini isteme hakkının", tüzel kişiler bakımından, tüzel kişilerin ticari alandaki gizliliklerini korumaya alan bir üst norm olarak değerlendirilebileceği doktrinde kabul edilmiştir (Küpeli, 2019).

2.5.2.1.2 4721 Sayılı Türk Medeni Kanunu

Tüzel kişilerin, bireylere özgü haklar dışında, gerçek kişiler gibi sahip oldukları kişilik hakları bulunmaktadır. Tüzel kişiler de, bireyler gibi, isim, kredi bilgisi, ticari sırlar, onur ve itibar gibi kişilik değerleri ve haklarına sahiptir. Bu nedenle, adın korunmasına yönelik sağlanan korumadan tüzel kişilerin de faydalanabileceği kabul edilmektedir. Emsal bir Yargıtay kararında; "Dava konusu olayda, Medeni Kanun'un adın korunması hükümlerine atıf yapılmak suretiyle ismin gasp edildiğine karar vererek tüzel kişi lehine manevi tazminata hükmetmiştir". Tüzel kişilerin adına yönelen saldırılar, aynı zamanda tüzel kişiliğin verilerine de saldırı anlamına gelecektir. Tüzel kişiliğin ödeme durumu, kredi bilgileri, iflas durumu, kara listeye alınma değerlendirmelerinin, tüzel kişiliğin şeref ve haysiyetini etkileyeceği belirtilmiştir (Küpeli, 2019).

Medeni Kanun'un 48. maddesinde tüzel kişilerin hak ehliyeti düzenlenmiştir.

B. Hak ehliyeti

MADDE 48- Tüzel kişiler, cins, yaş, hısımlık gibi yaradılış gereği insana özgü niteliklere bağlı olanlar dışındaki bütün haklara ve borçlara ehildirler.

Bu düzenlemelere göre, gerçek kişiler ve tüzel kişiler hak sahipliği açısından eşit konumdadır; yalnızca hak sahipliği ve borç yükümlülüğü bakımından aralarında kapsam ve nicelik açılarından farklar bulunmaktadır (Arslan, 2018).

2.5.2.1.3 6102 Sayılı Türk Ticaret Kanunu

27846 sayılı ve 14 Şubat 2011 tarihli Resmi Gazetede yayımlanan 6102 Sayılı Kanunun 16. maddesinde tüzel kişilerin tanımı yapılmıştır.

II - Tüzel kişiler

MADDE 16- (1) Ticaret şirketleriyle, amacına varmak için ticari bir işletme işleten vakıflar, dernekler ve kendi kuruluş kanunları gereğince özel hukuk hükümlerine göre yönetilmek veya ticari şekilde işletilmek üzere Devlet, il özel idaresi, belediye ve köy ile diğer kamu tüzel kişileri tarafından kurulan kurum ve kuruluşlar da tacir sayılırlar.

Türk Ticaret Kanunu'nun 16' ncı maddesi uyarınca, tacirler, dernekler, ticari işletme işleten vakıflar ve tacir sayılan kamu kurum kuruluşlarının ticari sırra haiz olabilecekleri ve bu korumadan yararlanabilecekleri hükme bağlanmıştır (Küpeli, 2019).

Ticari sırlar işletmeler için, piyasadaki rekabetin devamı ve ekonomik değeri bulunması sebebi ile hayati öneme haizdir. Yasal düzenlemelerimize göre, Türk Ticaret Kanunu 54 ile 63. maddeleri arasında düzenlenmiş olan haksız rekabet hükümleri ile korunur. Haksız rekabet, dürüstlük ilkesine aykırı şekilde ekonomik rekabetin kötüye kullanılması anlamına gelmektedir. Anayasa'da doğrudan haksız rekabet ile ilgili bir düzenleme bulunmamaktadır. Fakat Anayasa'nın 48. maddesine göre; "Herkes, dilediği alanda çalışma ve sözleşme hürriyetlerine sahiptir. Özel teşebbüsler kurmak serbesttir." Özel teşebbüs kurma özgürlüğünün kabulü, rekabet etme hakkını da beraberinde getirir (Sulu, 2020).

II - Dürüstlük kuralına aykırı davranışlar, ticari uygulamalar

MADDE 55- (1) Aşağıda sayılan hâller haksız rekabet hâllerinin başlıcalarıdır:

b) Sözleşmeyi ihlale veya sona erdirmeye yöneltmek; özellikle;

3.İşçileri, vekilleri veya diğer yardımcı kişileri, işverenlerinin veya müvekkillerinin üretim ve iş sırlarını ifşa etmeye veya ele geçirmeye yöneltmek,

1/b-3 de belirtilen bu sırlar, bir malın formülü ya da üretim tekniği veya modeli gibi üretime ilişkin sırlar olabileceği gibi, işletmeye ilişkin müşteri listeleri, müşterilere yapılan iskontolar ya da bunların satın aldıkları malı nasıl ödediklerine ilişkin bilgiler ve o işletmenin gelecekteki yıllara ilişkin üretim tasavvurları gibi sırlar da olabilir. Bu düzenlemenin uygulanması için, üretim veya iş sırrı niteliğindeki ticari sırları açıklamaya

veya elde etmeye teşvik etmek yeterlidir. Bilginin, açıklandıktan sonra ya da ele geçirildikten sonra kullanılıp kullanılmadığı önemli değildir (Sulu, 2020).

İşçinin, işini yapmak üzere öğrendiği bilgileri üçüncü kişilere bir maddi karşılık ile açıklaması durumunda, bilgiyi edinen kişi Türk Ticaret Kanunu 55/1(b)(3) maddesi gereğince haksız rekabet yapmış olacaktır (Bağrıaçık, 2017) (Baylan, 2020).

II - Dürüstlük kuralına aykırı davranışlar, ticari uygulamalar

MADDE 55- (1) Aşağıda sayılan hâller haksız rekabet hâllerinin başlıcalarıdır:

d) Üretim ve iş sırlarını hukuka aykırı olarak ifşa etmek; özellikle, gizlice ve izinsiz olarak ele geçirdiği veya başkaca hukuka aykırı bir şekilde öğrendiği bilgileri ve üretenin iş sırlarını değerlendiren veya başkalarına bildiren dürüstlüğe aykırı davranmış olur.

Hukuk ve etik kurallarına aykırı bir biçimde edinilen ticari sırların kullanılması ve ifşası haksız rekabettir ve ticari sırların ihlali demektir. Buradaki ticari sırlar, tacirin oluşturduğu ve üçüncü kişilerden gizlemek istediği ve bunda haklı olduğu bilgilerin tümüdür. Bunlara örnek olarak, adres ve isim ile birlikte başkaca bilgilerinde bulunduğu müşteri listesi, firmanın dağıtım, organizasyon, üretim alanlarında oluşturduğu know-how niteliğindeki teknik-ticari bilgi ve tecrübelerin değerlendirilmesi verilebilir. Üretim veya iş sırrı kapsamında bulunan bir bilginin hukuka uygun olarak öğrenilmesi sonrasında hukuka aykırı olarak açıklanması da bu kapsamda genel koruma himayesi görecektir. Bu ticari sırlardan mali bir gelir temin edilip edilmediğinin bir önemi bulunmamaktadır (Sulu, 2020).

Üretim ve diğer iş ile ilgili sırların yasalara aykırı şekilde temin edilerek başkaları ile paylaşıldığına ilişkin Yargıtayın içtihatları bulunmaktadır. Bazen bu öğrenme, işyeri personelinin yardım ve desteği ile olmakta, görevini kötüye kullanan personelin yardımı ile yetkisiz kişilerin üretim ortamlarına girişi sağlanarak sözkonusu bilgiler elde edilmektedir. Bu türden olayların engellenebilmesi için şirket yönetiminin yetkilendirme prosedür ve politikalarını hazırlaması ve görevlendirmeleri yapması gerekir. Ayrıca uygulamaların sık aralıklarla denetlenmesi sağlanmalıdır.

B) Hukuki sorumluluk

I - Çeşitli davalar

MADDE 56- (1) Haksız rekabet sebebiyle müşterileri, kredisi, meslekî itibarı, ticari faaliyetleri veya diğer ekonomik menfaatleri zarar gören veya böyle bir tehlikeyle karşılaşabilecek olan kimse;

a) Fiilin haksız olup olmadığının tespitini,

b) Haksız rekabetin men'ini,

c) Haksız rekabetin sonucu olan maddi durumun ortadan kaldırılmasını, haksız rekabet yanlış veya yanıltıcı beyanlarla yapılmışsa bu beyanların düzeltilmesini ve tecavüzün önlenmesi için kaçınılmaz ise, haksız rekabetin işlenmesinde etkili olan araçların ve malların imhasını,

d) Kusur varsa zarar ve zıyanın tazminini,

e) Türk Borçlar Kanununun 58 inci maddesinde öngörülen şartların varlığında manevi tazminat verilmesini, isteyebilir.

Haksız rekabet eylemine maruz kalarak zarar gören taraf, sözkonusu hukuki haklardan yararlanarak zararlarının tazminini isteyebilecektir.

II - Çalıştıranın sorumluluğu

MADDE 57- (1) Haksız rekabet fiili, hizmetlerini veya işlerini gördükleri sırada çalışanlar veya işçiler tarafından işlenmiş olursa, 56 ncı maddenin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı davalar, çalıştıranlara karşı da açılabilir.

(2) 56 ncı maddenin birinci fıkrasının (d) ve (e) bentlerinde yazılı davalar hakkında Türk Borçlar Kanunu hükümleri uygulanır.

C) Ceza sorumluluğu

I - Cezayı gerektiren fiiller

MADDE 62- (1) a) 55 inci maddede yazılı haksız rekabet fiillerinden birini kasten işleyenler,

b) Kendi icap ve tekliflerinin rakiplerininkine tercih edilmesi için kişisel durumu, ürünleri, iş ürünleri, ticari faaliyeti ve işleri hakkında kasten yanlış veya yanıltıcı bilgi verenler,

c) Çalışanları, vekilleri veya diğer yardımcı kimseleri, çalıştıranın veya müvekkillerinin üretim veya ticaret sırlarını ele geçirmelerini sağlamak için aldatanlar,

d) Çalıştıranlar veya müvekkillerden, işçilerinin veya çalışanlarının ya da vekillerinin, işlerini gördükleri sırada cezayı gerektiren bir haksız rekabet fiilini işlediklerini öğrenip de bu fiili önlemeyenler veya gerçeğe aykırı beyanları düzeltmeyenler,

fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, 56 ncı madde gereğince hukuk davasını açma hakkını haiz bulunanlardan birinin şikâyeti üzerine, her bir bent kapsamına giren fiiller dolayısıyla iki yıla kadar hapis veya adli para cezasıyla cezalandırılırlar.

II - Tüzel kişilerin cezai sorumluluğu

MADDE 63- (1) Tüzel kişilerin işlerini görmeleri sırasında bir haksız rekabet fiili işlenirse 62 nci madde hükmü, tüzel kişi adına hareket eden veya etmesi gerekmiş olan organın üyeleri veya ortakları hakkında uygulanır. Haksız rekabet fiilinin bir tüzel kişinin faaliyeti çerçevesinde işlenmesi hâlinde, tüzel kişi hakkında bunlara özgü güvenlik tedbirlerine de karar verilebilir.

IV - Sır Saklama Yükümü

MADDE 527- (1) 404 üncü madde hükmü saklı kalmak üzere, görevi dolayısıyla incelemesine sunulan defter ve belgeleri inceleyenlerin, elde ettikleri veya verilen

bilgilerden öğrendikleri iş ve işletme sırlarını açıklamaları yasaktır. Aksi hâlde şirketin maddi ve manevi zararını tazmin ederler.

(2) Ceza mevzuatının, suç ihbarına ilişkin hükümleri saklıdır.

Bir ticari işletmenin ticari sırlarının hukuka aykırı kullanılması her zaman rakip işletme tarafından gerçekleştirilmeyebilir. Ticari sırlar, bazen içeriden kişiler tarafından görev icabı öğrenilir. Bu kişilerin öğrendikleri sırların ifşası şayet haksız rekabet oluşturmuyor ise, bu maddeye dayanılarak zararın tazmini mümkün olmaz. İşte bu gibi durumlar için kanun koyucu Türk Ticaret Kanunu m.527 hükmünü vaz'etmiştir. Görevi gereğince incelemek üzere kendilerine sunulan belge ve defterleri inceleyenler, çalışmaları sonucunda öğrendikleri firmaya ait bilgileri ve sırları açıklayamazlar. Aksi taktirde şirketin bundan kaynaklanan maddi ve manevi zararlarını tazmin etmek durumundadırlar. Madde gerekçesine göre bu hükmün kapsamına şirkette yönetici, tasfiye memuru, kurucu gibi bir sorumluluğu bulunmayan, noter, aracı kurum uzmanı, avukat, bilirkişi gibi alanında yetkin kişiler girmektedir. Türk Ticaret Kanunu m.527 hükmündeki önemli bir husus, açıkça ticari sır ihlali halinde şirkette manevi zarar oluşabileceği ve ihlali yapan kişinin bu zararı tazminle yükümlü olduğunun düzenlenmesidir. Bir ticari sır ihlalinde şirketin itibarı bağlamında kişilik haklarının ihlal edilmesi olağandır (Sulu, 2020).

G) Denetçilerin sır saklamadan doğan sorumluluğu

MADDE 404- (1) (Değişik birinci cümle: 26/6/2012-6335/21 md.) Denetçi ve özel denetçi, bunların yardımcıları ile denetleme yapmasına yardımcı olan temsilcileri, denetimi dürüst ve tarafsız bir şekilde yapmak ve sır saklamakla yükümlüdür. Faaliyetleri sırasında öğrendikleri, denetleme ile ilgili olan iş ve işletme sırlarını izinsiz olarak kullanamazlar. Kasten veya ihmal ile yükümlerini ihlal edenler şirkete ve zarar verdikleri takdirde bağlı şirketlere karşı sorumludurlar. Zarar veren kişi birden fazla ise sorumluluk müteselsildir.

(3) Denetçinin bağımsız denetim yapmak üzere yetkilendirilen bir sermaye şirketi olması hâlinde sır saklama yükümü bu kurumun yönetim kurulunu ve üyelerini ve çalışanlarını da kapsar.

2.5.2.1.4 5237 Sayılı Türk Ceza Kanunu

Kanun'un 239. maddesinde ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin ifşası halinde cezai düzenlemeye yer verilmiştir. Devam eden 243-246 maddelerinde de bilişim sistemine hukuka aykırı halde girilmesi durumuna ilişkin hükümlere yer verilmiştir. Hizmet nedeni ile güvenin kötüye kullanılması halinde uygulanacak hükümler, kanunun 155. maddesinde düzenlenmiştir.

Ticari sırların cezai önlemlerle korunması ve ticari sır hırsızlığının suç sayılması gerektiği konusunda uluslararası alanda bir görüş birliği bulunmaktadır. Bu sebeple, ticari sırların yasal düzenlemeler kapsamına alındığı her ülkede cezai yaptırımlar ile korunması sağlanmaktadır. Ülkemizde de bu anlayış kabul edilmiştir. Ceza kanununda, "Ekonomi, Sanayi ve Ticarete İlişkin Suçlar" arasında ticari sırların ihlal edilmesini cezalandırmaya yönelik olarak 239. madde ihdas edilmiştir. Madde gerekçesi, "Bir bilgi veya belgenin bu nitelikte (ticari sır) olup olmadığı, ilgili kanunda belirlenen ölçütler göz önünde bulundurularak hâkim tarafından belirlenir" şeklindedir. Bir kanuni yükümlülüğü ifa ederken firmaya veya bir başkasına ait olan ticari sırların beyan edilmesi hukuka uygundur. Sır sahibinin onayının bulunduğu hallerde, ticari sırrın kullanılması veya açıklanması hukuka aykırılık sayılmayacaktır. Rızanın, tüzel kişiyi temsile yetkili kişi ya da tüzel kişilik organları tarafından açıklanması mümkündür (Sulu, 2020).

Yerel mahkeme kararlarının Yargıtay tarafından yapılan incelemesinde, davaya konu bilgilerin ticari sır kapsamında olup olmadığı, kamuya açık bilgi olup olmadığı hususunun yerel mahkeme tarafından araştırılıp araştırılmadığı değerlendirilmektedir. İnceleme sonucunda bu yönde bir eksiklik görülmesi halinde, dosyanın bu açıdan yeniden araştırılmak üzere mahkemesine gönderildiğine ilişkin çok sayıda Yargıtay kararı bulunmaktadır.

Ekonomi, Sanayi ve Ticarete İlişkin Suçlar

Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması

MADDE 239- (1) Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren

veya ifşa eden kişi, şikayet üzerine, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır. Bu bilgi veya belgelerin, hukuka aykırı yolla elde eden kişiler tarafından yetkisiz kişilere verilmesi veya ifşa edilmesi halinde de bu fıkraya göre cezaya hükmolunur.

(2) Birinci fıkra hükümleri, fenni keşif ve buluşları veya sınai uygulamaya ilişkin bilgiler hakkında da uygulanır.

(3) Bu sırlar, Türkiye'de oturmayan bir yabancıya veya onun memurlarına açıklandığı takdirde, faile verilecek ceza üçte biri oranında artırılır. Bu halde şikayet koşulu aranmaz.

(4) Cebir veya tehdit kullanarak bir kimseyi bu madde kapsamına giren bilgi veya belgeleri açıklamaya mecbur kılan kişi, üç yıldan yedi yıla kadar hapis cezasıyla cezalandırılır.

Bilişim Alanında Suçlar

Bilişim sistemine girme

MADDE 243- (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

MADDE 244- (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması

MADDE 246- (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Belirtilen suçlar, bilişim sistemine izinsiz girme, sistemi engelleme, bozma şeklindeki eylemlerle işlenmektedir. Dolayısı ile söz konusu suçlar, dijital sistemde kayıtlı tüm verilere (kişisel veri ve tüzel kişi verileri) yönelik olarak işlenebilmektedir. Alınacak teknik, idari, hukuki, eğitim önlemleri ile riskin azaltılması, hatta ortadan kaldırılması mümkün olabilecektir.

Hizmet ilişkisi gereğince vakıf olunan, kendisine teslim edilen bilgi belgelerin bu güveni sarsacak şekilde, menfaat sağlayarak, izinsiz kullanılması halinde ise hizmet nedeni ile güveni kötüye kullanma suçu oluşacaktır.

Güveni kötüye kullanma

MADDE 155- (1) Başkasına ait olup da, muhafaza etmek veya belirli bir şekilde kullanmak üzere zilyedliği kendisine devredilmiş olan mal üzerinde, kendisinin veya başkasının yararına olarak, zilyedliğin devri amacı dışında tasarrufta bulunan veya bu devir olgusunu inkar eden kişi, şikayet üzerine, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılır.

(2) Suçun, meslek ve sanat, ticaret veya hizmet ilişkisinin ya da hangi nedenden doğmuş olursa olsun, başkasının mallarını idare etmek yetkisinin gereği olarak tevdi ve teslim edilmiş eşya hakkında işlenmesi halinde, bir yıldan yedi yıla kadar hapis ve üçbin güne kadar adlî para cezasına hükmolunur.

2.5.2.1.5 6098 Sayılı Türk Borçlar Kanunu

Kanun'un 396. maddesinde, işçinin işverene karşı özen ve sadakat, iş sırlarını açıklamama borcuna ilişkin düzenlemelere yer verilmiştir.

II. Özen ve sadakat borcu

MADDE 396- ...İşçi, iş gördüğü sırada öğrendiği, özellikle üretim ve iş sırları gibi bilgileri, hizmet ilişkisinin devamı süresince kendi yararına kullanamaz veya başkalarına

açıklayamaz. İşverenin haklı menfaatinin korunması için gerekli olduğu ölçüde işçi, hizmet ilişkisinin sona ermesinden sonra da sır saklamakla yükümlüdür.

Tarafların aralarında imzaladığı ve sırların saklanmasına ilişkin gizlilik sözleşmeleri, ticari sırların korunmasında önemli hukuki dayanaklardır. Sır saklama yükümlülüğünü gizli olarak içinde bulunduran sözleşmeler bulunmaktadır. Bunlar, hizmet, vekalet, franchise, tek satıcılık ve know-how sözleşmeleridir. Bunların ortak özelliği, gizliliğe ilişkin hüküm barındırmasalar veya ayrıca bir sır saklama sözleşmesi yapılmasa dahi taraflara kendiliğinden bu yükümlülüğü getirmesidir. Bununla birlikte ayrı bir gizlilik sözleşmesi ile gizliliğin sınırlarının belirlenmesi de yararlı olacaktır. Taraflar arasındaki ilişkinin sona ermesi ya da gizli bilgi sahibinin isteği ile gizli bilgileri içeren belgelerin sahibine geri verilmesini sağlamak üzere, gizlilik sözleşmesi düzenlenerek imzalanması gereklidir (Sulu, 2020).

Lojistik şirketler açısından değerlendirildiğinde, ticari, hizmet ya da vekalet sözleşmesi gereği, bilgi ve belge paylaşılan kişi ve firmalar ile detaylı sır saklama sözleşmesi akdedilmesi faydalı olacaktır. Sözleşme de gizlilik sınırları net olarak belirlenmelidir. Gizli bilgi tanımlanmalı ve gizli bilgi, ticari sır olarak adlandırılmayan hususlar açık ve net olarak belirlenmelidir. Gizli bilgilerin kopyalanmaması, görevli olmayan kişilerin gizlilik özelliği taşıyan verinin bulunduğu ortama girişine izin verilmemesi, bu bölgelerin güvenlik kameraları ile izlenmesi, gizli bilginin güvenli kasalarda saklanması gibi hususlara gizlilik sözleşmelerinde yer verilebilir.

Gizlilik sözleşmelerinin bir başka şekli Borçlar Kanunu 444 madde de düzenlenen rekabet yasağı sözleşmesidir. Bu düzenlemeye uygun olarak sözleşme ile işçi, işverenine karşı, aralarındaki iş ilişkisi sona erdiğinde işverenin iştigal alanında çalışmamayı, ona rakip olacak bir firma açmamayı, diğer başka bir rakip firmada çalışmamayı, ya da rakip işletmeyle herhangi bir çıkar ilişkisine girmemeyi yazılı şekilde taahhüt etmektedir. Bu yasak, maddenin 444/2 bendi uyarınca, hizmet ilişkisi işçiye müşteri çevresi veya üretim sırları ya da işverenin yaptığı işler hakkında bilgi edinme imkânı sağlıyor ve ayrıca bu bilgilerin kullanılması, işverenin önemli bir zararına sebep olacak şekilde ise geçerli olacaktır (Sulu, 2020).

VII. Rekabet yasağı

MADDE 444- Fiil ehliyetine sahip olan işçi, işverene karşı, sözleşmenin sona ermesinden sonra herhangi bir biçimde onunla rekabet etmekten, özellikle kendi hesabına rakip bir işletme açmaktan, başka bir rakip işletmede çalışmaktan veya bunların dışında, rakip işletmeyle başka türden bir menfaat ilişkisine girişmekten kaçınmayı yazılı olarak üstlenebilir.

Rekabet yasağı kaydı, ancak hizmet ilişkisi işçiye müşteri çevresi veya üretim sırları ya da işverenin yaptığı işler hakkında bilgi edinme imkânı sağlıyorsa ve aynı zamanda bu bilgilerin kullanılması, işverenin önemli bir zararına sebep olacak nitelikteyse geçerlidir.

Sır saklama sözleşmesi ile rekabet yasağı sözleşmesi arasında fark vardır. Buna göre, sır saklama sözleşmesinin rekabeti önleyici bir yönü bulunmamaktadır. Rekabet yasağı sözleşmesinde belirli bir yer ve zamanla sınırlandırılmış olsa da işçinin aynı iş alanında çalışmasına yasak getirildiğinden mesleki ilerleyişi bundan etkilenmektedir. Bu sözleşmenin içeriğinin geniş olmaması önemlidir (Sulu, 2020).

Firmalar tarafından öncelikli olarak yapılması gereken, şirket veri envanterini çıkararak, verileri derecelendirmek ve sınıflandırmaktır. Böylelikle şirketin, hangi türde verileri kayıt altına aldığı, önem ve korunma dereceleri belirlenebilecektir.

Ticari sırlar, iş birliği veya franchise sözleşmesi gibi oldukça fazla ticari sırrın ifşa edildiği sözleşmeler kapsamında açıklanabildiği gibi, tedarik sözleşmeleri kapsamında da ifşa edilebilir. Bundan dolayı, ticari sözleşmeler için de gizlilik yükümlülüklerinin geniş kapsamlı tutulması, sırların korunması bakımından oldukça önemlidir. Bunun için, öncelikli olarak sözleşme içinde, ticari sır tanımı geniş kapsamlı yapılmalıdır. Ayrıca, gizlilik yükümlülüğünün tarafların çalışanları, temsilcileri ve danışmanları bakımından da geçerli olacağı ve sırrın aktarıldığı çalışan, temsilci veya danışmandan gizlilik taahhütnamesi alınacağı şeklinde düzenlemeler sözleşme içeriğine eklenebilir (Baylan, 2020).

2.5.2.1.6 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Tüzel kişiliğe ilişkin veriler, Kişisel Verilerin Korunması Kanunu kapsamında koruma altına alınmamıştır. Kurulun 19/11/2018 tarihli ve 2018/131 sayılı Karar Özetinde kısaca:

"Bir tüzel kişiliğe ait elektronik ortamda yer alan verilerin veri sorumlusu tarafından başka bir veri sorumlusuna aktarılması talebi ile ilgili tüzel kişi şirket tarafından Kişisel Verileri Koruma Kurumuna yapılan başvuru hakkında;

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 2 nci maddesinde "Kanun hükümlerinin, kişisel verileri işlenen gerçek kişiler hakkında uygulanacağı" belirtilmiş, "Tanımlar" başlıklı 3 üncü maddesinin (d) bendinde de "Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Bu sebeple, gerçek kişilere ait veriler Kanun kapsamında bulunurken, tüzel kişilere ait veriler ise Kanun kapsamında bulunmamaktadır" şeklinde açıklama ile talep red edilmiştir (Kişisel Verileri Koruma Kurulu Kararı, 2018).

Tüzel kişiler, yetkili organları aracılığı ile kararlar almakta ve temsil edilmektedir. Tüzel kişilik organları gerçek kişilerden oluşur. Bu kişilere ilişkin veriler, doğrudan belirli veya belirlenebilir bir tüzel kişi organ üyesi (gerçek kişi ile) ile ilişkilendirilebildiği müddetçe, mevzuat gereğince kişisel veri olarak kabul edilerek Kişisel Verilerin Korunması Kanunu gereğince korunacaktır.

2.5.2.1.7 Diğer ulusal düzenlemeler

6769 Sayılı Sınai Mülkiyet Kanunu

Amaç ve kapsam

MADDE 1- (2) Bu Kanun; marka, coğrafi işaret, tasarım, patent, faydalı model ile geleneksel ürün adlarına ilişkin başvuruları, tescil ve tescil sonrası işlemleri ve bu hakların ihlaline dair hukuki ve cezai yaptırımları kapsar.

Patentin konusu buluştur (Gürel, t.y.). Patent başvurusu yapıldığı andan patentin onaylanacağı veya reddedileceği tarihe kadar, buluşun ticari sır olarak değerlendirildiği

kabul edilmektedir. Fikrî ve Sınaî Haklar alanındaki ticari sırlara ilişkin diğer konu, endüstriyel tasarımlardır (Sulu, 2020).

Patent hakkına tecavüz niteliğinde olan fiillerin doğurabileceği cezai sorumluluk için ise 6102 sayılı Türk Ticaret Kanunu m.62 uyarınca Haksız Rekabetten kaynaklanan cezai sorumluluktan bahsedilebilir (Koç, 2022).

Haksız Rekabet

I - Cezayı gerektiren fiiller

MADDE 62- (1) a) 55 inci maddede yazılı haksız rekabet fiillerinden birini kasten işleyenler,

b) Kendi icap ve tekliflerinin rakiplerininkine tercih edilmesi için kişisel durumu, ürünleri, iş ürünleri, ticari faaliyeti ve işleri hakkında kasten yanlış veya yanıltıcı bilgi verenler,

c) Çalışanları, vekilleri veya diğer yardımcı kimseleri, çalıştıranın veya müvekkillerinin üretim veya ticaret sırlarını ele geçirmelerini sağlamak için aldatanlar,

d) Çalıştıranlar veya müvekkillerden, işçilerinin veya çalışanlarının ya da vekillerinin, işlerini gördükleri sırada cezayı gerektiren bir haksız rekabet fiilini işlediklerini öğrenip de bu fiili önlemeyenler veya gerçeğe aykırı beyanları düzeltmeyenler,

fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, 56 ncı madde gereğince hukuk davasını açma hakkını haiz bulunanlardan birinin şikâyeti üzerine, her bir bent kapsamına giren fiiller dolayısıyla iki yıla kadar hapis veya adli para cezasıyla cezalandırılırlar.

Haksız rekabet fiili, bir tüzel kişinin faaliyetleri sırasında işlenirse, yukarıda anılan cezalar tüzel kişi adına hareket eden veya etmesi gerekmiş olan organın üyeleri veya ortakları hakkında uygulanır. Yani, tüzel kişinin ticari temsilcisi, yönetim kurulu üyeleri ve ortaklarının sorumluluğu gündeme gelmektedir. Ayrıca, tüzel kişiye has emniyet tedbirlerine de karar verilebilecektir. Türkiye sınırlarında patent koruması bulunan bir ürünün, patent hakkı sahibinin izni olmaksızın kullanılması, üretilmesi, ithal edilmesi,

satılması gibi faaliyetler hem patent hakkına tecavüz hem de haksız rekabet teşkil edebilecek, patent hakkına tecavüz eden kimselerin hukuki ve cezai bakımdan sorumlu tutulmalarına sebep olabilecektir (Koç, 2022).

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Gerçek ve Tüzel kişilerin kişilik hakkı ihlalleri, dijital ortamda gerçekleşebilmektedir. Bu mağduriyetlerin önlenmesi için 5651 sayılı kanun yayımlanmıştır.

İçeriğin yayından çıkarılması ve erişimin engellenmesi

MADDE 9- (1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğin çıkarılmasını ve/veya erişimin engellenmesini de isteyebilir.

4054 sayılı Rekabetin Korunması Hakkında Kanun

Yasaklar

MADDE 25 – ... Kurul üyeleri ve personeli Kurumla ilgili gizlilik taşıyan bilgileri ve bu Kanunun uygulanması sırasında öğrendikleri teşebbüs ve teşebbüs birliklerinin ticari sırlarını görevlerinden ayrılmış olsalar bile ifşa edemezler, kendilerinin veya başkalarının menfaatine kullanamazlar.

5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK)

Tanımlar

MADDE 1/B – Bu Kanunda geçen tanımlardan;

a) Eser: Sahibinin hususiyetini taşıyan ve ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri olarak sayılan her nevi fikir ve sanat mahsullerini,

b) Eser sahibi: Eseri meydana getiren kişiyi,.....ifade eder.

Buna göre, Tüzel kişilerin faaliyetleri çerçevesinde eser sahibi olmaları söz konusudur.

Bunların yanında, Sermaye Piyasası Kanunu, Ticari Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısı, Bilgi Edinme Hakkı Kanunu, Elektronik Haberleşme Kanunu ve Arabuluculuk Mevzuatında Ticari Sırların Korunmasına yönelik olarak, edinilen bilgilerin ifşa edilmemesi, saklanmasına ilişkin hükümlere yer verilmiştir.

2.5.2.2 Uluslararası düzenlemelerde ticari sırların korunması

Ticari sırlar ülkemizde yasal düzenlemeler ile korunmaktadır. Diğer bazı ülkelerin ticari sırlarla ilgili yasal düzenlemeleri ise şu şekildedir. İngiliz Hukukunda ticari sırların korunmasına ilişkin kanunî bir düzenleme bulunmamaktadır. Koruma, içtihat hukuku uyarınca sağlanmaktadır. 200 yıl boyunca İngiliz mahkemelerinin vermiş olduğu yüzlerce karar ile ticari sırların korunması sağlanmıştır. Hakimler, her somut olayı ayrı ayrı değerlendirerek ticari sır ihlallerini farklı hukuki temellere dayandırmaktadır. Bu hukuki temeller; sözleşme, hakkaniyet, haksız fiil, mülkiyet ve sadakat yükümlülüğüdür.

Amerikan Hukukunda, İngiliz Hukukundan farklı olarak ticari sır kavramı yasal düzenlemeler altına alınmıştır. Amerika Birleşik Devletleri, fikri mülkiyet haklarını çok önemsemiştir. 1790 yılında Patent Kanunu'nu kabul etmiştir. Fikri mülkiyet hakları, ifade özgürlüğünden daha önce düzenlenmiştir. Başlıca hukuki düzenlemeler; Ticari Sırları Koruma Kanunu, Yeknesak Ticari Sırlar Kanunu, Birinci Haksız Fiil Düzenlemesi, Ekonomik Casusluk Kanunu ve Üçüncü Haksız Rekabet Düzenlemesi'dir. En önemli yasa, Yeknesak Ticari Sırlar Kanunudur. Birinci Haksız Fiil Düzenlemesi'nin de Amerikan hukukundaki önemi büyüktür. Ekonomik Casusluk Kanunu bir başka önemli hukuki düzenlemedir. Bu kanun, Ticari sırların cezaî olarak korunmasını amaçlamaktadır. Tüm bu yasal düzenlemelerin ticari sırların korunmasına ilişkin yeterli bulunmaması sebebiyle 2016 tarihinde Ticari Sırları Koruma Kanunu çıkarılmıştır. Yargı kararları da Amerikan Ticari Sırlar Hukukunun biçimlenmesinde önemli yer tutmaktadır (Sulu, 2020).

Sınaî hakların milletlerarası düzeyde korunması ihtiyacı sonucunda, 20 Mart 1883'de Paris'te "Sınai Mülkiyetin Himayesine Mahsus Milletlerarası Bir İttihad İhdas Edilmesine Dair Paris Sözleşmesi" imzalanmıştır. Bu sözleşmede birtakım sınaî haklara yer verilmiştir, ticari sır tanımı yer almamaktadır. Dünya Ticaret Örgütü nezdinde

gerçekleştirilen müzakerelerin sonunda Ticaretle Bağlantılı Fikri Mülkiyet Anlaşması (TRIPS) kabul edilmiştir ve ticari sırların korunması konusunda milletlerarası boyutta bir çalışma yapılmıştır. Bu anlaşma, Dünya Ticaret Örgütü üyelerinin ulusal mevzuatlarını hazırlarken dikkate almak zorunda oldukları bir kılavuz niteliğindedir (Sulu, 2020).

Türkiye, Dünya Ticaret Örgütü'nün kurucu üyelerindendir. Bu anlaşmaya Dünya Ticaret Örgütü kurulur iken taraf olmuş ve 2000 yılında anlaşmanın maddelerini uygulamaya geçmiştir (T.C. Kültür ve Turizm Bakanlığı, t.y.).

Ticaretle Bağlantılı Fikri Mülkiyet Hakları Anlaşması (TRIPS)

Açıklanmamış Bilgilerin Korunması

MADDE 39- (2) Gerçek ve tüzel kişiler yasal olarak kendi kontrolleri altındaki bilgilerin kendi izinleri olmadan, dürüst ticari uygulamalara aykırı, başkalarına ifşa edilmesini veya başkaları tarafından elde edilmesini veya kullanılmasını engelleme olanağına sahip olacaklardır, ancak şu koşulla ki, bu tür bilgiler;

a) Bir bütün olarak veya unsurlarının kesin konfigürasyonunda veya grubunda, normal olarak söz konusu türde bilgilerle uğraşan çevrelerdeki şahıslarca genelde bilinmeyen veya bu şahısların kolaylıkla elde edemeyeceği anlamında gizli olmalıdır;

(b) Gizli olduğu için ticari değeri olmalıdır ve

(c) Yasal olarak bu bilgileri kontrol eden şahıs tarafından, gizli kalması için, ilgili koşullar altında makul önlemler alınmış olmalıdır (T.C. Kültür ve Turizm Bakanlığı, t.y.) (Suluk, t.y.)

Avrupa Birliği Hukuki Düzenlemeleri

Avrupa Birliği, Birlik Hukuku literatüründe ticari sırlar, açıklanmamış ve gizli iş bilgisi veya gizli know-how gibi farklı adlandırmalar ile kullanılmaktadır. Avrupa Birliği Konseyi TRIPS'in tarafıdır ve Dünya Ticaret Örgütü'nün üyesidir. Bu sebeple, örgütsel olarak Avrupa Birliği ve de birlik üyesi devletler TRIPS ile bağlıdır. Ticaretle Bağlantılı Fikri Mülkiyet Hakları Anlaşması ile ilgili konular Birlik Hukuku bakımından da geçerlidir. Üye ülkelerin iç hukuklarında ticari sırra ilişkin çeşitli düzenlemeler

bulunmaktadır ancak bu konuda birlik düzeyinde bir düzenleme yapılmadığından ihtiyaç oluşmuştur. Avrupa Komisyonu "Açıklanmamış Know-how ve İş Bilgilerinin (Ticari Sırların) Korunması ve Yasadışı Edinimlerinin, Kullanılmalarının ve İfşalarının Önlenmesi Hakkındaki Direktif" i kabul ile Avrupa Parlamentosu'na göndermiştir (Sulu, 2020).

Sözkonusu Direktif (AB) 2016/943, Avrupa Parlamentosu ve Avrupa Konseyi'nin bir direktifidir. Direktifin amacı, Avrupa Birliği içinde, ticari sırların kötüye kullanılmasına karşı korumaya ilişkin mevcut farklı ulusal yasaları uyumlu hale getirmek, böylece şirketlerin ticari sırlarını iç pazarda ayrıcalıklı iş ortaklarıyla paylaşabilmesini sağlamaktır (Vikipedi, t.y.).

2.5.3 Uluslararası sözleşmeler ve özel tedbirler

Bilişim suçları ile ilgili mücadelede zorluklar oluştuğundan bunların ortadan kaldırılması için çalışmalar yapılmıştır. Bu itibarla, öncelikle ülkelerin konuya aynı duyarlılıkla yaklaşması ve yasal düzenlemeler bakımından ülkeler arasında uyumluluğun sağlanması gerekmiştir. Böylece bilişim suçlularının, mevzuat farklılıklarını kendilerine bir sığınma limanı olarak görmeleri önlenerek yasalara karşı gelmelerinin önüne geçilmiştir. Uluslararası alanda adli iş birliğinin geliştirilmesi için girişimler başlatılmıştır. Yapılan en büyük girişim ülkemizin de taraf olduğu Avrupa Siber Suçlar Sözleşmesi'dir. Sözleşme ülkemizde 29.09.2014 tarihinde yürürlüğe girmiştir. Sözleşmenin onaylı çevirisi "Sanal Ortamda İşlenen Suçlar Sözleşmesi" şeklinde yapılmıştır (Aliusta ve Benzer, 2018).

Yasal düzenlemelerin yanında, bilgi güvenliğini korumak amacıyla devletler tarafından alınan özel önlemler ve kurulan yapılar da bulunmaktadır. Bu doğrultuda, siber saldırıların engellenmesi, olay sırasında hızlı müdahale edilebilmesi için Ulaştırma Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur. Merkez, yerelde ve milletlerarası düzeyde iletilen siber tehditleri değerlendirerek bu tehditlerin ortadan kaldırılması için kamu kuruluşları ve özel kişiler ile koordinasyonu oluşturmaktadır. İhbarlar geldiği andan çözüme kavuşturuluncaya kadar takip edilerek durum değerlendirilmektedir. Ayrıca kamuya ait kuruluşlar kapsamında ve kritik altyapı

sektörleri için Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME)'ler oluşturulmuştur (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2014, s. 6) (USOM, t.y.). Kritik altyapı sektörleri, elektronik haberleşme, ulaştırma, enerji, kritik kamu hizmetleri, finans ve su yönetimi olarak belirlenmiştir. Ulaştırma, lojistik hizmetler içerisinde oldukça önemli bir yere sahiptir. Ulaştırma alanında yaşanacak siber saldırılar siber olaylara müdahale ekiplerine bildirilecektir.

2.5.4 Avrupa Birliği Siber Güvenlik Kanunu

Kanun, 11 Mart 2019 tarihinde Avrupa Birliği Parlamentosu'nda onaylanmış, 7 Haziran 2019'da- Avrupa Birliği Resmi Gazetesi'nde yayımlanmıştır. Yasa, 27 Haziran 2019 tarihi itibariyle yürürlüğe girmiştir. Bu tarih itibariyle, mevcut Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) yeni yetki ve görevleriyle daimi bir AB Siber Güvenlik Ajansı haline gelmiştir. Söz konusu düzenlemeye göre, haberleşme ve bilişim teknolojileri hizmet, ürün ve işlemleri için siber güvenlik sertifikası hazırlanacak ve bunlar Avrupa Birliği üyesi ülkelerinde geçerli olacaktır. Kanun, siber saldırılarla başa çıkmak ve Avrupa Birliği'nde güçlü bir siber güvenlik sağlamak amacıyla çıkarılmıştır (Deloitte, t.y.) (Zümbül Hukuk, 2019).

2.6 Bilgi Güvenliği

2.6.1 Bilgi güvenliği ve standardları

Bir açıklamaya göre bilgi güvenliği, iletişim ağında, yedekleme cihazlarında, disklerde veya başka herhangi bir yerde depolanan verilerin ve her türlü bilginin korunmasını ifade eder. Bilgiler, kağıt üzerinde (fiziki olarak) ya da dijital ortamda (bilgisayar gibi) saklanabilir, elektronik posta veya normal posta ile iletilebilir (Yılmaz, 2014).

Bilgi güvenliğini oluşturan 3 temel prensip vardır.

- Gizlilik, bilgiye sadece yetkisi olan kişiler tarafından erişilmesi,
- Bütünlük, verinin yetkisi olmayan kişiler tarafından bozulamaması, tam olması,
- Erişilebilirlik ise, bilginin sürekli kullanıma elverişli halde olması yetkisi olanlar tarafından istenildiğinde ulaşılabilir olmasıdır. Bu üç ilke, sistem güvenliği için

standart olarak hizmet eden güvenlik üçgeni olarak adlandırılır. Bunlardan bir tanesinin zarar görmesi halinde güvenlik açığı, risk oluşacaktır (Çek, 2017).

Gizlilik kavramı, kişisel verilerin korunmasıyla sıkça ilişkilendirilir ve mahremiyetle yakından bağlantılıdır. Gizlilik hassas ve kişisel veriler bakımından çok önemlidir. Verileri kayıt edilen kişiler, verileri kayıt eden kuruluşlardan gizliliğin korunmasını talep hakkına sahiptir (Henkoğlu, 2015).

Aynı durum tüzel kişilerin kayıt altına aldığı diğer veriler içinde geçerlidir. Ticari sırlar, müşteri sırları gibi veriler büyük bir hassasiyet ile korunması gereken bilgilerdir. Bilgi güvenliği temel prensibi olan gizlilik, verileri işlenen kişi ve kurumlar için önemlidir, verileri işlenen kişiler, veri sorumlularına güven duymak isterler. Ülkemizde, bilgiye yönelik risk ve tehditlere karşı kişisel verilerin korunması kanununda yer verilen güvenlik önlemlerine benzer bir düzenleme, bilgi güvenliğine ilişkin diğer yasal düzenlemelerde bulunmamaktadır.

Bilgi güvenliği, farklı disiplinleri içeren kapsamlı bir konudur ve bu yönüyle geniş çapta ele alınması gereken bir alandır. Bilgi güvenliğini sağlama konusunda alınacak teknik önlemler ve bu yöndeki politikalar, riski azaltıp zararı önlemeye ve tehditleri ortadan kaldırmaya yönelik iken, hukuki düzenlemeleri kapsayan politikalar, farkındalık oluşturmaya, hak ve sorumlulukları öğretip caydırıcılık sağlamaya, zararı engellemeye ya da azaltmaya yönelik yapılmaktadır (Henkoğlu ve Yılmaz , 2013).

ISO 27001 BGYS, risk yönetimi prosesi uygulayarak verilerin gizliliğini, tamlığını ve erişilebilirliğini sağlar ve ilgililere risklerin uygun bir şekilde yönetildiği konusunda güven verir (ISO/IEC, 2022). Bu sistem, şirketlerin önemli bilgilerinin sistematik bir şekilde yönetilebilmesi için gerekli bir dizi politika ve prosedürlerden oluşur. Sistemin nihai amacı, güvenlik ihlallerinin etkilerini proaktif bir şekilde sınırlandırarak riskin azaltılması ve iş sürekliliğinin sağlanmasıdır (Big Danışmanlık, 2023).

Bunun için, kurulacak sistemin, kuruluş proseslerinin ve yönetim şeklinin bir parçası olması, bunlara entegre olması, şirket proses, bilgi sistem ve kontrollerinin planlanmasında bilgi güvenliğinin göz önünde bulundurulması gerekir. Bilgi güvenliği

yönetim sistemi uygulamasının kuruluşun ihtiyaçlarına göre ölçeklendirilmesi beklenmektedir (ISO/IEC, 2022).

Bir firmada bilgi güvenliği yönetim sisteminin kurulabilmesi için, öncelikle üst yönetimin veri güvenliğinin şirket için önemini anlaması ve hukuki yükümlülüklerinin farkında olması gerekmektedir. Şirket üst yönetiminin karar ve desteği olmadan bilgi güvenliğinin sağlanması güçtür.

ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi ana maddelerinde üst yönetim tarafından yapılması gerekenler düzenlenmiştir.

"ISO 27001:2022 Ana Maddeleri

5. Liderlik

5.1 Liderlik ve bağlılık

Üst yönetim, aşağıdakileri yaparak bilgi güvenliği yönetim sistemi ile ilgili olarak liderlik ve bağlılık göstermelidir:

a) Bilgi güvenliği politikasının ve bilgi güvenliği hedeflerinin oluşturulmasını ve kuruluşun stratejik yönü ile uyumlu olmasının sağlaması,

b) Bilgi güvenliği yönetim sistemi gerekliliklerinin kuruluşun süreçlerine entegrasyonunun sağlanması,

c) Bilgi güvenliği yönetim sistemi için ihtiyaç duyulan kaynakların mevcut olmasının sağlanması,

d) Etkili bilgi güvenliği yönetiminin ve bilgi güvenliği yönetim sistemi gerekliliklerine uygunluğun öneminin duyurulması,

e) Bilgi güvenliği yönetim sisteminin amaçlanan sonuca/çıktılara ulaşmasının sağlanması,

f) Bilgi güvenliği yönetim sisteminin etkinliğine katkıda bulunmaları için kişilerin yönlendirilmesi ve desteklenmesi,

g) Sürekli iyileştirmenin teşvik edilmesi ve

h) Sorumluluk alanları için geçerli olduğu şekliyle liderliklerini göstermek için diğer ilgili yönetim rollerinin desteklenmesi.

5.2 Politika

Üst yönetim, aşağıdaki hususları sağlayan bir bilgi güvenliği politikası oluşturmalıdır.

5.3 Kurumsal roller, sorumluluklar ve yetkiler

Üst yönetim, bilgi güvenliği ile ilgili roller için sorumlulukların ve yetkilerin atanmasını (belirlenmesini) ve kuruluş içinde duyurulmasını sağlamalıdır. Üst yönetim, aşağıdaki hususlar için sorumluluk ve yetki ataması yapmalıdır.

9.3 Yönetimin gözden geçirmesi

9.3.1 Genel

Üst yönetim, sürekli uygunluğunu, yeterliliğini ve etkinliğini sağlamak için kuruluşun bilgi güvenliği yönetim sistemini planlanan aralıklarla gözden geçirmelidir" (ISO/IEC, 2022).

ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi standard düzenlemesine göre, bilgi güvenliği yönetim sisteminin sağlanmasında şirket üst yönetiminin aktif karar ve eylemlerine ihtiyaç bulunmaktadır. Akademik çalışmalar da bu durumu destekler niteliktedir.

Üst yönetimin (karar vericilerin) bilgi güvenliği konusunda bilgilerinin arttırılması gerekliliği, doğru şekilde eğitim verilmesi gerekliliği konusuna vurgu yapılmıştır (Jalali, Siegel ve Madnick, 2019).

Siber saldırıların siber güvenlik sistemlerine yatırımı nasıl yönlendirdiği araştırılmıştır. Siber güvenlik yatırımı kuruluşlarda stratejik bir karardır. Çalışma şirket ölçülerinin siber güvenlik yatırımında önemli bir değişken olduğunu gösteren önceki çalışmaları desteklemektedir (Arroyabe, Arranz, Arroyabe ve Arroyabe, 2023).

Ernst&Young'ın (EY) yeni tarihli Küresel Siber Güvenlik Liderliği İçgörüleri araştırmasına göre;

> En etkili siber güvenliğe sahip şirketler, daha düşük performans gösterenlere göre daha az siber vakayla karşılaşıyor. Vakaları tespit etme ve yanıt verme konusunda da daha hızlı aksiyon alıyorlar….Araştırmada öne çıkan bir diğer risk

faktörü; tedarik zincirleri. Artık tüm kuruluşlar, tedarik zincirlerindeki işletmelere ayrılmaz bir şekilde ve dijital olarak bağlı. Son beş yılda tehdit aktörlerinin en zayıf halka olarak gördükleri tedarik zincirlerini hedef aldığı görünüyor. Bu sebeple bilgi güvenliği liderleri'nin, yalnızca bir defaya mahsus değil düzenli olarak kuruluşlarının tedarik zincirlerini kontrol altında tutması gerekiyor (Ernst ve Young, 2024).

2.6.1.1 ISO/IEC 27001 Bilgi güvenliği standardı ve tarihçesi

Bilgi Güvenliği Yönetim Sistemi (BGYS); Bilginin mahremiyetini, tamlığını ve ulaşılabilirliğini korumak üzere, planlanmış, kuralları belirlenmiş, devamlı geliştirilebilen, idareciler tarafından desteklenerek onaylanmış, uluslararası güvenlik standartlarının esas olarak alındığı bir işlemler bütünüdür (Çek, 2017).

Dijital ortamlara ulaşmak üzere yapılan saldırılar internet kullanılarak yapılmaktadır. Bu saldırılar gittikçe arttığından hatta küresel boyutlara ulaştığından dolayı ülkeler, uygulanacak güvenlik önlemlerinin yeknesak ve etkili olması düşüncesinden hareket ile milletlerarası boyutta çalışma yapılarak ortak standart geliştirilmesinin zorunluluk olduğuna karar vermişlerdir. 1990 yıllarda bilgi güvenliğini sağlamaya yönelik standartların oluşturulması çalışmaları başlamıştır.

- İngiltere tarafından 1995'de geliştirilmiş olan BS7799 standardı, ilk bilgi güvenliği standartlarındandır. Bilgi güvenliği politikalarında bulunması gereken unsurlara dair bilgileri içerir.

- BS7799 standardının birinci bölümü (BS7799-1), 2000 yılında, ISO ve IEC tarafından uyarlanarak ISO/IEC 17799 adını almış ve uluslararası standarda dönüştürülmüştür.

- 2005 yılında, ISO/IEC 17799 standardı yeni düzenlemelerle ISO 27001:2005 adını almıştır.

- 2007 senesinde standart, yeniden revize edilerek ISO bilgi güvenliği standardlarını içeren 27000 serisi içinde ISO/IEC 27002 ismini almıştır.

- Standart 2013 senesinde tekrar güncellenmiştir. Bu kez ISO/IEC 27001:2013 ismini alan standard her ölçekten firma ve kamu kuruluşları için uygulanabilir bir standarttır. Bu alanda en çok bilinen uluslararası bilgi güvenliği standardıdır (Henkoğlu, 2015).

- ISO 27001:2013 Standardının genel esas maddeleri ve kontrol maddeleri (Ek-A) bulunmaktadır. Ek-A'da belirtilen bilgi güvenliği kontrollerine ilişkin bölüm ISO 27002 olarak düzenlenmiştir. Ek-A, bilgi güvenliği kontrollerine ilişkin detaylı kılavuzluk sağlayan ve yönetimine rehberlik eden bir referans standardtır. Bu standard 15.02.2022 tarihinde değişikliğe uğrayarak ISO/IEC 27002:2022 ismini almıştır. Bu gelişmenin ardından, Uluslararası Standardlar Kuruluşu (ISO) tarafından 27001:2013 versiyonunda bazı değişiklikler yapılmış ve ISO 27001:2022 olarak 25 Ekim 2022 tarihinde yayınlanmıştır. Kurum ve firmalara yeni düzenlemeye geçiş için 3 yıllık süre tanınmıştır. Verilen sürenin son tarihi 31.10.2025'dir.

Ayrıca, ISO/IEC 27701:2019 Kişisel Veri Yönetim Sistemi (KVYS) standardı, ISO/IEC tarafından, dijital alanda bilgi güvenliğinin sağlanması, korunması ve gizliliğin düzenlenmesi ve yönetilmesi için geliştirilmiştir. Bu standart, ISO/IEC 27001'in bir gizlilik bileşenidir. İşletmelerin kişisel verilerin korunması yasası ve diğer bilgi koruma mevzuatlarına uygun hareket etmelerine de destek olmaktadır (AND Akademi, t.y.) (Kalitest, t.y.) (A1 Certification ve Inspection, t.y.).

- ISO (Uluslararası Standardlar Örgütü) bütün teknik ve teknik dışı konularda uluslararası standardlar geliştiren ve yayınlayan dünyanın en büyük kuruluşudur. Teşkilatın merkezi Cenevre, İsviçre'de olup 1947 yılında kurulmuştur. Şu anda 163 üye ülkeye sahip kuruluşa; Türkiye, Türk Standardları Enstitüsü (TSE) ile üye ülkeler arasındadır (Can, 2012).

ISO 27001 standardı, ülkemizde Türk Standartları Enstitüsü, TS ISO/IEC 27001:2005 olarak bir Türk standartı olarak tasdiklenmiştir. 2013'de ISO/IEC 27001'in yeni sürümü yayınlanmış ve bu standard TS ISO/IEC 27001:2013 olarak onaylanmıştır (Çek, 2017). Yapılan son değişiklik ile, TS ISO/IEC 27001:2022 "Bilgi Güvenliği, Siber Güvenlik Ve Gizlilik Koruması- Bilgi Güvenliği Yönetim Sistemleri- Gereksinimler" başlığı ile Aralık 2022'de yayınlanmıştır.

ISO/IEC 27001, işletmelerinde bilgi güvenliği yönetim sistemi kurmak isteyenlerin risk seviyelerini belirleyerek analizlerini yaptıktan sonra, güvenlik tedbirlerinin alınmasını ve risklerin kabul edilir bir seviyeye indirilmesine yardımcı olmaktadır (Henkoğlu, 2015). Bu standard, küçük, orta ve büyük ölçekteki işletmelerin fiziki ve dijital ortamda kayıt edilen, ticari sır, müşteri bilgileri, tüzel kişiliğe ait bilgiler ile kişisel veri niteliğindeki tüm verilerini koruma altına alarak risk seviyesini azaltmaktadır.

Literatür kaynaklarda, ISO 27001 BGYS'nin önem ve faydalarından söz edilmektedir. *"ISO 27001:2013 standardı, bilgilerin korunmasını sağlayan bir dizi strateji ve kontrol oluşturmak için en iyi uygulamalar ile güvenlik yönergelerinin uygulandığı en uygun modellerinden biridir ve çalışmada bilgi güvenliği yönetim sisteminin uygulanması önerilmektedir"* (Velasco, Ullauri, Pilicita, Jacome, Saa ve Moscoso-Zea, 2018)**.**

"Bir şirket her şeyden önce bilgi güvenliğini en iyi şekilde sağlayarak kendisini geliştirir. Herhangi bir kuruluşun güvenliği gizlilik, bütünlük ve erişilebilirlik ilkeleriyle başlar. Bunlar, sistem güvenliği için standart olarak hizmet eden güvenlik üçgeni olarak adlandırılır" (Li ve Liu, 2021). Bu güvenlik üçgeni, uluslararası güvenlik standardının da temelini oluşturmaktadır.

ISO 27001 BGYS standardını uygulamanın işletmelere çok sayıda katkısı bulunmaktadır; 1-Şirketler, bilgi varlıklarının farkına varıp korunmasını sağlar, 2-Bilgi varlıklarının korunması ile firmanın faaliyet, finansal kazanç, zaman ve saygınlığına yönelik kayıpları önlenir, 3-Tehdit ve riskler yönetilmek suretiyle iş sürekliliği sağlanır, 4-Yasa ve yönetmeliklere uyum ile yasal takipler önlenir, 5-Kuralların bilinip uygulanması sağlanarak şirket nezdinde bilgi güvenliği disiplini oluşturulur, 6-Şirketin ve de birlikte çalışılan iş ortaklarının riskleri azaltılarak, şirket nezdinde farkındalık sağlanır, 7-Kontrol ve güncellemeler ile güvenlik her daim güncellenebilir, 8-Değişen risklere karşı önceden önlem alınması kolaylaşır, 9-Piyasada güven oluşturarak rekabet avantajı sağlar, 10-İş, finans ve itibar kaybını minimize eder (Yılmaz , 2014).

Şirket nezdinde kurulacak bilgi güvenliği yönetim sisteminin, şirket iş süreçleri ve yönetim yapısı ile entegre olması önemlidir. Bilgi sistemleri ile kontrollerin tasarımında ve süreçlerde bilgi güvenliğinin dikkate alınması gerekir. Kurulacak sistem firmanın ihtiyaçlarına göre yapılandırılacaktır. Böylece, bilgi varlıkları koruma altına alınarak veri

ihlali kaynaklı riskler azaltılabileceğinden, firmanın zarara uğraması engellenebilecektir. Lojistik sektöründe bilginin kesintisiz olarak sürekli akışı, iş süreçlerinin devamı için önemlidir. Tedarik zinciri içerisinde fazla sayıda lojistik faaliyet gerçekleştiğinden, çok sayıda aktör, bilgi akışı ve hareket söz konusudur. Firma büyüklüğü farketmeksizin lojistik hizmet sunan firmaların ISO 27001 Bilgi Güvenliği Yönetim Sistemi'ni uygulaması önemlidir. Kurulacak bilgi güvenliği sistemi, sadece uygulayıcı şirkete değil, o şirkete güvenerek veri paylaşımında bulunan tüm kurum ve bireylere fayda sağlayacaktır.

> "Bilgi güvenliği, tedarik zincirlerindeki kuruluşlar için rekabetçi bir duruşun sürdürülmesinde hayati bir rol oynamaktadır. Güvenli bir bilgi sisteminin faydaları sadece iş sürekliliğini sağlamak, felaket yönetimi, iş risklerini en aza indirmek, yatırımların geri dönüşünü ve iş fırsatlarını en üst düzeye çıkarmakla sınırlı değildir, aynı zamanda taraflar arasında güven ve şeffaflık sağlayarak iş ortaklıklarını kolaylaştırmaktadır. Bu araştırma, bilgi güvenliği uygulamalarının önemini ortaya koymaya çalışmıştır" Bu akademik çalışma BGYS'nin faydalarını teyit eder niteliktedir (Sindhuja, 2021, s.382-383).

Bir şirketin ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) belgesine sahip olması, firmanın sahip olduğu bilgi varlıklarının farkında olduğunu, güvenlik risklerini bildiğini ve yönetebildiğini, ayrıca bu riskleri korumak için çeşitli yöntemler uyguladığını gösterir. Bu belgeyle şirket, kayıt altına aldığı bilgi varlıklarını korumak için standartta belirtilen kuralları uyguladığını tüm müşteri, personel, paydaş, iş ortakları ve üçüncü şahıslara taahhüt etmiş olur.

ISO/IEC 27001 standardı, şirketin BGYS oluşturmasında yardımcı olur, bilgi güvenliğinin nasıl yönetileceğini tanımlar. Bu standard, BGYS nin nasıl kurulacağı, uygulanması ve sürdürülebilmesi ile iyileştirmelerin nasıl yapılacağı konusunda şartları belirlemek için hazırlanmıştır. Kuruluşlar tarafından BGYS'nin kabul edilerek uygulanması stratejik bir karardır (Çubukçu, 2018).

Firmalar, ticari sırlar, üst yönetim tarafından alınan stratejik kararlar, finansal veriler, sinai haklar, ticari alışveriş gereğince alınan ve korunması gereken kıymetli evraklar, akdedilen sözleşmeler, var ise formüller gibi değişik türden verilere sahiptir. Bunlardan

bazıları gizli kalması gereken türden, bir kısmı ise sadece tüzel kişiliğe ilişkin veriler olup sadece firma içinde paylaşılmasına izin verilen türden veriler olabilmektedir. Kimi veriler de kamuya açık türdendir. Bu bilgiler çoğu zaman, tek bir yerde değil, lojistik işletmesinin faaliyette bulunduğu, merkez ofis, varsa şubeler (yurtiçi-yurtdışı) ve depolarında kayıt altına alınmaktadır. Bu durumda veriyi kayıt eden kişiler, kayıt edilen ortam ve kayıt edilen veri türü değişiklik göstermektedir. Bilgilerin tamamı tek bir ana merkezde toplanıyor olsa dahi, güvenliklerinin tüm bu birim/bölüm/departman/şube vs. kapsayacak şekilde sağlanması gerekir. ISO 27001 bilgi güvenliği yönetim sistemi, bu karmaşık yapıya uygun ve lojistik şirketlerin bilgi güvenliği ihtiyacını karşılayabilecek bir modeldir.

Büyük ölçekli firma yapılanmalarında karşılaşılan veri ihlaline ilişkin olarak, ihlalin tüm grup şirketlerini etkileyecek şekilde oluştuğuna dair, Kişisel Verileri Koruma Kurulu tarafından verilmiş kararlar bulunmaktadır.

> Şirketler Grubu bünyesinde faaliyet gösteren çok sayıdaki veri sorumlusu şirket, Kuruma intikal eden veri ihlal bildirimlerinde özetle: 01.11.2021 tarihinde sistemlerin çalışmadığının fark edilmesi üzerine fidye yazılımı saldırısına maruz kalındığının tespit edildiği, dosya sistemi, elektronik posta sistemi, muhasebe ve insan kaynakları departmanının kullandığı ERP sistemi, özlük dosyaları ile resmi ve özel dosyaların şifrelendiği, ihlalden etkilenen verilerin veri sorumluları sunucularında bulunan tüm kişisel verilerden oluştuğu, ihlalden etkilenen ilgili kişilerin; personel, mevcut ve potansiyel müşteriler ve kullanıcılar olarak veri sorumlularının süregelen faaliyetleri çerçevesinde verileri sistemde bulunan tüm kişiler olduğu (Kişisel Verileri Koruma Kurulu Kararı, 2021).

Karardan anlaşıldığı üzere, bir şirketler grubu bünyesinde değişik konularda faaliyet gösteren çok sayıdaki anonim şirket veri sorumlusu, veri ihlali yaşamış ve sistemlerinde bulunan tüm kişisel veriler siber saldırganların kontrolüne geçmiştir. Olayda, değişik veri sorumluları tarafından kayıt altına alınmış olan, çeşitli tür ve sayıdaki bilgilerin, yeterli güvenlik tedbiri alınmaması sebebi ile yetkisiz kişilerin eline geçmesi durumu söz konusudur.

Bazı hallerde de, işlemlerin devamı için, ISO/IEC 27001 bilgi güvenliği belgesine sahip olunması ve istenilen birime ibraz edilmesi zorunluluğu bulunmaktadır. Örneğin; 21 Mayıs 2014 tarih 29006 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Gümrük İşlemlerinin Kolaylaştırılması Yönetmeliği'nde", Yetkilendirilmiş Yükümlü Statüsü İçin Gereken Koşullar ve Başvuruda Aranacak Belgelere yer verilmiştir. Yönetmeliğin İkinci kısım, 10. Maddesi "Başvuru için aranacak belgeleri" düzenlemektedir.

"Gümrük İşlemlerinin Kolaylaştırılması Yönetmeliği

Başvuru için aranacak belgeler

MADDE 10 – (1) Başvuru sırasında Ek-1/A'da yer alan başvuru formunun yanısıra aşağıdaki belgeler de ibraz edilir.

e) Avrupa Akreditasyon Birliğinin karşılıklı tanıma anlaşmalarına imza atmış akreditasyon kurumları tarafından akredite edilmiş uygunluk değerlendirme kuruluşlarınca düzenlenecek ve akreditasyon kurumunun markasını taşıyan (Değişik ibare:RG-13/10/2017-30209) geçerli ISO 9001 ve ISO 27001 sertifikalarının aslı veya düzenleyen kuruluş tarafından onaylı örneği.

(3) (Değişik:RG-13/10/2017-30209) Birinci fıkranın (e) bendinde sayılan;

b) ISO 27001 sertifikası; gümrük ve dış ticaret işlemlerini ve bu işlemlerine ilişkin lojistik, depolama, muhasebe, finans ve bilgi işlem faaliyetlerinin bilgi varlıkları ile bu varlıkları korumak amacıyla kullandığı güvenlik önlemlerini, kapsamalı (Değişik ibare:RG-21/2/2020-31046 Mükerrer) ve bu faaliyetlerin yürütüldüğü, kısmen kiralama yoluyla edinilenler hariç olmak üzere on beşinci fıkra kapsamındaki tüm idari bina ve tesislere ilişkin olarak alınmış olmalıdır.

Bu kuralın istisnası;

(18) (Ek:RG-21/2/2020-31046 Mükerrer) 18/12/1981 tarihli ve 2565 sayılı Askeri Yasak Bölgeler ve Güvenlik Bölgeleri Kanunu kapsamında askeri yasak bölge ve askeri güvenlik bölgesi olarak belirlenen yerler içerisinde faaliyet gösteren firmaların, bu bölgede yer alan bina ve tesisleri için ISO 9001 ve ISO 27001 sertifikası aranmaz" şeklinde belirtilmiştir (T.C. Resmi Gazete, 2014).

Yasal düzenlemeye göre, ibraz edilmesi gereken ISO 27001 BGYS belgesinin, gümrük ve dış ticaret süreçleri ile bu süreçlere bağlı lojistik, finans, depolama ve bilişim faaliyetlerinin bilgi varlıkları ile bunları muhafaza etmek için kullanılan güvenlik önlemlerini kapsaması gerekmektedir. Ayrıca ISO belgesinin, işlemlerin gerçekleştirildiği tüm yönetim binaları ve diğer yapılara ilişkin olarak alınmış olması şartı aranmaktadır. Yasa koyucu faaliyetlerin yürütüldüğü tüm bina ve tesislerdeki veri güvenliğinin sağlandığını görmek istemekte bunun için de ISO 27001 BGYS belgesini aramaktadır**.**

2.6.1.2 ISO/IEC 27001 Bilgi Güvenliği standardı kapsamı, PUKÖ ile ilişkisi ve kanunlara uyum

Bilgi Güvenliği Yönetim Sistemi sürekliliği olan bir gelişim sürecidir. BGYS'nin kurulması ve idaresinde, PUKÖ (Planla, Uygula, Kontrol et, Önlem al) döngüsü Plan-Do-Check-Act süreçleri kullanılır (Çubukçu, 2018).

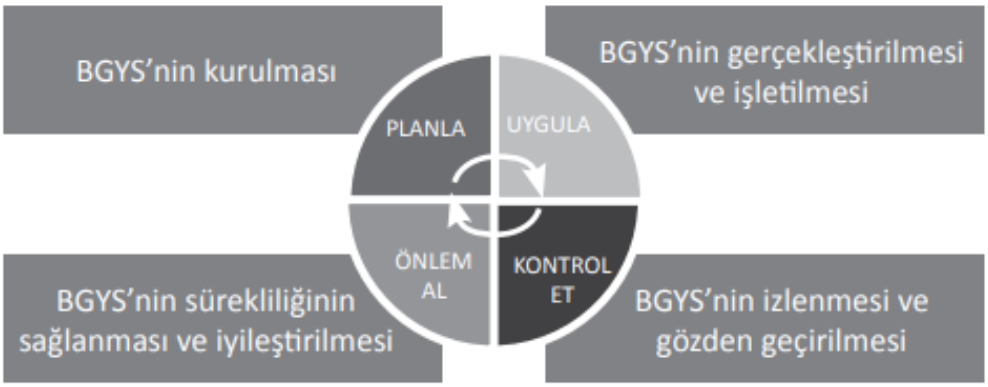
1-Ne yapılacağına karar verilmesi (Planla),

2-Kararların gerçekleştirilmesi (Uygula),

3-Kararların çalıştığının kontrol edilmesi (Kontrol et),

4-Çalışmayan kararların kontrol ve iyileştirilmesi (Önlem al).

PUKÖ döngüsü (Plan-Do-Check-Act/PDCA), W. Edwards Deming tarafından ortaya konulmuştur. Bu döngünün 4 aşamasında; Planlama, amaç ve hedefler belirlenmekte, Uygulama, prosedürler uygulanmakta, sonra ki aşamada gerekli kontroller yapılmakta ve Önlem alma son aşamada, süreçlerin iyileştirilmesi sağlanmaktadır (Araalan , 2020**).** PUKÖ döngüsü ve BGYS'nin çalışması Şekil 8'de gösterilmiştir.



Şekil 8. PUKÖ Döngüsü ve BGYS nin Çalışması (Yılmaz, 2014)

ISO/IEC 27001:2013 standardını uygulamak isteyen kurumlar, sektör ya da büyüklüğüne bakılmaksızın ana maddeleri uygulamak zorundadır. 25 Ekim 2022 tarihinde yapılan değişiklik ile ISO 27001 ana maddeler aynı kalmakla beraber alt maddelere ufak eklemeler yapılmıştır. Bu değişiklikler güncel teknolojik, idari, hukuki gelişmelere uyum sağlamak üzere yapılmaktadır. Çünkü dijitalleşme ile birlikte bilgi güvenliğine ilişkin riskler her geçen gün ve değişerek artmaktadır. BGYS kesintisiz devam eden bir ilerleme süreci olduğundan güncel gereksinimlere uygun hale getirilmesi ihtiyacı bulunmaktadır.

Standardın ana maddeleri Tablo 14'de yer almaktadır. Tablo 15'de ise bu ana maddeler ile PUKÖ döngüsü arasındaki ilişki gösterilmektedir.

Tablo 14. ISO/IEC 27001:2022 BGYS Standardı Ana Maddeleri (ISO/IEC, 2022)

1-Kapsam	6-Planlama
2-Bağlayıcı Atıflar	7-Destek
3-Terimler ve Tanımlar	8-İşletim
4-Kuruluşun Bağlamı	9-Performans Değerlendirme
5-Liderlik	10-İyileştirme

Tablo 15.ISO/IEC 27001:2022 BGYS Standart Maddeleri ve PUKÖ Döngüsü İlişkisi (ISO/IEC, 2022)

Standart Maddesi	Madde Başlığı	PUKÖ Döngüsü
4	Kuruluşun Bağlamı	Planlama
5	Liderlik	Planlama
6	Planlama	Planlama
7	Destek	Uygulama
8	İşletim	Uygulama
9	Performans Değerlendirme	Kontrol Et
10	İyileştirme	Önlem Al

ISO/IEC 27001 BGYS ana maddelerinden "Liderlik md.5" başlığı altında, politika hazırlığına ilişkin düzenlemelere yer verilmiştir.

"ISO 27001:2022 Ana Maddeleri

5.2 Politika

Üst yönetim, aşağıdaki hususları sağlayan bir bilgi güvenliği politikası oluşturmalıdır….

e) Dokümante edilmiş bilgi olarak mevcut olmalıdır,

f) Kuruluş içinde duyurulmalıdır,

g) Uygun olduğu şekilde, ilgili tarafların erişimine açık olmalıdır" (ISO/IEC, 2022).

Bilgi güvenliği yönetim sistemi için, şirket üst yönetiminin politikayı hazırlaması, kuruluş içinde duyurması ve erişime açık hale getirmesi ISO 27001 BGYS standartı gereğince zorunlu kılınmıştır.

Bilgi güvenliği yönetim sisteminin kurulmasında, firma yönetiminin teşviki ve tüm personelin sürece katılımı gerekir. Ayrıca süreci yönetecek ekibin kurulması da önemlidir. 2020 yılı Türkiye Siber Risk Algı Araştırması Raporunun sonuç bölümü; "*Her şirkette siber risklerin gelişimi ve stratejilerine yönelik çalışacak ayrı bir Siber Güvenlik Komitesi kurulması, bu komitenin insan kaynakları, operasyon, hukuk ve diğer iş birimlerinden yetkilileri barındırması, düzenli bir toplantı takvimi ile iletişimde kalması etkili bir yönetim şekli olabilecektir"* şeklindedir (Marsh ve TÜSİAD, 2020, s. 30).

Standardın ana maddelerinde, şirketlerin (iç ve dış) dökümanlarını oluşturmasından söz edilmektedir. Dış kapsam döküman içeriği, Yasalara uyumu da kapsamaktadır. Yine standardın Ek-A maddelerinde, yasalara uyum (kanun, sözleşmesel) belirtilmektedir (Çubukçu, 2018)**.** Dış kapsam yasalara uyum, şirket operasyonlarının yürürlükteki mevzuat ve sözleşmelere uygun olarak yürütülmesi şeklinde olacaktır.

"ISO 27001:2022 Ek-A maddeleri;

A 5.31: Bilgi güvenliği ile ilgili yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler ve kuruluşun bu gereklilikleri karşılama yaklaşımı belirlenmeli, dokümante edilmeli ve güncel tutulmalıdır.

A.5.32: Kuruluş, fikri mülkiyet haklarını korumak için uygun prosedürleri uygulamalıdır.

A.5.34: Kuruluş, yürürlükteki yasalara ve düzenlemelere ve sözleşme gerekliliklerine göre gizliliğin korunmasına ve PII'nin (kişiyi tespit bilgisi) korunmasına ilişkin gereklilikleri belirlemeli ve karşılamalıdır" şeklindedir (ISO/IEC, 2022, s. 13).

A.5.31 md. düzenlemesinin amacı, veri güvenliğine ilişkin hukuki, sözleşmeye dayalı ve düzenleyici gerekliliklere uyumu sağlamaktır. İş yapılan diğer ülkeler veya yasal zeminleri de dikkate almak gerekir. A.5.32 md. düzenlemesinin amacı, fikri mülkiyet hakları ve tescilli ürünlerin kullanımı ile ilgili hukuki, anlaşmaya dayalı ve düzenleyici gerekliliklere uyumu sağlamaktır. Hakların korunmasına ilişkin politika hazırlanabilir. Hangi varlıklar için fikri mülkiyet durumu olduğu envanterde belirlenebilir. A.5.34 md. düzenlemesinin amacı, kişisel verilerin korunmasının bilgi güvenliği yönleriyle ilgili hukuki, anlaşmaya dayalı ve düzenleyici gerekliliklere uyumu sağlamaktır (Tosunoğlu, t.y.).

2.6.1.3 ISO/IEC 27001 Bilgi Güvenliği standardı ve Kişisel Verilerin Korunması Kanunu

ISO/IEC 27001 standartının eki olan Ek-A maddeleri firmalara, bilgi güvenliğini sağlama konusunda kontrol listesi imkanı sunmakta ve rehberlik etmektedir. Denetim mekanizması ile de devamlılık arz eden açıklık ve zafiyet tespiti yapılabilmektedir.

ISO 27001:2013'den ISO 27001:2022 versiyonuna geçişte, standardın ana maddeleri değişmemiş sadece ufak eklemeler yapılmıştır. Bunlardan 6.3 maddesi standarda eklenen yeni bir maddedir.

"ISO 27001:2022 Ana Maddeleri

6.3 Değişikliklerin planlanması

Kuruluş, bilgi güvenliği yönetim sisteminde değişiklik ihtiyacı belirlediğinde, değişiklikler planlı bir şekilde gerçekleştirilmelidir" (ISO/IEC, 2022).

Madde, ihtiyaç halinde yapılacak değişikliklere dikkat çekmektedir. Teknolojinin hızla ilerlemesiyle birlikte risklerin türü ve biçimi de değişmektedir. Bu durum, bilgi güvenliği önlemlerinin tekrar incelenmesini ve yenilenmesini gerekli kılmaktadır. Standart, bu konuya açıklık getirerek, değişikliklerin belli bir plan çerçevesinde yapılması gerektiğini belirtmektedir.

ISO 27001:2013'de, standardın eki Ek-A kontrolleri belgesi 14 madde başlığından oluşmakta iken (A.5 – A.18 maddeleri), ISO 27001:2022 versiyonunda 4 madde başlığı altında (A.5 – A.8 maddeleri) toplanmıştır. İçerik aynı kalmakla birlikte kısaltmalara gidilmiş ve güncel gelişmelere uygun ekleme, birleştirme ve ad değiştirme şeklinde düzenlemeler yapılmıştır. Örneğin, A.5.23 Bulut Hizmetleri Kullanımı için Bilgi Güvenliği, A.5.7 Tehdit İstihbaratı ve A.7.4 Tesislerin Fiziksel Güvenlik İzleme başlıkları şeklinde yeni madde eklemeleri yapılmıştır. Böylece, kontrol maddeleri içinde, günümüz uygulamalarında önemli bir yeri olan bulut hizmetleri için bilgi güvenliği düzenlemelerine yer verilmiştir. Yeni standard, iş uygulamalarının dijital dönüşümü ile ilgili daha fazla gizlilik ve siber güvenlik konularını içerecek şekilde genişletilmiştir.

ISO 27001 BGYS standardı günümüz ihtiyaç ve gelişmelerine uygun olarak revize edilmektedir. Bu haliyle, bilgi güvenliğini sağlamaya yönelik en iyi standart olduğunu ortaya koymaktadır. Tablo 16'da ISO/27001:2013 Ek-A kontrol madde başlıkları gösterilmiştir.

Tablo 16. ISO/27001:2013 BGYS Ek-A Maddeleri (Batı Akdeniz İhracatçılar Birliği, 2017)

A.5	Bilgi güvenliği politikaları	A.12	İşletim güvenliği
A.6	Bilgi güvenliği organizasyonu	A.13	Haberleşme güvenliği
A.7	İnsan kaynakları güvenliği	A.14	Sistem temini, geliştirme ve bakımı
A.8	Varlık yönetimi	A.15	Tedarikçi ilişkileri
A.9	Erişim kontrolü	A.16	Bilgi güvenliği ihlal olayı yönetimi
A.10	Kriptografi	A.17	İş sürekliliği yönetiminin bilgi güvenliği hususları
A.11	Fiziksel ve çevresel güvenlik	A.18	Uyum (Yasalara uyum)

2022 yılında yapılan değişiklik ile 4 ana başlık altında toplanmış olan Ek-A kontrol maddelerine Şekil 9'da yer verilmiştir.



Şekil 9. ISO/27001:2013 Ek-A ve Değişen ISO/IEC 27001:2022 Ek-A Kontrol Maddeleri (Tosunoğlu, t.y.)

Kişisel Verilerin Korunması Kanunu 12'nci maddesinde, veri sorumlularının, kişisel verilerin muhafazasını sağlamak üzere gereken tüm idari ve teknik tedbiri almak zorunda oldukları belirtilmiştir. Alınacak tedbirlere açıklık getirilmek üzere, Kurum tarafından, Kişisel Veri Güvenliği İdari ve Teknik Tedbirler Rehberi yayımlanmıştır. Rehberde yer alan tedbirlere ilişkin düzenlemelere Tablo 17 ve Tablo 18'de yer verilmiştir.

Tablo 17. Kişisel Verilerin Korunması Kanunu İdari Tedbirler (Kişisel Verileri Koruma Kurumu, 2018)

İDARİ TEDBİRLER
Kişisel veri işleme envanteri hazırlanması
Kurumsal politikalar (Erişim, Bilgi güvenliği, Kullanım, Saklama ve imha vb.)
Sözleşmeler (Veri sorumlusu-Veri sorumlusu, Veri sorumlusu-Veri işleyen arasında)
Gizlilik taahhütnameleri
Kurum içi periyodik ve/veya rastgele denetimler
Risk analizleri
İş sözleşmesi, disiplin yönetmeliği (Kanuna uygun hükümler ilave edilmesi)
Kurumsal iletişim (Kriz yönetimi, kurul ve ilgili kişiyi bilgilendirme süreçleri, itibar yönetimi vb.)
Eğitim ve farkındalık faaliyetleri (Bilgi güvenliği ve kanun)
Veri sorumluları sicil bilgi sistemine (VERBİS) bildirim

Tablo 18.Kişisel Verilerin Korunması Kanunu Teknik Tedbirler (Kişisel Verileri Koruma Kurumu, 2018)

TEKNİK TEDBİRLER	
Yetki matrisi	Log kayıtları
Yetki kontrol	Veri maskeleme
Erişim logları	Veri kaybı önleme yazılımları
Kullanıcı hesap yönetimi	Yedekleme
Ağ güvenliği	Güvenlik duvarları
Uygulama güvenliği	Güncel anti-virüs sistemleri
Şifreleme	Silme, yok etme veya anonim hale getirme
Sızma testi	Anahtar yönetimi
Saldırı tespit ve önleme sistemleri	

Rehberde idari tedbirler bakımından, risk ve tehditlerin tespit edilmesi, çalışanların bilgilendirilmesi ve farkındalık çalışmaları, kişisel bilgi güvenliği politika ve prosedürlerinin belirlenmesi, gizlilik ve veri işleyenler ile ilişkilerin yönetimi gibi konulara yer verilmiştir. Kanunlara uygun politika ve prosedürlerin hazırlanması gerekliliği belirtilmiştir.

Kişisel Verilerin Korunması Kanunu gereğince alınması gereken her iki tedbir türü ile ISO/IEC 27001:2013 bilgi güvenliği standard maddelerinin karşılaştırma tablosuna Tablo

19'da yer verilmiştir. Karşılaştırma tablosu incelendiğinde, her iki düzenleme kapsamında, bilgi güvenliği politikaları ile kanuni düzenlemelerin ve kanuna uygun yönergelerin hazırlanmasının önemine yer verildiği gibi, teknik konular, risk değerlendirme, analiz ile bilgi güvenliği konusunda eğitim ve personel farkındalığının arttırılmasının önemine vurgu yapıldığı görülmektedir.

Tablo 19. KVKK ve ISO 27001:2013 BGYS Standardı Karşılaştırması (CottGroup, 2022)

KVKK Rehberine Göre Alınması Gereken Teknik ve İdari Tedbirler	**ISO/IEC 27001:2013 Standart Maddesi**
Yetki Matrisi	A.9.2 Kullanıcı erişim yönetimi
Yetki Kontrol	
Erişim Logları	A.12.4.1 Olay kaydetme
Kullanıcı Hesap Yönetimi	A.9.4.2 Güvenli oturum açma prosedürleri
Ağ Güvenliği	A.13.1.2 Ağ hizmetlerinin güvenliği
Uygulama Güvenliği	A.14.2.6 Güvenli geliştirme ortamı
Şifreleme	A.10.1 Kriptografik Kontroller
Sızma Testi	A.12.6.1 Teknik açıklıkların yönetimi
	A.12.6.1 Teknik açıklıkların yönetimi
Saldırı Tespit ve Önleme Sistemleri	
Log Kayıtları	A.12.4.1 Olay kaydetme
Veri Maskeleme	Yok
Veri Kaybı Önleme Yazılımları	A.12.6.1 Teknik açıklıkların yönetimi
Yedekleme	A.12.3.1 Bilgi yedekleme
Güvenlik Duvarları	A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması
Güncel Anti-Virüs Sistemleri	A.12.2.1 Kötücül yazılımlara karşı kontroller
Silme, Yok Etme veya Anonim Hale Getirme	A.8.3.2 Ortamın yok edilmesi
Anahtar Yönetimi	A.10.1.2 Anahtar yönetimi
Kişisel Veri İşleme Envanteri Hazırlanması	**A.8.1.1 Varlıkların envanteri**
Kurumsal Politikalar (Erişim, **Bilgi Güvenliği,** Kullanım, Saklama ve İmha vb.)	**5.2 Politika**
Sözleşmeler (Veri Sorumlusu – Veri Sorumlusu, Veri Sorumlusu – Veri İşleyen Arasında)	A.7.1.2 İstihdam hüküm ve koşulları

Gizlilik Taahhütnameleri	A.15.1.2 **Tedarikçi anlaşmalarında** güvenliği ifade etme
Kurum İçi Periyodik ve/veya Rastgele **Denetimler**	9.2 **İç tetkik**
Risk Analizleri	6.1.2 Bilgi güvenliği **risk değerlendirme**
İş Sözleşmesi, Disiplin Yönetmeliği **(Kanuna Uygun** Hükümler İlave Edilmesi)	A.7.2.3 Disiplin prosesi A.18 **Uyum (Yasalara uyum)**
Kurumsal İletişim (**Kriz Yönetimi,** Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.)	A.17 İş sürekliliği yönetiminin bilgi güvenliği hususları
Eğitim ve Farkındalık Faaliyetleri **(Bilgi Güvenliği ve Kanun)**	A.7.2.2 **Bilgi güvenliği farkındalığı**, eğitim ve öğretimi A.18 **Uyum (Yasalara uyum)**
Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim	Yok

Kişisel Verilerin Korunması Kanunu kapsamında oluşturulan tedbirler, ISO/IEC 27001 bilgi güvenliği standartlarına benzer nitelikte ve uyumludur. Bundan dolayı, ISO 27001 BGYS standartına sahip kuruluşların KVKK düzenlemesine uyumu daha kolay olmaktadır. Ayrıca ISO 27001 BGYS standartı sadece kişisel verileri değil her türden veriyi koruma altına alan bir düzenlemedir. Diğer taraftan, KVKK hükümlerine göre idari ve teknik tedbirleri yerine getiren firmalar, ISO 27001 bilgi güvenliği standardının gerekliliklerine uyum sağlamakta zorlanmayacaktır.

Kişisel Verileri Koruma Kurumu Veri Güvenliği Rehberi'nde kurumlardan; risk ve tehditlerin değerlendirilmesi, personelin eğitilerek farkındalıklarının sağlanması, veri güvenliği politika ve prosedürlerinin oluşturulması, veri işleyenlerle ilişkilerin sürdürülerek yönetilebilmesi için gereken idari ve hukuki tedbirlerin alınması beklenmektedir. BGYS, kuruluşların bilgi güvenliği risklerini yönetme sürecinde yasal, fiziksel ve teknik kontrolleri içeren politika ve prosedürleri içerir. BGYS içerisinde personel davranışları, süreçler ve teknoloji vardır. Bu sistem, sadece belirli bir bilgiyi yönetmek için kullanılabileceği gibi kurumun tüm süreçlerine de uygulanabilir. Kurumların yerine getirmesi gereken İdari Tedbirler Tablo 17'de yer alan Risk Analizleri konusu, ISO 27001 BGYS'nin ele aldığı temel konulardan birisidir. BGYS kapsamında risk yaklaşımını hayata geçiren kurumlar KVKK'nın beklediği Risk Analizi çalışmasını yerine getirmiş olurlar. KVKK – BGYS ilişki Tablosu 19 incelendiğinde ve risk analizi ve dokümantasyon hazırlama hususları dikkate alındığında KVKK ile BGYS arasında

güçlü bir bağ olduğu görülecektir. Kişisel Verilerin Korunması Kanunu uyum sürecinde kanunun hukuki ve teknik boyutlarını ele alırken ISO 27001 BGYS Sertifikası'nın KVKK'yı desteklediği ve etkin bir rol aldığı görülecektir (Tosunoğlu, t.y.).

Literatür çalışmalarında, ISO 27001 bilgi güvenliği standardını uygulayan sertifikalı firmaların, Avrupa Birliği tarafından yayınlanan Genel Veri Koruma Tüzüğü'ne (GDPR) uyumda zorluk çekmedikleri ve standardın yasal düzenlemelere uyumu kolaylaştırıcı özelliği olduğu ifade edilmiştir.

Dijitalleşmenin yaygınlaşmasıyla birlikte dünya, siber saldırılara karşı giderek daha savunmasız hale gelmiştir. Avrupa Birliği'nde, örneğin, son yıllarda Siber Güvenlik Stratejisi ile ilgili konularda çeşitli direktifler ve yönetmelikler yayınlanmış ve uygulanmıştır. Bunlar, şirketlerin bilgi güvenliği gereksinimlerine uyum göstermelerine yardımcı olmada standartların ve sertifikaların hayati rolünü açıkça vurgulamaktadır. ISO/IEC 27001, veri güvenliğinin sağlanması için geliştirilmiş en önemli uluslararası standarttır (Mirtsch, Blind, Koch ve Dudek, 2021).

Halihazırda ISO 27001 standardlarını uygulayan ve bir BGYS ve ilgili güvenlik kontrollerini kullanan kuruluşlar, GDPR gerekliliklerine uymak için çok daha az çabaya ihtiyaç duyarlar (Diamantopoulou, Tsohou ve Karyda, 2020).

ISO/IEC 27001 sertifikalı firmaların temel olarak, bilgi güvenliğini artırma ve güvenlik ihlalleri riskini azaltma gibi önleme hedefleri ve ikinci olarak, pazara erişim sağlama, iyileştirme, kurumsal imaj, satış artışları gibi pazarlama hedefleri gereğince standartı önemsediği anlaşılmaktadır. Ayrıca, yakın zamanda yapılan araştırmalar, ISO/IEC 27001'in benimsenmesini, Genel Veri Koruma Yönetmeliği (GDPR) veya ulusal siber güvenlik yasaları ile ilgili düzenlemelere uyumun sağlanmasıyla giderek daha fazla ilişkilendirdiklerini göstermektedir. Şirketler, ISO/IEC 27001'in GDPR uyumluluğuna yardımcı olduğu Genel Veri Koruma Tüzüğü gerekliliklerine uymak zorundadır (Mirtsch, Kinne ve Blind, 2021).

2.7 Veri İhlalleri

Bilgiye yönelik tehdit çeşitleri fiziksel, yazılım kaynaklı ve kullanıcılardan kaynaklı olarak sıralanabilir. Ayrıca kullanılan araç veya sayısına göre de bir sınıflandırma

yapılması mümkündür. Günümüzde dijitalleşme ile birlikte oluşan yeni tehditler içinde siber saldırılar önemli bir yer tutmaktadır. Gelinen aşamada bilgi güvenliği riskleri şirketler bakımından önem vermeleri gereken bir mesele haline gelmiştir (Alemdaroğlu, 2020).

2.7.1 Siber saldırılar

Siber saldırı, bilgisayar ve internet kullanılmak suretiyle ve yasal olmayan amaçlarla verileri çalmak veya ele geçirmek, kullanmak, değiştirmek için siber saldırganlar tarafından yapılan yasadışı bir eylemdir. Eylemi gerçekleştirenler, kullanıcıları yanıltmak üzere çeşitli türde yöntem kullanmaktadır (Hatipoğlu ve Tunacan, 2021). Siber saldırılar sistemdeki güvenlik zaafiyetleri kullanılarak yapılır.

Saldırılar, kötü niyetli yazılımlar ile yapılabildiği gibi, donanımlar kullanılarak da yapılabilir. Bazı popüler türler şöyledir;

- Kötü niyetli yazılımlar; Bilgisayar ve farklı teknolojik cihazları ve sistemleri çalışmaz hale getirerek, çoğalabilir ve gizlenebilirler. Bulaştıkları sistemlerin normal çalışmalarını engelleyerek, gönderilme amacına hizmet etmesini sağlarlar.

- Zincir E-Posta; Gönderilen e-postalar ile bireylerin bunları diğer bireylere göndermesi amaçlanır. Böylece kullanıcıların e-posta adres listesinden yararlanılarak daha fazla kişiye erişim sağlanması amaçlanmaktadır.

- Casus yazılım (Truva atı); Truva atı kendisini belleğe yükler ve sistemin zaafiyetlerinden yararlanarak programı kontrol eder. Bilgisayar, tablet ve telefonlarda kendini belirgin hale getirebilmektedir.

- Hizmet Aksatma (DDoS ve DoS); İnternet sitelerine, çevrim içi servislere çoklu istek göndererek bunların çalışamaz hale gelmesine sebep olur.

- Oltalama saldırısı; Genellikle sahte web siteleri kullanılmaktadır. E-posta gönderilerek ve inandırıcı bir hikaye metni ile bireyleri aldatmaya yönelik kullanılan bir siber saldırı çeşididir.

- İstem Dışı Alınan E-posta (Spam); Web sayfalarından alınan e-posta adreslerine iletilen ve ticari gaye güden e-postalardır.

- Sosyal Mühendislik; Kullanıcıları bazı amaçlarla aldatmayı ve bunun sonucunda özel bilgiler almayı hedefleyen bir yöntemdir. Kurum yapısı, çalışanların bilgileri, şifreleri ve saldırıda kullanılabilecek her türlü bilginin toplanmasıdır. İnsan unsuru bu saldırı türünde önemlidir.

- Tedarik Zinciri Saldırıları; Tedarik zincirindeki yeterince emniyetli olmayan uygulamalara yönelik yapılan saldırılar neticesinde bu uygulamaların elde edilmesi ve bunlar üzerinden kuruma ve bireylere zarar verme amacı taşıyan saldırı tipidir (Aslay , 2017) (Alemdaroğlu, 2020) (Turan, 2021).

2.7.2 Veri ihlaline ilişkin araştırmalar

Dijitalleşme birey ve kurumların yaşam ve iş şekillerini değiştirdiği gibi, siber saldırganların yöntemlerini de dönüştürmektedir. Siber saldırganlar yeni teknolojilerin güvenlik açıklarından faydalanırken diğer taraftan da kendi saldırı yöntemlerini dijital hale getirerek yeni teknolojileri saldırılarında kullanmaktadır. Şekil 10'da, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA)'nın bir saldırı ortamında kullanılabilecek olan farklı yöntemleri tasviri gösterilmektedir (Zaralı, 2022).



Şekil 10. ENISA Saldırı Ortamı (Zaralı, 2022)

Araştırmalara göre, ülkemiz, 2020 yılında siber saldırganların hedefindeki ülkelerin başında gelmiştir. 2018 yılında 73.000 siber saldırı olayı gerçekleşmişken, 2020'de bu rakam 100.000'i geçmiştir. Çok sayıdaki kuruluşun sistemlerine girilerek siber saldırılar düzenlenmiş ve fidye talebinde bulunulmuştur (BT Haber , 2021).

Bütünleşik siber güvenlik alanında lider olan WatchGuard Tehdit Laboratuvarı verilerine göre, "2022 yılında Türkiye'de vuku bulan yazılım saldırıları, geçen yıla kıyasla büyüme göstererek 1.015.810 olmuştur. Artan saldırılara karşı kurum ve bireylerin dikkatli olmaları gerektiği" belirtilmiştir (EPN Haber Merkezi, 2023).

Siber savunma firması Kaspersky'nin, Orta Doğu, Türkiye ve Afrika bölgelerini kapsayan '9. yıllık Cyber Security Weekend META 2024' etkinliğinde bölge ülkelerinin siber tehdit ortamının gelişimi ve kırılganlıkları ele alınmıştır. Buna göre, çevrimiçi tehditlerden etkilenen en yüksek kullanıcı sayısının Türkiye'de görüldüğüne dikkat çekilmiştir. 2024 yılında bu saldırıların daha da artacağı belirtilmiştir. Bunun en önemli sebepleri ise, Türkiye'nin fiziki konumu gereğince önemli bir coğrafyada yer alıyor olması, siber güvenlik alanında farkındalık yetersizliği, yüksek nüfus ve güvenliğe yeterli bütçe ayrılmaması gösterilmiştir (Para Dergi, 2024).

Araştırmalar, siber saldırıların sayısında ve çeşitlerinde bir artış olduğunu ortaya koymaktadır. Firmalar, saldırganların fidye talepleri ile maddi zarara uğramakta ayrıca, ihlal olayının sonucunda firmanın sektördeki itibarı, güvenilirliği ve rekabet gücü de olumsuz şekilde etkilenmektedir.

Yargı kararları veri ihlallerinin çoğu kez şirket içi kaynaklı olduğunu göstermektedir. Ayrıca, sadece dijital sistemlerde saklanan verilere değil, çoğu kez fiziksel olarak muhafaza edilen verilere de izinsiz erişim ve kullanım girişimlerinde bulunulmaktadır. Fiziki varlıklar, kağıt belgeler, kambiyo senetleri, değerli kağıtlar, fotokopi makinası gibi varlıklar şeklinde sayılabilir. Fiziki varlıkların muhafaza edildiği ortamlar, dolap, kasa gibi alanlardır. Diğer taraftan personelin farklı şekillerde edindiği bilgiler (bayi ziyaretleri, tanıtımlar gibi) de bulunmaktadır. Bu varlıkların tamamının izinsiz erişimlere karşı korunması gerekir.

Bazen de siber saldırılar, hizmet alınan diğer şirketlerin sistemlerine yönelik yapılmakta ve bu sebeple asıl şirket çalışmaları bu durumdan etkilenmektedir. Örneğin, bir olayda havayolu şirketi siber saldırıya uğradıklarını açıklamıştır. Domain hizmeti aldıkları üçüncü kişi firmanın sistemlerine yasadışı bir saldırı yapıldığını, bu sebeple ziyaretçilerin kendi web sayfalarına gelemeden başka bir sayfaya yönlendirildiklerini, kendi firma hizmetlerine, bilgilerine ve sunucularına yönelik herhangi bir erişim veya girişimin söz konusu olmadığını belirtmiştir (Sözcü Gazetesi , 2021). Olayda, siber saldırı, havayolu şirketinin dışarıdan domain hizmeti aldığı diğer şirketin sistemine yönelik yapılmıştır. Hizmet satınalınan şirket yeterli güvenlik tedbirini almadığından hizmet alan şirketin iş süreçleri kesintiye uğramıştır. Bu örnek, sadece şirket bilgi güvenliğini sağlamanın yeterli olmadığını, ayrıca hizmet alınan firmalar ile tedarikçi firmaların bilgi güvenliklerini sağlamış olmasının da gerekli olduğunu göstermesi açısından önemlidir.

Siber riskleri engellemek etkili bir veri güvenliği planlaması ile sağlanabilir. Bu planlamanın başarısı, tüm paydaşları sürece dahil eden siber yönetişim ile mümkündür. Bu çalışmada güvenliğin sağlanması için siber yönetişimin ehemmiyeti ve gerekliliği vurgulanmaktadır (Savaş ve Karataş, 2022).

2020 yılı Türkiye Siber Risk Algı Araştırması Raporu'na göre; "*Günümüzde birlikte çalışan şirketlerin (tarafların) birbirine güven duyması zincirin düzgün bir şekilde faaliyetine devam etmesi için önemlidir(…) Şirketlerden siber güvenlik konusundaki sorumluluklarının farkında olmaları beklenmektedir(...) Şirketler, işletme için geçici bir süreliğine hizmet veren kişilerden kaynaklı siber risklere karşı daha savunmasızdır"* (Marsh ve TÜSİAD, 2020).

ISO 27001:2022 Ek-A kontrol maddeleri A5.20 maddesinde, tedarikçi anlaşmalarında bilgi güvenliği düzenlemesine yer verilmiştir. "*İlgili bilgi güvenliği gereklilikleri, tedarikçi ilişkisinin tipine dayandırılarak her tedarikçi ile oluşturulmalı ve üzerinde anlaşmaya varılmalıdır"* (ISO/IEC , 2022).

Düzenlemenin amacı, tedarikçi ilişkilerinde üzerinde anlaşmaya varılmış bir bilgi güvenliği düzeyini sürdürmektir. Düzenleme veri ihlali kaynaklı zararlardan korunmak açısından önemlidir. Her halükarda yeterli tedbiri almayarak zarara sebebiyet veren taraf

bunlara katlanmak zorunda olacaktır. Önemli olan, gerekli güvenlik tedbirlerinin zamanında ve yeterli ölçüde alınarak riskin önlenmesi ve zarar oluşmasına engel olunmasıdır.

Literatür çalışmalarında, ISO 27001 BGYS'nin küçük ve orta büyüklükteki işletmeler için önemi üzerinde durulmuştur. Antunes, Maximiano, Gomes ve Pinto (2021), sonuçlar, bilgi güvenliği yönetiminin küçük ve orta ölçekli firmalara önemli faydalarını göstermiştir. ISO-27001:2013 çerçevesi, literatürde KOBİ'lerde bilgi güvenliğinin söz konusu olduğu en iyi uygulama olarak tanımlanmıştır.

Lojistik sektörü de büyüklükleri değişen firmalardan oluşmaktadır. İçlerinde küçük ve orta ölçekli (KOBİ) şirketler de bulunmaktadır. Birçok küçük ve orta ölçekteki işletme bilgi güvenliği standardına sahip değildir bunun çeşitli sebepleri olabilir. Ancak günümüzde siber saldırganların hedefinde, yaygın olarak bu büyüklükteki işletmeler bulunmaktadır.

"Bilgi güvenliği, işletmelerin yönetiminde önemli bir yere sahiptir çünkü verinin gizliliği, bütünlüğü ve erişilebilirliği gibi en değerli kaynaklarıyla ilgilenir. Küçük ve Orta Büyüklükteki İşletmeler (KOBİ), esas olarak büyüklükleri, bölgesel kapsamları ve finansal kaynakları nedeniyle bilgi güvenliği ve siber güvenlik yönetiminde kör nokta olarak görülmektedir" (Antunes, Maximiano, Gomes ve Pinto, 2021).

Siber Güvenlik İhlalleri Araştırmasına (2021,2022,2023) göre, her ölçekten firma siber saldırıların hedefindedir. Ancak siber saldırganlar çoğu kez, güvenlik tedbirleri iyileştirilerek geliştirilmiş şirketler yerine nispeten daha kolay ve karlı olarak düşündükleri küçük ve orta ölçekli firmalara yönelmektedir. Bazende ana hedefe ulaşmak için, tedarik zincirlerinde güvenlik açığı bulunan firmalar üzerinden asıl hedef verilerine ulaşmaktadırlar. Büyük ölçekli firmalar da saldırganların hedefindedir. Kişisel Verileri Koruma Kurulu'nun büyük ölçekli firma ve grup şirketleri hakkında verilmiş çok sayıda veri ihlal kararı bulunmaktadır. Bu sebeple, riski azaltmanın yolu, alınacak tedbirler ile bilgi güvenliğinin tam ve yeterli derecede sağlanmasıdır.

2.8 Türkiye Ulaştırma Politika Belgesi, Ulaştırma ve Haberleşme Şurası

Çalışmanın diğer amacı, araştırma kapsamında, Ulaştırma ve Altyapı Bakanlığı'nca hazırlanan 2020 tarihli, Türkiye Ulaştırma Politika Belgesinin "Veri (Bilgi)" başlıklı bölümünde yer alan siber güvenliğin sağlanmasına yönelik düzenlemelerin Lojistik Sektörü için uygun ve yeterli olup olmadığı hususunun değerlendirilmesidir.

Türkiye Ulaştırma Politika Belgesinin "Veri (Bilgi)" başlıklı bölümünde siber güvenlik konularına yer verilerek:

> Ulusal siber güvenliğimizin sağlanması için ulusal stratejiler geliştirileceği ve güncelleneceği; Ulusal stratejiler temel alınarak siber güvenliğin sağlanması için eylem planları oluşturulacağı; Kritik altyapıların kullanıldığı haberleşme,ulaştırma gibi alanlarda bilişim sistemlerinin güvenliğini sağlamak için risk analizleri, sektörel düzenlemeler yapılmasının gerekli olduğu; Ulaştırma verilerine KVKK'ya uygun ve güvenilir şekilde erişime sahip olunması, paylaşımı için veri yönetişimi mekanizmaları geliştirileceği; Ülkemizde üretilen ulaştırma ve haberleşme verilerinin,uluslararası arenada kabul görmüş güvenlik standartları ve gereksinimlerini karşılayacak şekilde üretimi, iletimi, saklanması, ve paylaşımının yapılacağı; Siber Güvenliğe ilişkin ulusal mevzuatın geliştirilmesinde uluslararası düzenlemeler ve standartların dikkate alınacağı; Ulusal siber güvenliğin sağlanması amacıyla kamu kurum ve kuruluşları, sivil toplum kuruluşları, yerel yönetimler, üniversiteler ve özel sektörün iş birliği içinde çalışacağı; Siber güvenliğin sağlanması konusunda bireylerin, kurum ve kuruluşların ve tüm paydaşların üzerine düşen sorumlulukları anlayarak bu sorumlulukları yerine getirecek şekilde hareket etmeleri gerektiği; Siber güvenlik alanında uzman insan kaynağının geliştirilmesine yönelik faaliyetlerin sürdürüleceği; Bilgi teknolojileri ile ilgili sağlanan her türlü hizmet, işlemde ve sunumunda kullanılan sistemlerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanmasına yönelik çalışmalar yürütüleceği; Siber güvenliğin sağlanması ve riskler ile mücadele için farkındalığın artırılarak konuya ilişkin eğitimler düzenlenerek bu eğitimlerin teknik bilgiler ile birlikte olayı bir bütün olarak görülmesini sağlayan hukuki,

idari, ekonomik, politik ve sosyal kısımları da içerek şekilde oluşturulmasının sağlanacağı önemle ifade edilmiştir (T.C. Ulaştırma ve Altyapı Bakanlığı, 2020b, s. 10-11).

Belirlenen bu politikaların ele alındığı 12. Ulaştırma ve Haberleşme Şurası, 6-7-8 Ekim 2021 tarihinde İstanbul'da yapılmış ve şura sonuç bildirgesi yayınlanmıştır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2021).

3. YARGI VE KURUL KARARLARI

3.1 Kişisel Verileri Koruma Kurulu Kararları

6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12. maddesine göre, yaşanan veri ihlallerinin veri sorumluları tarafından kişisel verileri koruma kuruluna iletilmesi gereklidir. Bazı hallerde, veri sorumluları tarafından kurula ihlal durumu bildirilmez. İlgili kişilerin kurula şikayet hakları bulunmaktadır. Kurul'un res'en yapacağı inceleme ya da ilgililerin şikayeti üzerine yapılan araştırma sonucunda, verilere yönelik ihlalin oluştuğunun anlaşılması durumunda Kurul, tespit ettiği yasal düzenlemelere ilişkin aykırılıkların veri sorumlusu tarafından giderilmesine karar verir. Her iki şekilde de Kurula iletilen ihlal ve şikayetlerin Kurul tarafından incelenmesi sonucu oluşan karar örnekleri veri güvenliği konusundaki risklere somut örneklerdir.

1- Veri sorumlusu sıfatını haiz olan Limited Şirket tarafından Kurula gönderilen veri ihlali bildiriminde özetle;

> Veri sorumlusunun bağlı olduğu Perakende Grubu ve Ulusal Şirketleri tarafından kullanılan sistemlerin bir siber saldırının hedefi olduğu, operasyonlarının bulunduğu ülkelerde fiziksel ve çevrimiçi mağazalardaki sunucular dâhil olmak üzere yaklaşık 3200 Windows sunucusunun söz konusu ihlalden etkilendiği, 08.11.2021 tarihinde tespit edilen veri ihlalinin, 08.11.2021 tarihinde başlayıp 10.11.2021 tarihinde sona erdiği,(...)

ifade edilmiştir. Kurul, veri ihlali bildiriminin Kurum'un internet sayfasında ilan edilmesine karar vermiştir (Kişisel Verileri Koruma Kurulu Kararı, 2021).

Örnek kararda veri ihlali, şirketin tüm bağlı gruplarını etkilemiştir. Fiziksel ve çevrimiçi mağazalarındaki sunucuları işlemez hale getirerek, iş akışları durmuş ve zarar meydana gelmiştir. Diğer taraftan, ihlalden etkilenen kişi grup ve sayılarının tespiti sonucunda, olaydan etkilenen veri sahiplerinin zararlarının tazminini talep etme hakları bulunmaktadır. Çünkü veri sorumlusu şirketin, kayıt altına aldığı verileri koruma

yükümlülüğü bulunmaktadır. Kanuni sorumluluğun yerine getirilmemesi halinde veri sorumlusu firmaya, idari para cezası verilebileceği gibi, cezai ve hukuki davalar açılması da söz konusudur. Diğer taraftan şirket üst yönetimi, zararın oluşmasında ihmali olanlar hakkında hukuki yollara başvurma hakkına sahiptir.

2- Veri sorumlusu sıfatını haiz olan Anonim Şirket tarafından Kurula iletilen bir başka veri ihlal bildiriminde özetle; "*Veri ihlalinin, yetkisiz erişen kişi/kişiler tarafından iletilen e-posta üzerine 27.02.2022 tarihinde tespit edildiği, İhlalden etkilenen ilgili kişi grupları ve kişi sayısının henüz belirlenemediği, İhlalden etkilenen kişisel veri kategorilerinin henüz belirlenemediği, bilgilerine yer verilmiştir."* İhlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir (Kişisel Verileri Koruma Kurulu Kararı, 2022).

Örnek kararda, ihlali yaşayan veri sorumlusu, bir Anonim şirkettir. Firma büyük ölçeklidir ve çok sayıda veri kaydı yapılmasına karşın, bilgi güvenliği önlemlerinin yeterli olmadığı anlaşılmaktadır. Şirket olaydan, siber saldırıda bulunan kişi/kişilerden gelen bir e-posta ile haberdar olmuştur. İhlalden etkilenen kişi sayısı ile kategoriler belirlenememiştir. İhlal olayı, firmanın piyasa itibarını zedeleyebilir ve müşteri güvenini yitirmesine yol açabilir. Ayrıca, veri ihlalinin sisteme izinsiz şekilde erişim sağlayan kişilerin e-postasından öğrenilmiş olması nedeniyle, siber saldırganların veri sorumlusundan fidye talebinde bulunma olasılığı da bulunmaktadır.

3- İlgili kişinin Kurula şikayetinde özetle;

> Bir e-ticaret firmasından satın aldığı ürünü tarafına teslim edecek **Kargo Firmasının** siparişi ilgili kişiye teslim etmesini müteakip ilgili kişi tarafından kargo paketinin üzerinde kendisi dışında isim benzerliği bulunan başka bir kişiye (üçüncü kişi) ait adres ve iletişim bilgilerinin yer aldığını gördüğü, veri sorumlusu kargo firmasına...başvuruda bulunarak sorulduğu..., veri sorumlusu tarafından ilgili kişiye gönderilmek üzere faturalandırılan gönderinin acente personeli tarafından toplu şekilde barkodlama işlemi yapılırken aynı isimli başka bir müşteriye ait gönderi ile isim benzerliği nedeniyle karıştırıldığının ve çapraz barkodlama hatası yapıldığı belirtilmiştir.

Şikayet üzerine Kurul tarafından verilen kararda,

> İlgili kişinin kişisel verilerinin üçüncü kişi ile paylaşılmasının yeni bir veri işleme faaliyeti olduğu, veri sorumlusunun anılan fiilinin kanunun 12'nci maddesine aykırı olduğu, ayrıca, bu durum bir veri ihlali olmasına karşın veri sorumlusunun kurula veri ihlal bildiriminde bulunmadığı(...)yükümlülüklerini yerine getirmeyen veri sorumlusu hakkında 75.000 tl idari para cezası verilmiştir (Kişisel Verileri Koruma Kurulu Kararı, 2023).

Örnek kararda, kargo firmasının çapraz barkodlama işlemi neticesinde oluşan durum, Kanun'un veri güvenliğinin sağlanmasına ilişkin 12.madde düzenlemelerine aykırıdır. Ayrıca veri ihlali gerçekleşmiş olduğu halde, bu durumun veri sorumlusu tarafından Kurula bildirilmemiş olması da, yükümlülük ihlali olarak değerlendirilerek Kurul tarafından firmaya idari para cezası verilmiştir.

4- Kurula intikal eden **Gıda Lojistik faaliyeti yapan** bir firmaya ilişkin veri ihlal bildiriminin incelenmesi sonucunda,

> (…)Veri sorumlusuna ait bir web uygulama sunucusu üzerindeki açık sebebiyle sunucuya erişildiği, İhlalden 21.504.083 kullanıcının etkilendiği,(...)ihlalin çok büyük çaplı olduğu, (...)Sisteme giren kişi ya da kişilerce, zararlı yazılım ve araçlarla sisteme giriş yaptıktan sonra diğer sistemlere de erişilerek bilgi toplandığı, sisteme zararlı yazılımların yüklenip, çalıştırılmasının veri sorumlusunca 8 gün boyunca fark edilemediği....bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi noktasında veri sorumlusunun kusurunun bulunduğu, 18.03.2021 tarihinden itibaren güvenlik yazılımlarında alarmlar oluştuğu, oluşan bu alarmların üçüncü parti firmalar tarafından izlenen ürünlerde....Güvenlik Ekiplerine ilgili bildirimler yapılamadan ve gerekli aksiyonlar alınmadan kapatıldığı, 25.03.2021 tarihinde iletilen alarmın.....Güvenlik Ekiplerince incelenmesi sonucu siber saldırının farkına varıldığı dikkate alındığında bu durumun veri sorumlusunun hizmet aldığı üçüncü parti firmalar üzerinde etkin bir denetim mekanizmasının bulunmadığının ve güvenlik yazılımlarının takibi ile güvenlik prosedürlerinin kullanılması noktasında da eksiklerinin bulunduğunun göstergesi olduğu,

> Saldırganların veri sorumlusundan elde ettikleri veriyi Fransa'da bulunan bir IP adresine/sunucuya ait lokasyona ilettiği, (…)firewall üzerinde izlerin olmasına rağmen bu boyutta verinin dışarı sızdırılmasının fark edilememesinin veri sorumlusu tarafından güvenlik kontrolleri ve veri güvenliği takibinin düzgün bir şekilde yapılmadığının göstergesi olduğu,(...)veri sorumlusu tarafından sızma testlerinin etkin bir şekilde yapılmadığını/yaptırılmadığını gösterdiği,(...)müdahalede geç kalmasının mevcut risk ve tehditleri iyi belirlemediğinin göstergesi olduğu hususları dikkate alındığında,....veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak 1.900.000 TL idari para cezası uygulanmasına karar verilmiştir" (Kişisel Verileri Koruma Kurulu Kararı, 2021).

Örnek kararda, ihlal olayı, gıda lojistiği hizmeti veren veri sorumlusu firmanın sistemlerindeki açık sebebi ile gerçekleşmiştir ve çok büyük çaplıdır. İhlal 8 gün boyunca fark edilememiştir. Güvenlik yazılımları alarm vermiş olduğu halde, hizmet alınan şirket tarafından bu alarmların dikkate alınmadığı görülmektedir. Bu halde, veri sorumlusu firmanın, hizmet aldığı üçüncü kişi şirket üzerinde etkin bir denetim mekanizmasının bulunmadığı söylenebilecektir. Verilerin, siber saldırganlar tarafından yurtdışına aktarılması durumu söz konusudur. Anonim şirket statüsündeki firma, çok sayıda veri kaydı yapmasına karşın, ihlali tespit edememiştir. Olayda, bilgi güvenliğiyle ilgili birçok teknik, idari ve hukuki eksikliğin bulunduğu görülmektedir. Şirket, bilgi güvenliği eksikliklerini, ihlal olayı yaşandıktan sonra fark etmiştir. Bu durum, şirketin etkin bir veri güvenliği sistemi ve denetim mekanizmasına sahip olmadığını veya mevcut mekanizmaların düzgün çalıştırılamadığını ortaya koymaktadır. Firmanın, üçüncü kişi şirketin (hizmet alınan şirket) verilerin korunması konusunda uygun ve yeterli tedbir düzeyini alıp almadığını kontrol noktasında üzerine düşen denetim görevini yapmadığı anlaşılmaktadır.

5- Veri sorumlusunun Kurula intikal eden veri ihlal bildiriminde;

> *İhlalin, bazı müşterilerin yeni bir hesap açarken kişisel verilerinin yanlışlıkla bir URL üzerinden veri sorumlusunun iç sistemlerine ve çalıştığı bazı üçüncü taraf satıcı/sağlayıcılara aktarılması şeklinde gerçekleştiği (...) veri ihlallerinin*

tespitinin yaklaşık bir yıl sonra yapılmış olmasının, gerçekleştirilen işlemlere dair Şirketin log kaydı/takip alarm sistemlerinin bulunmadığının ya da etkin bir şekilde kullanılmadığının ve Şirket tarafından gerekli kontrollerin yapılmadığının göstergesi olduğu," tespit edilerek firmaya idari para cezası uygulanmasına karar verilmiştir (Kişisel Verileri Koruma Kurulu Kararı, 2020).

Örnek karar, bilgi güvenliğinin sağlanmasında teknik ve idari anlamda ciddi eksiklikler bulunduğunu ortaya koymaktadır. Firma bir yıl süresince veri ihlaline maruz kaldığı halde durumdan haberdar olmamıştır. Sistemlerinde teknik eksiklikler olduğu ve bir denetim mekanizmasının bulunmadığı anlaşılmaktadır.

6- Veri sorumlusunun Kurula intikal eden veri ihlal bildiriminde;

Veri işleyenin kişisel verileri muhafaza ettiği dijital ortamlara yönelik ihlalden önce gerçekleştirilmiş bir sızma testi raporu bulunmadığı; buna paralel olarak veri sorumlusunun veri işleyen bünyesinde ihlalin gerçekleşmesine sebep olabilecek teknik zafiyetlerin neler olduğuna ilişkin bilgi sahibi olamadığı; dolayısıyla veri işleyenin kişisel verilerin korunması hususunda uygun güvenlik düzeyini temin etmesini garanti altına almak noktasında üzerine düşen denetim tedbirini almadığı;

Ayrıca veri sorumlusunun, veri işleyenin muhafaza ettiği kişisel verilerin imhasına yönelik olarak aralarındaki ticari ilişkinin sonlanmasını müteakip gerekli girişimlerde bulunması gerekirken bunu ihlalden sonra yaptığı;

Bu itibarla Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendinde yer alan "kişisel verilerin hukuka aykırı olarak işlenmesini önlemek" amacıyla gerekli tedbirleri almaktan imtina ettiği; anılan gerekçelerle veri sorumlusunun veri işleyen ile ilişkilerin yönetimi noktasında özensiz davrandığı, değerlendirmelerinden hareketle, Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 450.000 TL idari para cezası uygulanmasına, karar verilmiştir (Kişisel Verileri Koruma Kurulu Kararı, 2021).

Örnek kararda veri sorumlusu firma, hizmet aldığı veri işleyenin, bilgi güvenliği konusunda uygun ve yeterli tedbir düzeyini temin etmesini garantiye almak üzere, üzerine düşen denetim görevini yerine getirmemiştir, görevini ihmal etmiştir. Firmanın sadece kendi bilgi güvenliğini sağlamış olması yeterli değildir. Özellikle lojistik sektörü gibi çok sayıda paydaş ve veri paylaşımı yapılan bir alanda, tedarik zinciri içerisindeki üçüncü kişi firmaların bilgi güvenliklerini sağlamış olması önemlidir. Diğer taraftan Kanunun 12'nci maddesinin (2) numaralı fıkra *"Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur."* hükmü çerçevesinde *"*veri sorumlusunun veri güvenliğine yönelik yükümlülüklerinin ortadan kalkmadığı" şeklindeki düzenlemesi gereğince, veri sorumlusu şirket, kişisel verilerin korunması ile ilgili önlemlerin alınmasında bu kişilerle birlikte sorumlu olacaktır, yükümlülükleri ortadan kalkmamaktadır.

Ayrıca kararda hizmet alınan firma (veri işleyen) ile ticari iş ilişki sonlandırıldığında işlenen verilerle ilgili veri imha prosedürleri uygulanmamıştır. Veri sorumlusu firmanın bu tedbirsizliği işlenen veriler bakımından risk oluşturmaktadır.

7- Veri sorumlusunun Kurula intikal eden veri ihlal bildiriminde;

> Bir şirket tarafından sunulan mobil uygulamanın dünya genelinde yaklaşık 162 milyon civarındaki kullanıcı hesabına ait bilgilerinin(…)web'te satıldığı, veri ihlalinin nasıl gerçekleştiğinin bilinmediği, veri ihlalinden bir gazeteci vasıtasıyla haberdar olunmasının şirketin teknik ve idari tedbirler bakımından kusurlu olduğunu gösterdiği, büyük çaptaki bu veri ihlaline rağmen şirketin kullanıcılarını bu konuda bilgilendirmediği hususları dikkate alınarak, Kanunun 12 nci maddesinin (1) numaralı fıkrasında yer alan veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı sebebiyle şirket hakkında 680.000 TL, veri ihlalinin şirket tarafından Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer alan "en kısa sürede bildirim" yükümlülüğüne aykırılık teşkil eden uygulaması nedeniyle Şirket hakkında 50.000 TL olmak üzere toplam 730.000 TL idari para cezası uygulanmasına, ihlalden, halka açık profilinde ilişkili ülke olarak Türkiye'yi tanımlayan 679.269 kişinin etkilendiği

dikkate alındığında, Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası gereğince, söz konusu ihlalin Kurumun internet sitesinde ilan edilmesine, karar verilmiştir (Kişisel Verileri Koruma Kurulu Kararı, 2019).

8- Veri sorumlusu Anonim Şirketin Kurula iletilen veri ihlal bildiriminde;

> Veri sorumlusunun anlaşmalı olduğu bayi ve yetkili servis çalışanlarının satış hedefleri kapsamında ek menfaat niteliğinde ödül kazandıkları, …..mobil uygulama ve internet sitesinin barındırıldığı tedarikçi sistemlerinde tespit edilen bir güvenlik zafiyeti dolayısıyla kişisel verilere yetkisiz erişim sağlandığı,…Almanya'da görünen bir IP adresine kişisel verilerin alındığının tespit edildiği, ihlalden etkilenen ilgili kişi sayısının tahmini 30.373 kişi olduğu

belirtilerek incelemenin devam ettiği, söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir (Kişisel Verileri Koruma Kurulu Kararı, 2023).

Örnek olayda, ihlalden etkilenen kişi sayısı oldukça fazladır ve veriler yurtdışına aktarılmıştır. İhlal sebebi olarak, tedarikçi sistemlerinde tespit edilen güvenlik zaafiyeti gösterilmiştir. Bu olay, şirket bilgi güvenliğinin sağlanmasının yanı sıra, veri paylaşımında bulunulan tedarikçiler bakımından da bilgi güvenliğini sağlanmanın önemini ortaya koymaktadır.

9- Veri sorumlusu Kargo Taşımacılığı A.Ş. tarafından Kurula iletilen veri ihlal bildiriminde;

> İhlalin, hizmet aldıkları şirketin sunucularına yapılan siber saldırı sonucu depolama aygıtlarında bulunan verilerin şifrelenmek suretiyle erişilemez duruma gelmesiyle gerçekleştiği, ihlalden müşteri verilerinin etkilendiği, ihlalin 25.07.2023 tarihinde meydana geldiği ve 04.08.2023 tarihinde tespit edildiği belirtilerek, incelemenin devam ettiği ve ihlal bildiriminin kurumun sitesinde yayınlanmasına, karar verilmiştir (Kişisel Verileri Koruma Kurulu Kararı, 2023).

Örnek kararda bir kargo şirketi, hizmet aldığı üçüncü kişi firmanın sunucularına yapılan siber saldırı sebebiyle verilere ulaşamamıştır. Olay uzun bir süre tespit edilemediği gibi, kargo firmasının müşteri verileri zarar görmüştür. Kargo firmaları çok sayıda müşterinin işlem yaptığı ve hizmetin sürekliliği için bilgi akışının son derece önemli olduğu bir iş alanıdır. Büyük ölçekli (Anonim şirket) bir şirket olan olan kargo firması hizmet aldığı üçüncü kişi firmanın güvenlik açığı sebebi ile müşterilerini mağdur etmiştir. Üçüncü kişi şirket nezdinde yapılması gereken kontrol yükümlülüğünü yerine getirmemiş, denetim tedbirini almamıştır.

10- Veri sorumlusu Limited Şirket tarafından Kurula iletilen veri ihlal bildiriminde özetle;

> Bir siber saldırı sonucunda ihlalin gerçekleştiği ve veri sorumlusundan fidye talep edildiği, ihlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim, lokasyon, özlük, hukuki işlem, müşteri işlem, fiziksel mekân güvenliği, işlem güvenliği, risk yönetimi, finans, mesleki deneyim, pazarlama, görsel ve işitsel kayıtlar olduğu, ihlalden etkilenen özel nitelikli kişisel veri kategorilerinin; kılık ve kıyafet, sağlık bilgileri, biyometrik veri, ceza mahkûmiyeti ve güvenlik tedbirleri olduğu, incelemenin devam ettiği

belirtilerek veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir (Kişisel Verileri Koruma Kurulu Kararı, 2024).

Örnek olayda, siber saldırganlar tarafından, veri sorumlusundan, fidye talep edildiği görülmektedir. Kurulun önceki kararlarında fidye talebine ilişkin bir bilgi bulunmamaktadır. O sebeple örnek olay, veri sorumlularından fidye talebinde bulunulmaya başlandığını göstermesi bakımından önemlidir.

Kişisel Verileri Koruma Kurulu, gelen ihlal başvurularının nedenlerini ve oluşum biçimlerini ayrıntılı bir şekilde inceleyerek araştırmaktadır. Veri sorumlularının denetim görevlerini yerine getirip getirmedikleri, bilgi güvenliği eğitimlerinin verilmiş olup olmadığı ve güvenlik önlemlerinin olayın oluşumundaki etkileri gibi detaylı bir şekilde incelenmektedir. Kararlar genel olarak göstermektedir ki, her ölçekten firma veri ihlali tehlikesi ile karşı karşıyadır. Bilgi güvenliğine önem vermeyen, önlem almayan ve gerekli

kontrolleri yapmayan şirketler, veri ihlallerini fark edememektedir. İhlalin boyutu kimi kez grup şirketlerin tümünü etkileyebilecek büyüklüktedir.

3.2 Yargıtay Kararları

Araştırma kapsamında, hukuk içtihatlarının yer aldığı Lexpera, Legalbank, HukukTürk, Yargıtay kararları gibi hukuk siteleri tarandığında, bilişim sistemine izinsiz girme, kişisel veri ihlali, ticari sır ifşası, sır saklama yükümlülüğünü ihlal, hizmet nedeniyle güveni kötüye kullanma, kişilik hakkına saldırıya ilişkin olarak Yargıtay Ceza Daireleri ve Yargıtay Hukuk Daireleri tarafından verilmiş örnek kararlara ulaşılmıştır.

> **1- Lojistik** ve insan kaynaklan müdürü olarak çalıştığı şirkette yapılan denetim neticesinde; davacının üretim alanında şirket personeli olmayan ... şahısları bulundurduğu, bu şahısların şirketin en önemli üretim sahalarında çalışarak şirketin gizli bilgilerini ve ticari sırlarını öğrendikleri, davacının başka şirketler/şirketlerin işleri ile uğraşılarak sözleşmesine aykırı olarak rekabet yasağını ihlal ettiği, Şirketin gizli bilgilerini ve/veya ticari sırlarını iş akdine aykırı olarak ifşa ettiği tespitlerine dayanılarak iş akdinin feshedildiği anlaşılmıştır (Yargıtay 9. HD., 2016).

> **2-** Sanığın, dış ticaret elemanı olarak çalıştığı ve katılanların yetkilisi olduğu şirketin her türlü üretim bilgisine vakıf olması nedeniyle bu durumu kendi menfaatine kullanarak şirkete ait bilgileri, rakip firmalara ve 3. kişilere verdiği, çeşitli yazışmalar yaparak başka firmaların ürünlerinin pazarlamasını yaptığı ve bunların karşılığında komisyon aldığı, bu suretle hizmet nedeniyle güveni kötüye kullanma ve ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi ve belgelerin açıklanması suçlarını işlediği(…) (Yargıtay 15.CD., 2019).

Örnek birinci kararda, şirket personeli olmayan şahısların şirketin üretim alanına girmesine izin verilmiştir. Karardan anlaşıldığı üzere bu duruma izin veren, firmanın insan kaynakları-lojistik müdürüdür. Karar, bilgi güvenliği açısından değerlendirildiğinde, şirket yetkili personeli dışındaki kişilerin, firmanın iş sırlarının muhafaza edildiği bir ortamda bulunmasına izin verilmesi büyük bir güvenlik açığı olarak değerlendirilebilir. Şirket verilerinin saklandığı ortamlar için güvenlik önlemi alınması,

yönetici ve diğer çalışan kriterlerinin belirlenmesi, yetkilendirme, sorumluluk ve denetleme kurallarının yazılı olarak hazırlanarak şirket içinde duyurulması ve giriş çıkışların kontrol edilmesi gerekmektedir. Uygulamalar belli aralıklarla denetlenmeli ve tespit edilen eksiklikler düzeltilerek güncellenmelidir. Yetkisiz kişilerin üretim alanında bulunmasına izin veren yönetici personel, şirket için ayrı bir risk oluşturmaktadır. Kritik görevlerde bulunan personel için çalışma ve denetleme kriterlerinin, şirketin çalışma prensiplerine uygun olarak açık ve net bir şekilde belirlenmesi ve iş sözleşmelerine eklenmesi, riski azaltıcı çözümler olarak değerlendirilebilir. Aynı personel, eylemleri sebebi ile sözleşmesine aykırı olarak rekabet yasağını ihlal etmiştir. Çalıştığı şirketin gizli bilgilerini ve/veya ticari sırlarını iş akdine aykırı olarak ifşa etmesi sebebiyle de iş akdi sona erdirilmiştir. Örnek ikinci kararda işçi, iş gereği öğrendiği şirkete ait bilgileri kötü niyetle kullanmaktadır. Borçlar Kanunu 396. madde de düzenlenen işçinin özen ve sadakat borcuna aykırılık durumu söz konusudur. Bu durumda riski azaltmak için, çerçevesi net olarak belirlenmiş bir gizlilik sözleşmesi düzenlenmesi mümkündür.

> **3-** Suç tarihinde(...),mühendis olarak çalışmakta olan sanığın, şirketin ana bilgisayarına güvenlik sistemini devre dışı bırakıp uzaktan girerek kendi bilgisayarına veri transferi yaptığı ve 2490 adet dosyayı şifreleyerek ZIP formatında harici belleğe kopyalayıp yeni işe başladığı firmanın ana bilgisayarına aktardığı iddia edilen olayda(...)mevcut kayıtların teknik bilgi ve tecrübeyi gerektiren konulara ilişkin olduğu nazara alınarak; kopyalanan kayıtlarda yer alan bilgilerin ticari sır veya müşteri sırrı niteliğinde olup olmadığı hususlarında konusunda uzman bilirkişilerden rapor alınması(...) (Yargıtay 5.CD., 2017).

Örnek kararda, şirketin teknik personeli mühendis, şirket ana bilgisayarının güvenlik sistemini devre dışı bırakarak sisteme uzaktan girebilmektedir. Sistemin devre dışı bırakılarak müdahale edilebiliyor olması hali, şirketin teknik önlemlerinin yetersizliğini, güvenlik açıkları olduğunu göstermesi bakımından önemlidir. Bilgi güvenliği çok yönlüdür, teknik, idari ve hukuki önlemlerin bir bütün olarak alınması gerekir. Teknik önlem almış olmak tek başına yeterli olmasa da oldukça önemlidir. Örnek olay değerlendirildiğinde, şirket ana bilgisayarına girişlerde birden fazla kişinin birlikte hareketi ve şifre paylaşımı şeklinde (her bir yetkiliye giriş şifresinin bir bölümünün

verilmesi) önlem alınması mümkündür. Böylece ana bilgisayara girişler, birden fazla kişinin birlikte hareketi ile sağlanabilecek ve bireysel hareket imkanı ortadan kaldırılmış olacaktır. Ayrıca şirket ana bilgisayarı gibi kritik bölgelere müdahaleyi önlemek üzere sistem izleme ekibi kurulması da değerlendirilebilir. Böylece sisteme olumsuz müdahale halinde izleme ekibine gönderilecek alarm ile ekibin müdahaleden haberdar olması sağlanabilecektir. Alınabilecek teknik önlem örnekleri çoğaltılabilecektir.

Çalışanların, şirket ticari sırlarını üçüncü kişilere iletmesi ya da önemli verilerin yer aldığı şirkete ait bilgi ve belgeleri işten ayrılmaları ile birlikte beraberlerinde götürmeleri mümkündür. Bu türden olaylar sık yaşanmaktadır. Örneğin, General Motors Şirketi'nin değeri milyonlarca dolarla ölçülen planları kapsayan çok sayıda verisi 2010 senesinde, çalışanları tarafından kopyalanarak başka bir otomobil üreticisi ile paylaşılmıştır (Yüksel, 2018).

> **4-** Dosyadaki bilgi ve belgelerden 01.07.2016 günü istifa dilekçesi veren davalının bundan bir gün önce 30.06.2016 gününde stratejik plan başlıklı dökümanları kendi kişisel elektronik posta adresine gönderdiği, davacının bu dökümanların işyerine ait sırları ihtiva ettiğini ileri sürdüğü, davalının imzasını taşıyan bilgi koruma taahhütnamesinde işyerine ait dökümanların amir onayı olmadan herhangi bir yolla işyeri dışına çıkarılması, paylaşılıp depolanmasının yasaklandığı, aksi davranışın ise taahhütnamenin 9. maddesinde cezai şarta bağlandığı anlaşılmaktadır(…)İstifa etmeden bir gün önce çeşitli dökümanları kişisel hesabına gönderen işçinin en baştan uymayı taahhüt ettiği bilgi koruma kurallarına aykırı hareket ettiği ortadadır.Şu halde davalının 30.06.2016 günü kişisel elektronik postasına gönderdiği bütün dökümanlar üzerinde bilirkişi incelemesi yaptırılarak sır saklama yükümlülüğü kapsamında işyerine ait çeşitli özel bilgiler ihtiva edip etmediği araştırılıp(…) (Yargıtay 9.HD., 2021).

Örnek kararda işçinin, istifa dilekçesinden bir gün önce işyerine ait stratejik planları (işyeri sırları) şahsi elektronik posta adresine (şirket dışına) göndermesi durumu söz konusudur. Karar içeriğine göre şirket, bilgi güvenliğini sağlamak üzere idari ve hukuki önlemlerini almıştır. İşyerine ait dökümanların amir onayı olmaksızın işyeri dışına çıkarılmasını yasaklayan bilgi koruma taahhütnamesi çalışanlara imzalatılmıştır. İşçi ise

taahhütnameyi imzalamasına karşın kötüniyetli davranışta bulunmuştur. İşverenin öngörü sahibi bir iş insanı olarak verileri korumak üzere aldığı önlem, imzalı taahhütname, kendisi lehine mahkemede delil olarak kullanılmış ve mahkemece işçinin, taahhütnameye aykırı hareket ettiği kabul edilmiştir. Veri sorumluları tarafından alınan bilgi güvenliği önlemleri ihtilaf halinde mahkemede delil olarak kullanılabilmektedir. Diğer taraftan mahkeme, işçi tarafından izinsiz olarak alınan belgelerin ticari sır kapsamında olup olmadığının araştırılması için dosyanın bilirkişi incelemesine gönderilmesine karar vermiştir. Bu aşamada, firmanın veri envanterinin varlığı, verilerin çeşitlilik, risk ve önemine göre (kişisel veri, ticari veri, ticari sır vb) sınıflandırılarak hazırlanmış olması önem taşımaktadır. Mahkemenin yaptırdığı bilirkişi incelemesinde tüm bu hususlar birlikte değerlendirilecektir.

> **5-** (…)Maddi gerçeğin hiçbir kuşkuya yer bırakmayacak şekilde ortaya çıkarılması açısından, sanığın sıfat ve görevi gereği katılan şirkette ticari sır kapsamındaki ne tür bilgilere sahip olduğu,(…)keza mahkemece aldırılan bilirkişi raporunda katılan şirkete ait hangi nitelikteki bilgilerin ticari sır kapsamında değerlendirildiğinin somut verilerle gösterilmediği ve hangi bilgilerin paylaşıldığı hususunda da bir açıklık bulunmadığı nazara alınarak, konusunda uzman 3 kişilik bilirkişi heyetinden bu konularda tekrar rapor alınması ve 5237 Sayılı TCK'nın 239. maddesinde düzenlenen ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması suçunun oluşabilmesi için "yetkisiz kişilere verme" ya da "ifşa etme" şeklindeki seçimlik hareketlerden birinin gerçekleştirilmesi gerektiği de gözetilerek(…)" (Yargıtay 5. CD, 2019)**.**

> **6-** (…)San. ve Tic. A.Ş. bünyesinde pazarlama şefi olarak çalışmakta olan sanığın, görevi gereği vakıf olduğu bilgileri rakip firma görevlisine elektronik posta ile göndermek suretiyle ticari sır niteliğindeki bilgileri açıklama suçunu işlediği;(…) ilgili şirketten sanığın suç tarihindeki görevinin ne olduğu, gönderilen bilgilerin piyasaya bildirilmesi hususunda amirlerin talimatının bulunup bulunmadığı hususlarının sorulması, elektronik posta içeriklerinde yer alan bilgilerin ticari sır niteliğinde olup olmadığı hususlarında ticaret hukuku alanında uzman bilirkişiden rapor alınması(…)." (Yargıtay 5. CD, 2015).

İki örnek karar arasında ortak nokta, dava konusu belgelerin ticari sır niteliğine sahip olup olmadığının mahkeme tarafından araştırılmasıdır. Diğer taraftan, sanıkların suç tarihindeki görevleri ve bu görevlerinden kaynaklı olarak şirkette ticari sır kapsamında edindikleri bilgiler incelenmektedir. Bilgi güvenliğinin etkin bir şekilde sağlanabilmesi için, verilere erişim hakkına sahip personelin belirlenmesi ve bu kişilere hangi bilgilere erişim yetkisi tanınacağı konusunun kapsamlı bir şekilde düzenlenmesi gereklidir. Mahkeme, veri ihlali yapan personelin verilere erişim yetkisini ve diğer sorumluluklarını incelemektedir. Ayrıca sanık tarafından ifşa edilen bilgilerin, piyasaya açıklanmasına ilişkin olarak amir talimatının bulunup bulunmadığı da mahkeme tarafından araştırılmaktadır. Firmanın bilgi güvenliğini sağlama sorumluluğunu yerine getirmek amacıyla oluşturacağı teknik, idari ve hukuki düzenlemeler, veri ihlali durumunda mahkemeye delil olarak sunulabilecektir.

Firmaların kendileri için önemli olan ticari bilgi vasfı taşıyan dosyalara "gizlidir" ve "ticari bilgiler içerir" şeklinde isimler koyması, çalışan ya da başka üçüncü şahısların bu dosyaları izinsiz elde etmesine engel oluşturmayabilir. Ancak işletmenin bu şekilde davranması, mahkeme aşamasında, personelin bu türden dosyaların gizliliği konusunda ikaz edildiği firmanın buna gayret göstermiş olduğunun kanıtı olarak kullanılabilecektir. Bu sebeple işletmelerin önemli ve ticari bilgi ve belgelerini çalışanları bakımından belirgin duruma getirmiş olması önemlidir (Yüksel, 2018).

> **7-** (...)Sanayii Anonim Şirketinde kalıplı üretim elemanı olarak çalışan sanığın işten çıkarılması üzerine şirkete ait, ticari işletmenin işleyişine ilişkin özel belgeler olan ve ticari sır niteliğindeki hammadde izleme kartları ile makine silo takip formlarını …Bulaşık Makinası İşletmesine götürerek yetkilisi(…)'a verdiği iddiasıyla sanık hakkında ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması suçundan kamu davası açıldığı ve mahkemece atılı suçtan sanığın mahkumiyetine karar verildiği anlaşılmıştır(…) (Yargıtay 5.CD, 2023).

Örnek kararda, işten çıkarılan bir personelin işyerine ait bilgileri üçüncü kişi firmalar ile paylaşımı söz konusudur. Bilgi güvenliği için, işten çıkarılan personel ile ilgili olarak alınacak bazı hukuki ve idari önlemler bulunmaktadır. Personelin şirket ile ilişkisinin

tamamen sonlandırılması, tüm bilgisayar girişlerinin iptal edilmesi, sahip olduğu bilgi ve belgelerin teslimi ile yetkilerinin sona erdirilmesi gerekmektedir. Karar içeriğinden anlaşılmamakla birlikte, işçinin söz konusu belgeleri, iş akdinin feshinden önce şirket dışına çıkarmış olma ihtimali de bulunmaktadır. Bu durumda da, şirketin bilgi güvenliği zaafiyetinden söz etmek mümkündür. Örnek kararlar, veri ihlallerinin çoğunlukla şirket içi kaynaklı olduğunu göstermesi bakımından önemlidir.

> **8-** Sanıkların suç tarihinden önce katılan şirketin ortakları olduğu, şirketin müdürü ve yazılım müdürü oldukları, şirketin bünyesinde bulunan programları.. şirket IP'sine uzaktan erişimle dışarıdan bağlanarak sildikleri ve program kodlar, database, yapılan geliştirme ve güncellemeleri (...) no'lu IP adresteki bilgisayara aktardıkları, (...)sanıkların haksız olarak ele geçirdikleri bu programları Intıme ... isimli kendi kurdukları şirketin ticari faaliyetlerinde kullanmak suretiyle haksız rekabet, hizmet nedeniyle güveni kötüye kullanma ile bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçlarını işledikleri iddia olunan somut olayda(...) (Yargıtay 15.CD, 2020).

Örnek karar, haksız rekabeti de kapsayan bilişim sistemini engelleme ve bozma suçuna ilişkindir ve suç şirketin eski ortakları tarafından işlenmiştir. Sanıklar eski çalıştıkları şirketin IP'sine uzaktan bağlanarak programları da silmiştir. Suç tarihinde sanıkların şirket ortağı olmadığı anlaşılmaktadır. Ana şirketin, bilgisayar sistemlerine dışarıdan müdahaleye karşı, dosyalarına izinsiz erişime ilişkin bir güvenlik tedbirinin bulunmadığı teknik önlemlerinin olmadığı görülmektedir. Firmanın, teknik önlemler yanında şirket ile olan iş ilişkisi sona eren kişilere karşı uygulanacak idari ve hukuki tedbirlere de sahip olması gerekir. Bu haliyle şirket risklere açık haldedir, güvenlik zaafiyetleri bulunmaktadır.

> **9-** Dava, kişilik haklarına saldırıya dayalı manevi tazminat ve ihtiyati tedbir istemlerine ilişkin olup,(…) Davacı, davalı B. Ç.'in "www.muhalifgazete.com" isimli internet sitesinde "(…)şirketinde sular durulmuyor" başlığı ile kaleme aldığı yazı ile kişilik haklarına saldırıldığını belirterek uğradığı manevi zararının davalılar tarafından tazminini ve hukuka aykırı yayının kaldırılması,

durdurulması ve önlenmesi yönünde ihtiyati tedbir kararı verilmesini talep etmiştir(…) (Yargıtay 4.HD, 2013).

Örnek karar, yapılan haber nedeniyle, tüzel kişiliğin kişilik haklarına saldırının önlenmesi ve korunmasına ilişkindir.

Hukukumuzda, tüzel kişiler yönünden de özel hayata saygı hakkının kabulü gerekir. Tüzel kişilerin gerçek kişiler gibi incinecek duyguları olmamakla birlikte itibarları zarar görebilecektir. Ayrıca acı çekmeleri, üzüntü duymaları imkansız olmakla birlikte tüzel kişiliğe karşı duyulan güven azalabileceğinden özel hayata saygı hakkı kabul edilmelidir (Küpeli, 2019).

10- "Türk Ceza Kanunu'nun 132/2; kişinin kendisiyle yapılan haberleşme içeriğini, belirli olmayan ve birden fazla kişi tarafından algılanabilme imkanı bulunan aleni bir ortamda, ilgilisi veya ilgililerinin rızası dışında ifşa etmesi eyleminin aynı Kanunun 132/3. maddelerinde düzenlenen haberleşmenin gizliliğini ihlal suçu kapsamında değerlendirileceği,(…)Bu açıklamalar ışığında incelenen dosya kapsamına göre; sanık'ın ortağı ve müdürü olduğu firmaya bağlı olarak yayın yapan haber içerikli bir internet sitesinde köşe yazarı olarak çalışan katılanın firma tarafından tahsis edilen elektronik posta hesabına, (…).adlı kişinin gönderdiği bir elektronik iletisinin, işten ayrılmasını müteakip, anılan sitede başkalarının bilgi ve görgüsüne sunulduğu iddiasına konu olayda,(…)Sanıkların eylemlerinin, kanıtlanması halinde, TCK'nın 132/2-4. maddesinde tanımlanan haberleşmenin gizliliğini ihlal suçunu oluşturabileceği" (Yargıtay 12. CD, 2014).

11- Sanığın, tarafı olduğu haberleşme içeriklerini, belirli olmayan ve birden fazla kişi tarafından algılanabilme imkanı bulunan aleni bir ortamda ifşa etmemesinden dolayı TCK'nın 132. maddesinin 3. fıkrasında tanımlanan haberleşmenin gizliliğini ihlal suçunun yasal unsurlarının somut olayda gerçekleşmemesi nedeniyle sanıkla aralarındaki ilişkinin varlığını ve boyutunu kendisinde saklı tutan katılanın özel yaşam alanı kapsamındaki konuşmalarını içeren ses kaydını katılanın tanıdığına gönderen sanığın eyleminin TCK'nın 134. maddesinin 2. fıkrasındaki görüntü veya seslerin ifşa edilmesi suretiyle özel

hayatın gizliliğini ihlal suçunu oluşturacağı gözetilmeden, suç vasfında yanılgıya düşülerek, mahkumiyet hükmü kurulması (Yargıtay 12. CD, 2018).

Özel hayata ve hayatın gizli alanına karşı işlenen suçlara ilişkin örnek yargıtay kararları, gerçek kişiler açısından önemlidir. Tüzel kişiler, gerçek kişi verilerini de kaydetmektedir.

3.3 Adli Karar İstatistikleri

Adalet Bakanlığı bünyesinde kurulan Adli Sicil ve İstatistik Genel Müdürlüğü, adli suçlara ilişkin davalar ve kararlara ilişkin istatistikleri tutmaktadır. Konuya ilişkin verileri toplayarak her yıl istatistik raporlarını yayınlamaktadır (Karaca, 2019).

Yargıya intikal etmiş olan bilişim alanındaki suçlar (TCK m.243-246) ve kişisel verilerin hukuka aykırı şekilde ele geçirilmesi, kaydedilmesi suçlarının da içinde bulunduğu, Özel hayata ve hayatın gizli alanına karşı suçlar (TCK m.132-140) ve Ekonomi, sanayi ve ticarete ilişkin suçlarda (TCK m.239) verilen kamu davası açılması, takipsizlik kararı veya diğer kararlara ilişkin Adli İstatistik verilerinin son 7 yıllık istatistik sonuçlarına Tablo 20, Tablo 21 ve Tablo 22'de yer verilmiştir.

Tablo 20. TCK 'ya Göre Bilişim Suçları ile İlgili Olarak Şüpheli Kişiler Hakkında Verilen Kararlar (Adli Sicil ve İstatistik Genel Müdürlüğü, 2017-2023)

Yıl	Suç Türü	Kamu Davası Açılan	Kovuşturmaya Yer Olmadığı	Diğer Kararlar	Toplam
2017	Bilişim Suçları 243-246	20.631	36.538	42.378	99.547
2018	Bilişim Suçları 243-246	23.197	41.414	41.534	106.145
2019	Bilişim Suçları 243-246	26.093	37.989	36.375	100.457
2020	Bilişim Suçları 243-246	**17.790**	38.659	28.455	**84.904**
2021	Bilişim Suçları 243-246	**19.947**	71.131	32.167	**123.245**
2022	Bilişim Suçları 243-246	12.526	70.574	14.001	97.101
2023	Bilişim Suçları 243-246	12.306	47.772	10.776	70.854

Tablo 21. TCK 'ya Göre Özel Hayatın Gizliliğine Karşı Suçlar ile İlgili Olarak Şüpheli Kişiler Hakkında Verilen Kararlar (Adli Sicil ve İstatistik Genel Müdürlüğü, 2017-2023)

Yıl	Suç Türü	Kamu Davası Açılan	Kovuşturmaya Yer Olmadığı	Diğer Kararlar	Toplam
2017	Özel Hayata Karşı Suçlar 132-140	8.823	20.743	5.006	34.572
2018	Özel Hayata Karşı Suçlar 132-140	10.841	27.050	6.700	44.591
2019	Özel Hayata Karşı Suçlar 132-140	15.502	36.249	7.884	59.635
2020	Özel Hayata Karşı Suçlar 132-140	**14.311**	37.112	8.594	**60.017**
2021	Özel Hayata Karşı Suçlar 132-140	**19.367**	55.786	12.471	**87.624**
2022	Özel Hayata Karşı Suçlar 132-140	16.214	50.971	11.203	**78.388**
2023	Özel Hayata Karşı Suçlar 132-140	17.569	57.504	13.204	**88.277**

Tablo 20 bulguları, son yıllarda özellikle pandemi ile birlikte bilişim alanındaki suçlar bakımından yargıya intikallerde artış yaşandığını, dosyalardan bazıları için kovuşturmaya yer olmadığı kararı verilmiş ise de, kamu davası açılan dosya sayılarında artış olduğunu göstermektedir. Bazı hallerde de şirketler veri ihlallerini çeşitli sebeplerle mahkemeye getirmeden şirket içinde çözmeyi tercih etmektedir.

Tablo 21 bulgularında da benzer bir durum söz konusudur. 2022 yılı itibari ile özel hayatın gizliliğine karşı suçlar bakımından yargıya intikal ile karar verilen dosya sayısı (toplam 78.388), bir önceki yıla kıyasla azalmış gibi görünüyor olsa da, 2023 yılı verilerine bakıldığında, karar dosya sayısı toplamının (toplam 88.277) önceki yıllara göre artış gösterdiği görülmektedir. Özellikle pandemi ile birlikte bu suçlar bakımından da yargıya intikallerde artış yaşandığını (2020-2021 yılları arası), dosyalardan bazıları için kovuşturmaya yer olmadığı kararı verilmiş ise de, kamu davası açılan dosya sayılarında artış olduğu görülmektedir. Yayınlanmış olan son adalet istatistik verisi 2023 tarihlidir.

Tablo 22. TCK 'ya Göre Ekonomi, Sanayi ve Ticarete İlişkin Suçlardan 239. Madde İle İlgili Olarak Şüpheli Kişiler Hakkında Verilen Kararlar (Adli Sicil ve İstatistik Genel Müdürlüğü, 2017-2021)

Yıl	Suç Türü	Kamu Davası Açılan	Kovuşturmaya Yer Olmadığı	Diğer Kararlar	Toplam
2017	Ekonomi, Sanayi Ve Ticarete Ilişkin Suçlar (239. madde)	71	189	96	356
2018	Ekonomi, Sanayi Ve Ticarete Ilişkin Suçlar (239. madde)	86	267	155	508
2019	Ekonomi, Sanayi Ve Ticarete Ilişkin Suçlar (239. madde)	**77**	345	98	**520**
2020	Ekonomi, Sanayi Ve Ticarete Ilişkin Suçlar (239. madde)	**90**	343	86	**519**
2021	Ekonomi, Sanayi Ve Ticarete Ilişkin Suçlar (239. madde)	**130**	460	167	**757**

Tablo 22 Ekonomi, sanayi ve ticarete ilişkin suçlar (235-242) başlığı altında yer alan 239. madde, Ticari sırrın açıklanmasına ilişkindir. Tablo verileri, 2017-2021 yılları arasında 239. madde ile ilgili savcılığa intikal eden dosya ve verilen kararları göstermektedir. 2022 ve 2023 yıllarına ait istatistik verileri, 235-242. maddelere ilişkin toplu sonuçlar olarak sunulmuş olup, yalnızca 239. maddeye özel olarak bir veri verilmediğinden bu yıllar için 239. madde sonuçlarına tabloda yer verilememiştir.

Tablo verileri incelendiğinde, Ticari, müşteri ve bankacılık sırrın ifşasına ilişkin suç bakımından toplam karar dosya sayılarında artış yaşandığı görülmektedir. Aynı şekilde kamu davası açılma oranı da yıllar içinde artış göstermiştir. 2019' da 239. madde kapsamında kamu davası açılan dosya sayısı 77 iken, 2020 yılında 90, 2021 yılında ise 130 dosya şeklinde olmuştur.

Bilişim alanında ki suçlar, özel hayatın gizliliğine ilişkin suçlar ve ekonomi alanındaki suçlar (TCK m.239) ile ilgili olarak son 5 yıllık süreçte verilmiş olan mahkumiyet ve beraat kararlarına ilişkin veriler 23, 24 ve 25 numaralı Tablolarda yer almaktadır.

Tablo 23. TCK Uyarınca Bilişim Suçları ile İlgili Olarak Davalarda Verilen Kararlar ve Oranları (Adli Sicil Ve İstatistik Genel Müdürlüğü, 2017-2021)

Yıl	Suç Türü	Mahkumiyet Kararı	Yüzdelik Dilim (%)	Beraat Kararı	Yüzdelik Dilim (%)	Toplam
2017	Bilişim Suçları 243-246	16.006	39,7	5.136	12,7	40.324
2018	Bilişim Suçları 243-246	20.479	45,4	5.583	12,4	45.074
2019	Bilişim Suçları 243-246	**22.269**	54,5	6.180	15,1	40.868
2020	Bilişim Suçları 243-246	14.415	50,9	4.120	14,6	28.293
2021	Bilişim Suçları 243-246	**24.336**	51,4	8.990	19,0	47.352

Tablo 24. TCK Uyarınca Özel Hayatın Gizliliğine Karşı Suçlar ile İlgili Olarak Davalarda Verilen Kararlar ve Oranları (Adli Sicil ve İstatistik Genel Müdürlüğü, 2017-2021)

Yıl	Suç Türü	Mahkumiyet Kararı	Yüzdelik Dilim (%)	Beraat Kararı	Yüzdelik Dilim (%)	Toplam
2017	Özel Hayata Karşı Suçlar 132-140	2.243	14,3	2.105	13,4	15.668
2018	Özel Hayata Karşı Suçlar 132-140	5.396	28,2	5.451	28,5	19.108
2019	Özel Hayata Karşı Suçlar 132-140	**4.902**	29,8	3.723	22,6	16.469
2020	Özel Hayata Karşı Suçlar 132-140	3.352	26,3	2.430	19,1	12.726
2021	Özel Hayata Karşı Suçlar 132-140	**7.276**	31,5	4.442	19,2	23.115

Tablo 23 ve Tablo 24 bulguları incelendiğinde, seneler içinde, her iki suç bakımından verilen mahkumiyet kararlarında artışlar olduğu anlaşılmaktadır. Örneğin bilişim alanındaki suçlar bakımından 2019 yılı için verilen mahkumiyet karar sayısı 22.269 iken 2021 yılında sayı 24.336 olmuştur. Aynı şekilde özel hayata ilişkin suçlar bakımından, 2019 yılında verilen mahkumiyet karar sayısı 4.902 iken 2021 yılında sayı 7.276 olarak belirlenmiştir. Veriler, özellikle 2020 yılında yaşanan pandemi ile birlikte bilgi

güvenliğine ilişkin suçlar bakımından yargıya intikallerde artış yaşandığını göstermektedir. Yayınlanmış olan son adli istatistik verisi 2021 tarihlidir.

Tablo 25. TCK Uyarınca Ekonomi, Sanayi ve Ticarete İlişkin Suçlardan 239. Madde İle İlgili Olarak Davalarda Verilen Kararlar (Adli Sicil ve İstatistik Genel Müdürlüğü, 2017-2021)

Yıl	Suç Türü	Mahkumiyet Kararı	Beraat Kararı	Diğer Kararlar	Toplam
2017	Ekonomi, sanayi ve ticarete ilişkin suçlar (239. madde)	16	20	20	56
2018	Ekonomi, sanayi ve ticarete ilişkin suçlar (239. madde)	12	34	41	87
2019	Ekonomi, sanayi ve ticarete ilişkin suçlar (239. madde)	**16**	37	30	83
2020	Ekonomi, sanayi ve ticarete ilişkin suçlar (239. madde)	1	21	22	**44**
2021	Ekonomi, sanayi ve ticarete ilişkin suçlar (239. madde)	**3**	37	45	**85**

Tablo 25 bulgularına bakıldığında, yıllar içinde mahkumiyet karar sayılarında azalma olduğu görülmektedir. Bu durum, suçun ispatlanamamasından kaynaklanıyor olabilir. Mahkemece diğer görevsizlik şeklinde kararlar da verilmiş olabilir. Dosya sayıları açısından bakıldığında pandemi ile birlikte yargıya intikal ile karar verilen dosya sayısında (2021 yılında verilen karar sayısı toplamı 85 dosyadır) artış olduğu görülmektedir, 2020 yılında bu sayı 44' dür. 2022 ve 2023 yıllarına ait istatistik verileri, 235-242. maddelere ilişkin toplu sonuçlar olarak sunulmuş olup, yalnızca 239. maddeye özel olarak bir veri verilmediğinden bu yıllar için 239. madde sonuçlarına tabloda yer verilememiştir.

4. YÖNTEM

Çalışmanın bu bölümünde araştırma yöntemi, "Araştırma Modeli", "Evren ve Örneklem", "Veri Türleri", "Hipotezlerin Oluşturulması" ve "Veriler ve Toplanması" alt başlıklarıyla aşağıdaki bölümlerde açıklanmıştır.

4.1 Araştırma Modeli

Kişisel ve ticari verilerin korunması konusunun kendi koşulları içinde tanımlanarak, açıklanması, ulusal ve uluslararası yasal düzenlemeler ile etkileşiminin incelenerek örnek bir bilgi güvenliği politika önerisi geliştirilebilmesi için çalışmada betimleyici tarama yöntemi kullanılmıştır.

"Betimsel çalışmalar bir durumu var olduğu şekliyle ortaya koyan araştırma yaklaşımıdır. Araştırmaya konu olan olay, birey ya da nesne kendi koşulları içinde ve olduğu gibi tanımlanmaya çalışılır. Onları herhangi bir şekilde değiştirme, etkileme çabası gösterilmez. Önemli olan, onu uygun bir biçimde gözleyip belirleyebilmektir" (Karasar, 2005, s. 97). Betimleyici araştırmaların çeşitleri açısından ele alındığı zaman bu çalışmanın modeli tarama modelidir (Ekiz, 2003, s. 20).

Araştırma verileri için, ticari ve kişisel verilerin korunmasına ilişkin mevcut yasal durumu betimlemek amacıyla mevzuat, yazılı döküman, yargıtay kararları taraması yapılmıştır. Türkiye'de, bilişim suçları, kişisel verilerin korunması, ticari sırların korunması ile ilgili davalarda verilmiş olan yargı kararları ve Kişisel Verileri Koruma Kurulu kararları, belgesel araştırma yöntemi kullanılarak, Kişisel Verileri Koruma Kurumu, Adli Sicil ve İstatistik Genel Müdürlüğü ve içtihat bankaları Kazancı, Lexpera, Legalbank, HukukTürk gibi web sitelerinden temin edilerek, bilgi güvenliği riskleri açısından değerlendirilmiştir. ISO 27001 bilgi güvenliğine ilişkin literatür araştırması ve belge taraması yapılmış ve Kişisel Verilerin Korunması Kanunu düzenlemesi ile benzer ve farklı yönleri incelenmiştir. ISO 27001 Bilgi Güvenliği Yönetim Sistemi, yasal düzenlemeler çerçevesinde değerlendirilmiştir. Lojistik işletmelerde bilgi güvenliği uygulamaları ve politikaları ile ilgili mevcut durumun tespiti amacıyla öncelikle, firmaların web sayfaları içerik analizi yöntemiyle taranarak incelenmiş ve elde edilen sonuçlar değerlendirilmiştir.

Bu işlemlerin ardından, lojistik işletmelerin bilgi güvenliği uygulamalarının belirlenmesi amacıyla, tespit edilen uygun sayıdaki işletmeye anket uygulanmıştır.

Anket, literatürde itibar gören bir yöntemdir. Anket ile, güncel bilgiler kısa sürede elde edilebildiği gibi, farklı kişilerden çok değişik ve çeşitte veri alabilmek mümkündür. Ayrıca bazen de ihtiyaç duyulan bilgilerin anket yöntemi dışında başkaca yollar ile elde edilmesi imkanı bulunmadığından anket önemli bir yöntemdir (Mungan, 2022). Anket çalışması ile, şirketlerin işlediği veri türleri, mevcut bilgi güvenliği politikaları, varsa veri ihlalleri, yasal düzenlemeleri, hak ve yükümlülük farkındalıkları konusunda mevcut durumları araştırılmıştır. Elde edilen bulgular, mevcut durum ve uygulamaları ile farkındalık ve geliştirilecek olan bilgi güvenliği politikası açısından değerlendirilmiştir. Araştırma yapılan lojistik işletmelerin siber saldırı ve kötü amaçlı girişimlerin hedefi olmaması amacıyla çalışmada firma isimlerine ilişkin bilgilere yer verilmemiştir.

4.2 Evren ve Örneklem

Araştırma kapsamında firmalara uygulanan anket öncesinde, araştırmanın evren ve örneklemi belirlenmiştir. "Araştırma sonuçlarının genellenmesinin istendiği elemanların tümü olarak tanımlanan evren, araştırmacının amacı doğrultusunda belirlenmektedir. Belli bir evrenden, evreni temsil ettiği kabul edilen belli kurallara göre seçilmiş küme, örneklem olarak tanımlanabilir" (Karasar, 2010). Örneklemin belirlenmesi, araştırma sürecinde elde edilen bulguların değerlendirilebilmesi ve anlamlı olması bakımından önemlidir. Bu sebeple araştırmanın en uygun örneklem ile yapılması gözetilmiş ve hedeflenmiştir. Çalışma kapsamında ele alınan hususların gözlemlenerek araştırma değişkenlerinin ölçümlenmesinde uygun örneklem tespiti gerekir (Güler , 2022).

Örneklem üzerinde tarama (anket) çalışması yapılmaktadır. Bu şekilde evren ile ilgili genel bir kanıya varılabilir. Bu sebeple, model genel tarama modeli çeşidi kapsamındadır (Karasar, 1999). Anket örneklem sayısının belirlenebilmesi için, sektördeki firmaların sayısı tespit edilmeye çalışılmıştır.

Ülkemizde, lojistik sektöründeki şirketlerin sayısı yetki belgesi almamış olanlar sebebiyle net olarak bilinmemektedir. Verilere göre, Türkiye'deki coğrafi dağılım şekline bakıldığında Marmara bölgesinde toplanmıştır. Kayıtlı yaklaşık 4.700 civarında

uluslararası karayolu taşımacılık yetki belgesi bulunan firmanın yaklaşık 1.000 tanesi İstanbul ve çevresindedir. Yurtiçi taşımacılık yetki belgeli yaklaşık 313 bin firmanın 105 bin tanesi İstanbul bölgesindedir. Uluslararası Nakliyeciler Derneği'ne kayıtlı 1.079 adet üyenin 306 tanesi İstanbul'da, Uluslararası Taşımacılık ve Lojistik Hizmet Üretenleri Derneğine bağlı 447 adet lojistik firmanın 363 tanesinin merkezi İstanbul'da bulunmaktadır (T.C.Kalkınma Bakanlığı, 2018). Bu verilere göre, yoğunluk İstanbul ve civarı olduğundan evrenin İstanbul olarak belirlenmesi düşünülmüştür.

Diğer taraftan, tam sayıyı tespit etmek üzere, sözkonusu lojistik derneklerine üye olan firmalar bakımından araştırma yapılarak sayı belirlenmeye çalışılmıştır. Ancak, lojistik derneklerine üye firmalar incelendiğinde de, bu kez aynı firmaların birden fazla lojistik derneğine üye oldukları görülmüştür. Bu durumda dernek üyelerinin sayısı dikkate alınarak ne bölgesel olarak ne de ülke genelinde tam bir sayı belirlemek mümkün olamamıştır.

Anket çalışmasının başlatılabilmesi için evren ile birlikte örneklem sayısının tespiti gerekmektedir, sayı tespiti için araştırmalara devam edilmiştir. Ulaştırma ve Altyapı Bakanlığı'nın resmi web sitesi incelenerek sektör temsilcileri ile görüşmeler yapılmıştır. Yasal düzenlemeler ve diğer kaynakların incelenmesi neticesinde, Kalkınma Bakanlığı'nın, 2018 tarihli 11. Kalkınma Planı Komisyon Raporunda yoğunluğun İstanbul ve civarında olduğu şeklinde bir bilgi olmasına rağmen Ulaştırma ve Altyapı Bakanlığı sitesindeki veriler evren ve örneklem hesabında dikkate alınarak, anket çalışmasının, Taşıma İşleri Organizatörlüğü (TIO) belgesi sahibi firmalara uygulanmasına karar verilmiştir. Böylece, anket uygulanacak firma evren ve örneklem sayısı net olarak belirlenebildiği gibi, aynı zamanda örneklem sayısı büyümüş, araştırma evreni belli bir bölge, il ile sınırlı kalmayıp ülke genelini kapsayacak şekilde belirlenmiştir.

4.3 Veri Türleri

Tüzel kişilerin işlediği veriler; "Tüzel kişiliğe ilişkin olan veriler", "Kişisel veriler" ve "Diğer veriler" şeklinde gruplandırılabilir. Anket hazırlık sürecinde, bu ayırımdan yola çıkılarak lojistik işletmelerin web sayfaları ve Verbis sayfaları (Veri sorumluları sicili)

taranarak kayıt altına aldıkları veri türleri incelenmiştir. Araştırma sonuçlarına bakıldığında, firmalar genel olarak;

- Kişisel Verilerin Korunması Kanunu gereğince, internet sitelerinde ve Verbis sisteminde, kişisel verilere ilişkin düzenlemelere genel olarak yer vermişlerdir. Böylelikle firmaların bu mecralarda paylaşmış oldukları bilgilere (kayıt edilen kişisel veri türleri, grupları gibi) ulaşılmıştır.

- Lojistik işletmelerin tüzel kişilere ilişkin verileri ile ilgili olarak KVKK benzeri bir yasal düzenleme olmadığından ve ticari sır niteliğindeki veriler gizli kalması gereken türden veriler olduğundan, şirketlerin web sitelerinde bu veriler bakımından Kişisel Verilerin Korunması Kanunu benzeri bir düzenlemeye yer verilmemiştir. Ancak şirketlerin, Türk Ticaret Kanunu'nun "Elektronik İşlemler ve Bilgi Toplumu Hizmetleri" "İnternet Sitesi" başlıklı 1524'üncü maddesi gereğince resmi web sayfalarında bilgi toplumu hizmetlerine yer vermeleri ve bunu herkesin erişimine açmaları gerekmektedir.

> Madde 1524- (Değişik: 26/6/2012-6335/34 md.): (1) 397 nci maddenin dördüncü fıkrası uyarınca denetime tabi olan sermaye şirketleri, kuruluşlarının ticaret siciline tescili tarihinden itibaren üç ay içinde bir internet sitesi açmak ve bu sitenin belirli bir bölümünü şirketçe kanunen yapılması gereken ilanların yayımlanmasına özgülemek zorundadır(...) (3) İnternet sitesinin bilgi toplumu hizmetlerine ayrılmış bölümü herkesin erişimine açıktır. Erişim hakkının kullanılması, ilgili olmak veya menfaati bulunmak gibi kayıtlarla sınırlandırılamayacağı gibi herhangi bir şarta da bağlanamaz. Bu ilkenin ihlali hâlinde herkes engelin kaldırılması davasını açabilir (Türk Ticaret Kanunu, 2011).

31 Mayıs 2013 tarih ve 28663 sayılı Resmi Gazetede yayınlanmış olan '*Sermaye Şirketlerinin Açacaklari İnternet Sitelerine Dair Yönetmelik'* hükümleri gereğince, şirketlerin, kamuya açık olan bilgilendirmeleri web sayfalarının "*Bilgi Toplumu Hizmetleri"* bölümünde yer almaktadır (T.C. Resmi Gazete, 2013). 30 Kasım 2022 tarih ve 32029 sayılı Resmi Gazete'de "Bağımsız Denetime Tabi Şirketlerin Belirlenmesine Dair Karar" yayımlanarak, bağımsız denetime tabi şirketler belirtilmiştir (T.C. Resmi Gazete, 2022).

- Bu veriler dışındaki bilgilere ancak şirketlerin web sitelerinde yer verildiği ölçüde ulaşılması mümkün olmaktadır. Bu noktada firmaların işledikleri diğer verilerin belirlenebilmesi için, şirketlerin hizmetleri, çalışma alanları, faaliyet kapsamı ile sahip oldukları belgelere bakılarak araştırma yapılmıştır;

- Çalışma alanları (ulusal-uluslararası),
- Sunulan lojistik hizmetleri bakımından işlenen veri türleri değişiklik göstermektedir, bu açıdan inceleme yapılmıştır,
- Üretim yapan bir firma olup kendi bünyesinde lojistik faaliyet yapıp yapmadığı bakımından (genel olarak büyük imalatçı şirketler lojistik faaliyetlerini kendileri gerçekleştirmekte ve lojistik işlemlerinin imalat işlemleri ile birleşik bir şekilde yapılması söz konusudur),
- Ayrıca, firmaların sahip olduğu ISO 27001 Bilgi Güvenliği Yönetim Sistemi belgesi varlığı açısından araştırma yapılmıştır.

Tüm bu araştırmalar sonucunda elde edilen bilgiler çerçevesinde değerlendirme yapılarak aşağıda sunulmuştur.

4.3.1 Kişisel veriler ile ilgili araştırma

Yasal düzenlemeler, Kişisel Verilerin Korunması Kanunu gereğince firmaların web sitelerinde yayınladıkları beyanları ve kamuya açık olan Verbis kayıtları incelendiğinde, lojistik işletmeler tarafından işlenen kişisel veri türlerine ulaşılmıştır. Tablo 26 ve Tablo 27'de örnek özet kişisel veri bilgi türlerine yer verilmiştir.

Tablo 26. Kişisel Veri Türleri (Kişisel Verileri Koruma Kurumu, t.y.)

Kimlik Bilgisi	İnsan Kaynakları Personel ve Finansal Veriler
İletişim Bilgisi	Hukuki İşlem
Aile Bireyi ve Yakın Bilgisi	Özel Nitelikli Kişisel Veri
İşlem Güvenliği Bilgileri	Eğitim Verisi
Özlük Bilgisi	Görsel ve İşitsel Veri
Lokasyon	Talep ve Şikayet Verileri
Müşteri İşlem	Fiziksel Mekan Güvenliği Bilgileri

Tablo 27. Kişisel Veri Konusu Kişi Grupları (Kişisel Verileri Koruma Kurumu, t.y.)

Firma hissedar/ortak gerçek kişiler	Tedarikçi, tedarikçi çalışanı, tedarikçi yetkilisi
Firma Yönetim Kurulu üyeleri ve diğer yetkili gerçek kişiler	Ürün veya hizmet alan kişi, ürün veya hizmet alan kişi tedarikçisi, potansiyel ürün veya hizmet alıcısı
Firmanın gerçek kişi müşterileri, tedarikçi ve yüklenicilerin yetkili gerçek kişileri ve bu kişiler tarafından görevlendirilen çalışanlar.	Potansiyel Müşteri (Lojistik şirketinin sunduğu hizmetleri kullanma ilgisini gösteren, müşteriye dönüşme potansiyeli olan web sitesinden veya diğer kanallarla hizmetlerden yararlanma iradesini ortaya koyan, teklif talep eden gerçek kişiler)
Firmada çalışan veya staj yapan gerçek kişiler, Firma çalışan adayı, çalışan yakını	Ziyaretçi

4.3.2 Tüzel kişi verileri ile ilgili araştırma

Tüzel kişilerin işlediği, tüzel kişiliğe ilişkin veriler ile ilgili olarak Kişisel Verilerin Korunması Kanunu gibi özel bir yasal düzenleme bulunmadığından, Borçlar Kanunu, Ticaret Kanunu, Ceza Kanunu, Medeni Kanun, Fikir ve Sanat Eserleri Kanunu'nda koruyucu düzenlemelere yer verilmiştir. Bundan dolayı, firmaların web sayfaları incelendiğinde, tüzel kişi verilerine ilişkin fazla bir bilgiye ulaşılamamıştır. İnceleme sonucu ulaşılan tüzel kişilere ilişkin örnek özet veriler şu şekildedir:

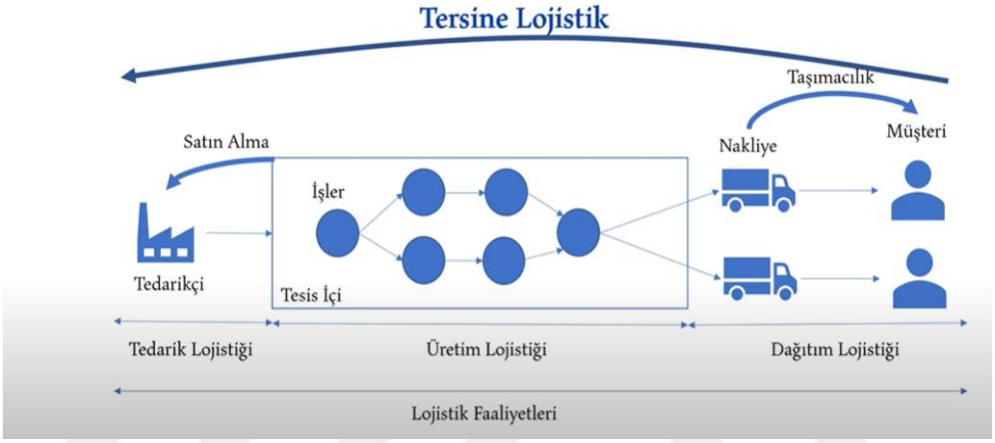
- Firmaların web sayfalarında kamuya açık olacak şekilde *''Bilgi Toplumu Hizmetleri"'* adı altında açıklanan bölümde firmaya ait şu verilere yer verilmektedir; Şirket türü (A.Ş., Ltd.Şti. gibi), firma ticaret ünvanı (firma ismi), sicil ve sermaye bilgileri, vergi numarası gibi ve iletişim bilgileri, yönetim kurulu ve denetçi bilgileri ile bazı şirket kararları (E-Şirket, t.y.).

- Tedarik zinciri, birlikte çalışan çok sayıda kuruluştan (tedarikçi, üretici, dağıtıcı gibi) oluşan bir ağdır. Zincir içinde yer alanlar; Hammadde tedarikçisi, Mamül ve hizmet üreticileri, Yan sanayii ürünleri tedarikçileri, Distribütörler, Alt montaj tedarikçileri, Lojistik hizmeti veren kuruluşlar, Toptancılar, Perakendeciler, Müşteriler, Bayiler, Satış sonrası destek hizmeti veren kuruluşlar şeklinde sayılabilir (Palamutçuoğlu, 2012). Lojistik işletmeler bu zincir içindedir. Zincir birçok lojistik faaliyetin birleşiminden oluşmaktadır.

Dolayısı ile yapılan her bir işlemde, lojistik işletme tarafından farklı birimler ile temas edilerek veri kaydı yapılması sözkonusudur. Karşı taraf müşterinin de tüzel kişi olması halinde karşılıklı tüzel kişilerin veri kaydından sözedilecektir. Aynı şekilde lojistik

işletme, bir mamul ve/veya hizmet üreten firmanın bünyesinde faaliyet gösteriyor ise bu halde işlenen veri çeşidinde (ürün formülleri, patent gibi) değişiklikler olabilecek farklı veri türleri eklenebilecektir.

- Müşterilerin ihtiyaçlarını gidermek üzere imalat ve tüketim yerleri arasındaki eşya, bilgi ve hizmetlerin, ileri ve geri yönlü hareketleri ile depolanmalarının verimli ve etkin şekilde organize edilmesi, yürütülmesi ve denetimini içeren tedarik zinciri aşamasına lojistik yönetimi denir (Palamutçuoğlu, 2012).



Şekil 11. Lojistik İş Süreçleri (Erden, 2021)

Lojistik faaliyet aşamalarının her birinde firmanın kayıt altına aldığı veri türleri değişebildiği gibi, irtibat kişileri de değişebilmektedir. Lojistik iş süreçleri Şekil 11'de gösterilmiştir.

Lojistik işletmelerin sunduğu hizmetler, Taşımacılık, Gümrük, Sigorta, Depolama, Talep ve Stok Yönetimi, Müşteri Hizmetleri, Muayene, Gözetim ve Terminal hizmetleri ile Paketleme, Etiketleme gibi Katma Değerli Hizmetlerdir (Tanyaş, t.y.).

Sunulan hizmetler ile ilgili olarak veritabanlarında depolanan bazı veri türleri aşağıda belirtilmiştir.

1- İşletme kayıtları: Lojistik faaliyetlerin maliyeti,

2-Yönetim ile ilgili olan kayıtlar: Satış tahminleri, ürün teklifleri,

3- İşkolu/dış kaynaklı veriler: Piyasa oranı, ürün ve finansal eğilimler,

4- İş süreçleri bilgisi: Nakliye ücreti, envanter, mal hareketleri,

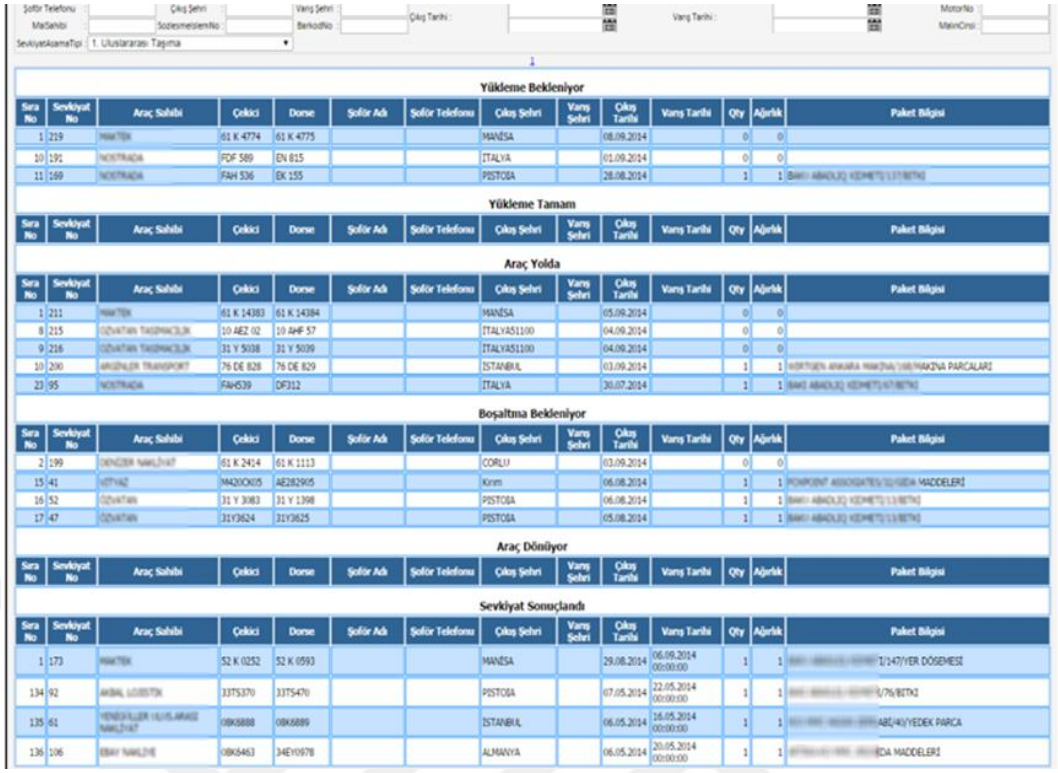
5- Sipariş işleme: Sipariş durumu, müşteri lokasyonu, sipariş günlüğü,

6- Rapor oluşturma: Lojistik performansı, sipariş ve nakliye verimliliği, atıklar ve yeniden kullanım, finansal değerlendirmeler,

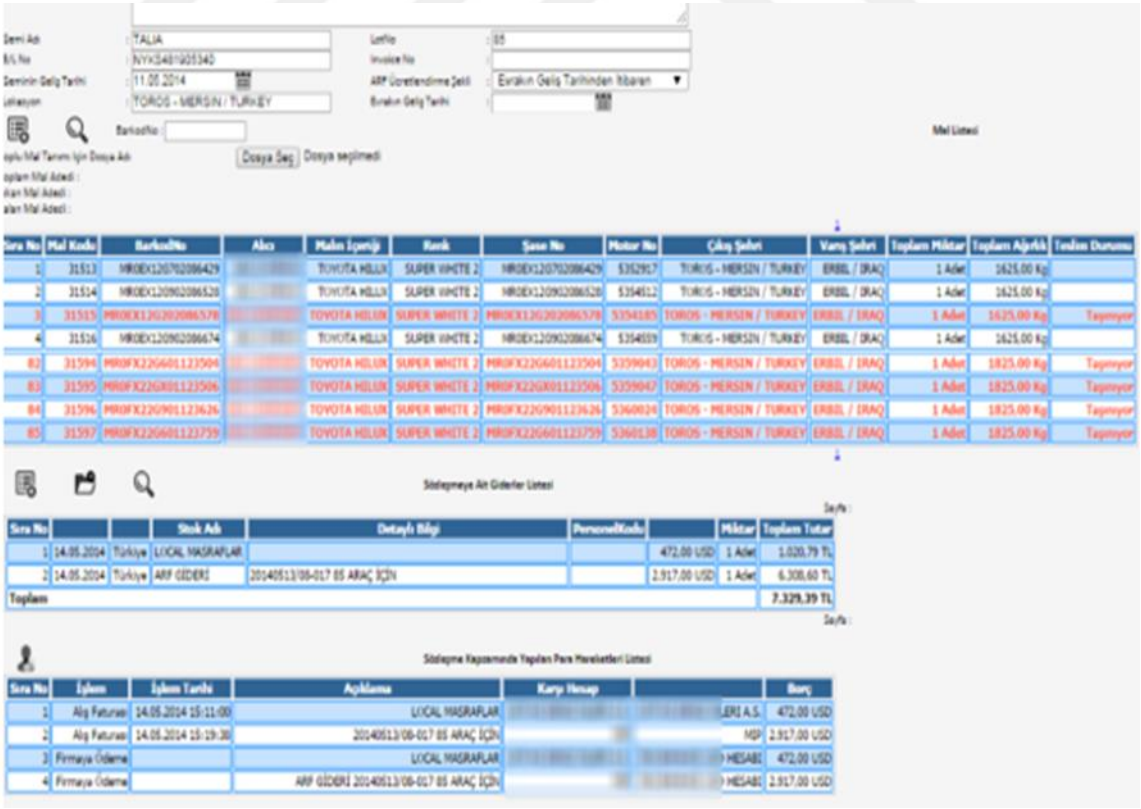
7- Diğer Veriler; Sipariş izleme, stok yönetimi, sipariş verme, satış tahmini, üretim planı ve taşıma operasyonları, dış ticaret, gümrük, müşteri ilişkileri, araç takip bilgileri, sigorta, gümrük işlemleri şeklinde sayılabilir (Palamutçuoğlu, 2012).

Yukarıda belirtilen bu verilerin bazıları gizli kalması gereken türden ticari sır kapsamında (çok gizli) iken, bir kısmı sadece tüzel kişiliğe ilişkin veriler olup belki sadece firma içinde paylaşılmasına izin verilen (gizli) verilerdir, kimi veri de kamuya açık türden bilgilerdir.

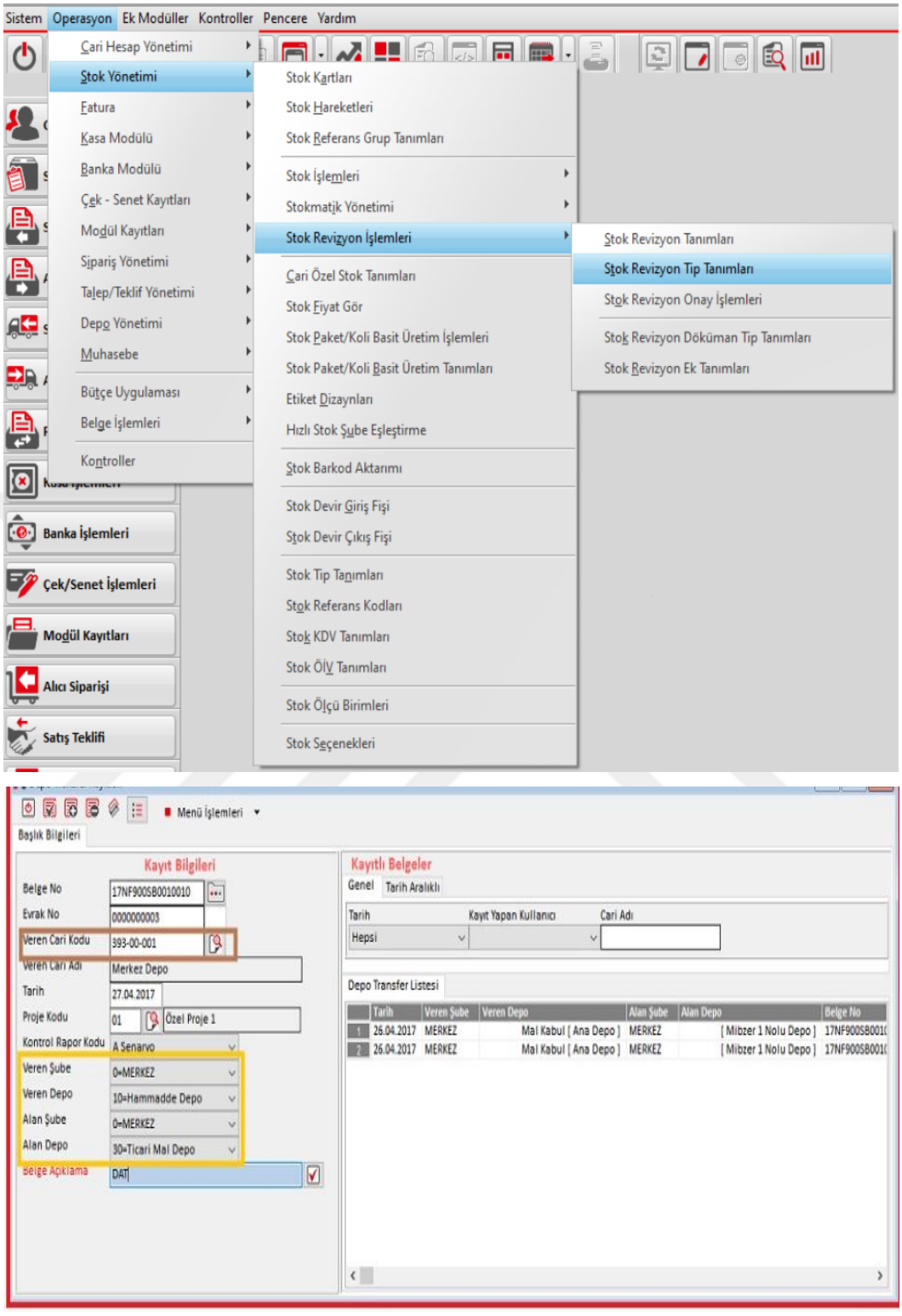
Veri kayıtları, firmanın elektronik ya da elektronik olmayan ortamlarında muhafaza edilmektedir. Elektronik ortamda kayıt altına alınan veriler için de ihtiyaca uygun, çeşitli yazılım programları kullanılmaktadır. Şekil 12, 13 ve 14'de, lojistik işletme tarafından sunulan hizmet türüne göre; Taşıma (nakliye), sipariş, stok ve depo gibi faaliyetleri için elektronik ortam kayıt görselleri yer almaktadır. Şekil 12 ve 13'de bir lojistik işletmesinin nakliye yönetimi sevkiyatlar ve siparişlere ilişkin elektronik kayıtları görülmektedir. Görsellerde, taşınacak malın teslim edileceği şehir, teslim tarihi, araç sahibi, plaka gibi veriler ile mala ilişkin bilgiler, borç detayları, miktar güzergah gibi ayrıntılı veriler elektronik ortamda kayıt altına alınmıştır.



Şekil 12. Nakliye Yönetim Modülü Sevkiyatlar (Lojistik Programı, t.y.)



Şekil 13. Sipariş Modülü (Lojistik Programı, t.y.)



Şekil 14. Stok ve Depo Modülü (Atiker Yazılım, 2019)

Şekil 14 görselinde, şirket stok ve depo ile ilgili ayrıntılı veriler elektronik ortamda kayıt altına alınmıştır.

Görsellerden anlaşıldığı üzere, lojistik işletmeleri, sundukları hizmetlere uygun olarak iş süreçlerini detaylı bir şekilde elektronik sistemlerde kayıt altına almaktadır. Ayrıca ticari faaliyetler kapsamında yapılan sözleşmeler, kambiyo senetleri ve üst yönetime ait kararlar ve üretim formülleri gibi değerli belgeler de fiziksel olarak, dolap, kasa, çekmece gibi ortamlarda saklanmaktadır. Dolayısı ile verilerin muhafaza edildiği elektronik ve fiziki ortamların izinsiz müdahalelere karşı korunması, güvenliklerinin sağlanması gerekmektedir.

Veri kayıtları, lojistik şirketin merkez binasında yapılabildiği gibi işin gereği olarak şube, mağaza veya depo gibi çalışma ortamlarında da yapılmaktadır. Gün sonunda, işletmeye ait bilgilerin tamamı merkez sistemde toplanıyor olsa da, koruma tedbirlerinin tüm iş ortamlarını kapsayacak şekilde alınması gerekir.

- Tüzel kişiler, ticari sır niteliğindeki verileri de kayıt altına almaktadır. Bazı ticari sır örneklerine Tablo 28'de yer verilmiştir.

Tablo 28.Ticari Sır Örnekleri (Kurt, 2019)

Fiyatlandırma politikaları	Finansal, ekonomik, borç ve nakit durumu
Pazarlama yöntemleri ve giderleri	Pazar oranları
Toptan satıcı ve perakendeci satıcı müşteri kapasitesi ve ağları	İç kuruluş yapısı ve organizasyonu
Ar-Ge faaliyetleri	İş planları
Temel malzeme kaynakları	İmalat ve üretimle ilgili teknolojik bilgiler

Kentucky Fried Chicken'in tarifi, Google arama motorunun algoritması ve Cola Cola'nın formülü ticari sır örnekleridir. İşletmeler için ticari sırlar kıymetli varlıklardandır. Amerika'da temyiz mahkemesi verdiği bir kararda ticari sırrı şöyle tanımlamıştır: "Ticari sır müşteri listesi, üretim usulü, bir içeceğin gizli formülü gibi bir bilgidir. Ticari sır sahibi bu bilgiyi çalışanları ile veya diğer kişilerle gizlilik anlaşması yaparak ve koruyarak, şifreleyerek ve başka usullerde gizleyerek gizli tutmaktadır. Öyle ki, ticari sırrın açığa çıkması sözleşmenin ihlali veya haksız fiil teşkil etmektedir" (Yüksel, 2018).

Diğer taraftan lojistik işletmelerinin kendi faaliyet alanlarına ilişkin olarak, hizmet verdiği ve hizmet aldığı müşterileriyle ilişkilerinde, ekonomik, likidite ve borç durumuna ilişkin doğrudan veya dolayısıyla edindikleri tüm bilgi ve belgeler de müşteri sırrı kapsamında değerlendirilecektir.

4.4 Araştırma Hipotezlerinin Oluşturulması

Anket çalışması ile, lojistik işletmelerde bilgi güvenliği uygulamalarının, farkındalıkların tespit edilmesi amaçlanmıştır. Bu amaç doğrultusunda hazırlanan ve elde edilen verilere göre test edilip analiz edilecek 9 adet hipotez oluşturulmuştur.

H1: Mali Durum, ISO 27001 Belgesi Sahibi Olunmasında Etkilidir.

H2: ISO 27001 Belgesi Sahibi Firmalar, Tedarikçi ve Müşterilerinin de ISO 27001 Belgesine Sahip Olmasının Öneminin Farkındadırlar.

H3: Eğitim, Veri İhlalleri Konusunda Farkındalık Oluşumunda Etkilidir.

H4: Bilgi Güvenliğine Harcama Yapan Firmalar, Veri İhlali Etkilerinin Farkındadırlar.

H5: Mali Durum, Bilgi Güvenliğine Yönelik Harcama Yapılmasında Etkilidir.

H6: Veri Güvenliğinden Yasal Sorumlu Olunduğunun Farkında Olunması, Veri Güvenliğinin Korunmasına Yönelik Önlem Alınmasında Etkilidir.

H7: Veri Güvenliğinden Yasal Sorumlu Olunduğunun Farkında Olunması, Bilgi Güvenliğine Bütçe Ayrılmasında Etkilidir.

H8: Bilgi Güvenliğinden Sorumlu Komisyon Kurulmuş Olması, Verilere İlişkin Prosedür ve Politikaların Oluşturulmasında Etkilidir.

H9: Şirket Personeline Bilgi Güvenliğine İlişkin Eğitim Veren Firmalar, Personel Sözleşmelerine Bilgi Güvenliği, Sır Saklama Yükümlülüğüne İlişkin Hüküm Koyulması Gerektiğinin Farkındadırlar.

4.5 Veriler ve Toplanması

4.5.1 Anket ve bulgular

Araştırma Evreni ülke genelinde faaliyet gösteren 5413 lojistik işletmesinden oluşmaktadır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2022). Araştırma evreninden %95 güvenilirlik sınırı içinde, %5 hata payı oranı öngörülerek seçildiğinde, 5413 kişilik evreni temsil etmek için asgari ulaşılması gereken örneklem sayısı 359 olarak belirlenmiştir. Evreni bilinen örneklem hacmi formülü kullanılarak yapılan bu hesaplama aşağıda sunulmuştur.

Formül;

$$n = \frac{N.t^2 p.q}{d^2(N-1)+t^2.p\ .q} \qquad (4.1.)$$

N: Evrendeki birey sayısı (5413)

n: Örnekleme alınacak birey sayısı (?)

p: İncelenen olayın görülüş sıklığı(olasılığı) (0,50)

q: İncelenen olayın görülmeyiş sıklığı(1-p) (0,50)

t: Belirli serbestlik derecesinde ve saptanan yanılma düzeyinde t tablosunda bulunan teorik değer (1,96)

d: Olayın görülüş sıklığına göre yapılmak istenen sapma (0,05) (Güler, 2022)

Değerler yerine yazıldığında;

$$\frac{5413*1{,}96^2*0{,}50*\ 0{,}50}{0{,}05^2(5413\ -1)+1{,}96^2*0{,}50*\ 0{,}50} = 359 \qquad (4.2.)$$

Bu araştırmada veri toplama anket formu 52 adet tek ve çoktan seçmeli sorudan oluşmaktadır. Araştırmada anket formu online (dijital) oluşturulmuş ve firmalara, web sayfalarından, sosyal medya gruplarından, linkedin ve firmaların verdiği bilgiler doğrultusunda anket linki paylaşılmış olup katılımcılara ulaşılmaya çalışılmıştır. Ankete katılım düzeyini arttırmak ve anketin doğru bireylere ulaştığını teyit etmek üzere telefon görüşmeleri gerçekleştirilmiştir. Yaklaşık 1000 firmaya anket formu yollanmış, tutarlı geri dönüşler incelendiğinde Örneklem hacmi 359 hesaplanmasına rağmen toplam 457 firmadan geri dönüş olduğu belirlenmiştir. Bu sebeple araştırmanın örneklemi 457 firmadan oluşmaktadır.

Anket beş bölümden oluşmaktadır. Anketin 1.bölümünde, "Firmalara İlişkin Bilgilerin" (demografik sorular) sorulduğu 6 soru bulunmaktadır. Anketin 2.bölümünde "Verilere İlişkin" 9 adet soruya yer verilmiştir. Anketin 3. bölümünde "Bilgi Güvenliği Yönetim Sistemi" ile ilgili soruların yönetildiği 10 adet soru bulunmaktadır. Anketin 4.bölümünde "Veri İhlali" ile ilgili 8 adet soru yer almaktadır. Anketin son bölümünde ise "Bilgi Güvenliğine İlişkin Tedbir Ve Yükümlülükler" ile ilgili mevcut durumu tespite yönelik 19 soruya yer verilmiştir.

Anketi yapılandırmak amacıyla, araştırma kapsamında literatürdeki kaynaklar incelenmiştir. Anket soruları hazırlanırken, Diamantopoulou, Tsohou ve Karyda (2020), Mirtsch, Kinne ve Blind (2021), Zaralı (2022), Mirtsch, Blind, Koch ve Dudek (2021), Henkoğlu (2015), Pawar ve Dr. Palivela (2022), Küpeli (2019), Pham, Nguyen, Mcdonald ve Tran-Kıeu (2019), Yılmaz (2018), Avci ve Karataş (2017), Durowoju, Chan, Wang ve Akenroye (2020), Safa, Maple ve Watson (2017), Zadeh, Ramayah, Hanifah, Kurnia ve Mahmud (2020), Houston (2021), Senarak (2021), Aver (2020), Karaca (2019), Wolden, Valverde ve Talla (2015), Boiko, Shendryk ve Boiko (2019), Şişkin (2020), Hashem ve Hanafy (2017) ve Sindhuja (2021)'a ait literatürdeki çalışma ve anketlerden, Kişisel Verilerin Korunması Kanunu, uygulama rehberleri ve verilerin korunmasına ilişkin diğer yasal düzenlemelerden, Marsh ve TÜSİAD tarafından hazırlanan 2020 yılı Türkiye Siber Risk Algı Araştırması Raporundan, ISO 27001 BGYS standartlarından, çeşitli kamu ve özel şirketlerin bilgi güvenliği politikalarından,

Cumhurbaşkanlığı dijital dönüşüm ofisi bilgi ve iletişim güvenliği rehberinden (2020), Bilgi güvenliğine ilişkin Yargıtay kararlarından faydalanılmıştır.

Araştırma kapsamında, bilgi güvenliğine ilişkin olarak tüzel kişi ve kişisel verilerin korunmasına dair mevcut durumu betimlemek amacıyla literatür taraması yapılmıştır. Yasal düzenlemeler, yazılı dökümanlar, yargıtay ve kurul kararları için belge taraması yapılarak toplanan bilgiler, döküman analizi tekniğiyle incelenmiştir. Türkiye'de, bilişim suçları, kişisel verilerin korunması, ticari sırların korunması ile ilgili davalarda verilmiş olan Yargıtay kararları ve Kişisel Verileri Koruma Kurul kararları, belgesel araştırma yöntemi kullanılarak, içtihat bankaları Lexpera, HukukTürk, Legalbank, Kazancı gibi ve Kişisel Verileri Koruma Kurumu web sitelerinden temin edilerek, bilgi güvenliği riskleri açısından değerlendirilmiştir. ISO 27001 bilgi güvenliğine ilişkin literatür araştırması ve belge taraması yapılmış, standard kapsamı yasal düzenlemeler çerçevesinde değerlendirilmiştir. ISO 27001 Bilgi Güvenliği Yönetim Sistemi düzenlemesi ile Kişisel Verilerin Korunması Kanunu düzenlemelerinin benzer ve farklı yönleri araştırılmıştır.

Lojistik işletmelerde bilgi güvenliği ve politikalarına ilişkin var olan uygulamaların tespit edilmesi amacıyla hazırlanan anket formu, Türkiye genelinde TIO belgesi sahibi lojistik işletmelere online olarak gönderilmiştir. Tutarlı geri dönüşler belirlenen örneklem sayısınında üzerinde olmuştur. Lojistik firmaları, ülkemizin değişik bölge ve şehirlerinde hizmet vermekte ve farklı ölçekten (Limited şirket, Şahıs şirketi, Anonim şirket gibi) firmalardan oluşmaktadır. Katılımcı firmalara cevaplamaları için, işledikleri veri türleri, mevcut bilgi güvenliği politikaları, yasal düzenlemeler, veri ihlalleri, hak ve yükümlülükler ile bilgi güvenliğine ilişkin farkındalıkları konularını kapsayan çeşitli sorular yöneltilmiştir.

Araştırma boyunca araştırma etiğine özen gösterilmiştir. Gizliliğin ihlali, anlaşmalara uyulmaması, yasalara uymama, katılımcıları yanıltma, sonuçları yanlış sunma gibi ihlaller yapılmamıştır (Mungan, 2022).

Araştırmanın bu kısmında araştırmaya gönüllülük esasında dahil olan katılımcıların, anket formunda her bir soru için verdikleri cevaplara ilişkin dağılımları verilmiştir. Elde edilen anket verileri SPSS 25.0 programı aracılığıyla analiz edilmiştir. Her bir soruya verilen yanıtların dağılımlarının incelenmesinde frekans ve yüzde analizi yapılmıştır.

Anketin 1. bölümünde katılımcılara, firmaların demografik özelliklerine ilişkin sorular sorulmuş ve edinilen bulgular aşağıda sunulmuştur.

4.5.1.1 Demografik özelliklere ait bulgular

Örneklemi oluşturan işletmelere ait demografik özellikler Tablo 29'da yer almaktadır.

Tablo 29. İşletmelerin Demografik Özellikleri

İşletmelerin Özellikleri

Toplam Çalışan Sayısı

Yanıtlar	n	%
10'dan az	126	27,6
10-50	151	33,0
50-250	144	31,5
250'den fazla	36	7,9
Toplam	**457**	**100,0**

Sermaye Yapısı

Yanıtlar	n	%
Yabancı	58	12,7
Yerli	299	65,4
Yabancı Ortaklı	100	21,9
Toplam	**457**	**100,0**

Son Mali Yıla Ait Yıllık Gelir(Şirket Cirosu)

Yanıtlar	n	%
5 Milyon TL altında	172	37,6
5-50 Milyon TL	175	38,3
50-250 Milyon TL	74	16,2
250 Milyon TL ve Üzeri	36	7,9
Toplam	**457**	**100,0**

Şirketiniz Hangi Coğrafi Alanda Hizmet Vermektedir?

Yanıtlar	n	%
Sadece Yurtiçi	268	58,6
Sadece Yurtdışı	28	6,1
Her İkisi Birlikte	161	35,2

Toplam	**457**	**100,0**

Şirket Büyüklüğü		
Yanıtlar	n	%
Küçük ve Orta Ölçekli	421	92,1
Büyük Ölçekli	36	7,9
Toplam	**457**	**100,0**

Şirketiniz Hangi Lojistik Hizmetleri Vermektedir?		
Yanıtlar	n	%
Taşımacılık	246	29,4
Gümrük	118	14,1
Sigorta	81	9,7
Depolama	113	13,5
Talep ve Stok Yönetimi	97	11,6
Muayene, Gözetim vb. Terminal Hizmetleri	76	9,1
Paketleme, Etiketleme vb.	107	12,8
Toplam	**838**	**100,0**
#Çoklu yanıt verildiğinden cevaplayıcı sayısı örneklem sayısını geçebilir.		

İşletme özelliklerine göre dağılımlar incelendiğinde, katılımcı şirketlerin %92,1'i (n:421) Küçük ve Orta ölçekli, %7,9'u (n:36) ise Büyük ölçekli firmadır. Bu durumda sektörde çok sayıda küçük ve orta ölçekli firmanın bulunduğu söylenebilecektir. Akademik çalışmalar, Pawar ve Palivela (2022), küçük ve orta ölçekli firmaların, siber tehditlere karşı en savunmasız ve veri ihlallerine karşı daha fazla tehlikede olduklarını göstermektedir.

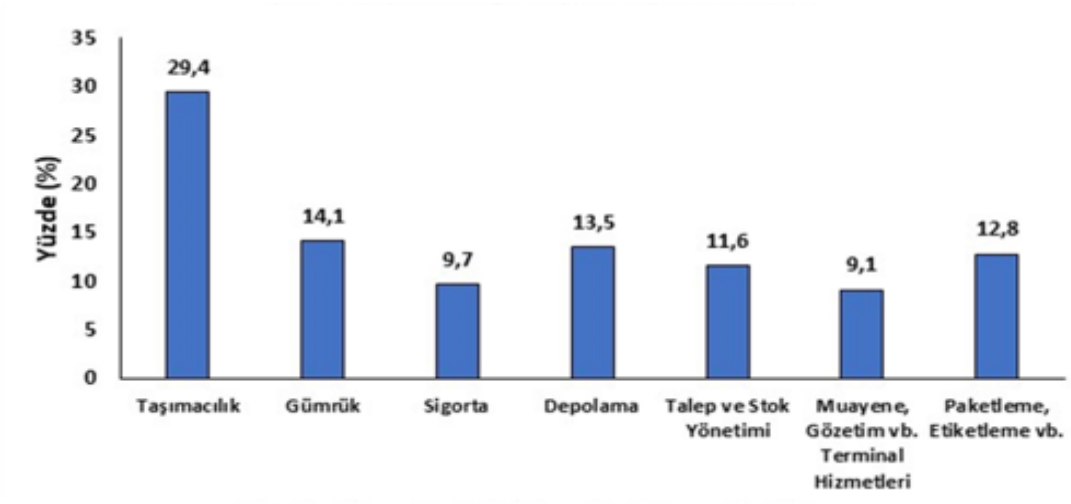
Katılımcı şirketlerin çalışan sayısı dağılımlarında ise, %33'ünün (n:151) 10-50 arasında, %31,5'inin (n:144) 50-250 arasında, %27,6'sının (n:126) 10'dan az çalışandan oluşan işletmeler olduğu görülmektedir. %7,9'unun (n:36) ise 250'den fazla işçisinin olduğu

belirlenmiştir. Firmaların %65,4'ü yerli sermayeli (n:299), %21,9'u yabancı ortaklı (n:100) ve %12,7'si ise yabancı sermayeli (n:58) işletmelerden oluşmaktadır.

Şirketlerin %58,6'sının (n:268) sadece yurtiçi, %6,1'inin (n:28) sadece yurtdışı ve %35,2'sinin (n:161) her iki coğrafi alanda hizmet sağladıkları belirlenmiştir. Sonuçlara göre, yurtdışına hizmet veren firma sayısının da fazla olduğu görülmektedir. Bu durumda kişisel veriler bakımından yurtdışına veri transferi ve bu verilerin korunmasına ayrıca özen gösterilmesi gerekmektedir. Diğer taraftan, yurtdışına lojistik hizmeti sağlayan firmalar için, uluslararası yasal düzenlemelerden sorumlu olma durumu söz konusudur. Özellikle Avrupa Birliğine üye devletler ile yapılacak lojistik işlemlerde firmalar Avrupa Veri Koruma Tüzüğü (GDPR) düzenlemelerine uymakla yükümlü olacaktır.

Katılımcı şirketlerin, %37,6'sının (n:172) 5 milyon TL'nin altında bir ciroya sahip olduğu, %38,3'ünün (n:175) 5-50 milyon TL'lik ciro, %16,2'sinin (n:74) 50-250 Milyon TL'lik ciroya, %7,9'unun (n:36) ise 250 Milyon TL üzerinde bir ciroya sahip olduğu belirlenmiştir.

Firmaların sunduğu lojistik hizmetlere göre dağılımları ise, %29,4'ünün (n:246) taşımacılık, %14,1'inin (n:118) gümrük, %13,5'nin (n:113) depolama, %12,8'inin (n:107) paketleme, etiketleme vb., %11,6'sının (n:97) talep ve stok yönetimi, %9,7'sinin (n:81) sigorta, %9,1'inin (n:76) muayene, gözetim vb. terminal hizmetleri alanında hizmet verdikleri belirlenmiştir. Şirketlerin sunduğu lojistik hizmetlere Şekil 15'de yer verilmiştir.



Şekil 15.Şirketlerin Sunduğu Lojistik Hizmetler

4.5.1.2 Veriler bölümüne ilişkin bulgular

Anketin 2. bölümünde katılımcılara, "Veriler" başlığı ile, işledikleri veri türleri, veri envanteri varlığı, kişisel ve tüzel kişi verileri, saklama ve kayıt ortamları, risk ve zararlara ilişkin yapılan çalışmalara dair konularla ilgili olarak sorular yöneltilmiştir.

Buna göre, %59,1'inin (n:270) şirkette kayıt edilen veriler ile ilgili olarak bilgi sahibi oldukları belirlenirken, %21'inin (n:96) bir bilgisi olmadığı, %19,9'unun (n:91) ise bir fikrinin bulunmadığı belirlenmiştir. Katılımcılardan elde edilen bulgulara Tablo 30'da yer verilmiştir.

Tablo 30. Şirketin Kayıt Altına Aldığı Veri Türleri

Şirketinizde Hangi Türden Verilerin Kayıt Altına Alındığını Biliyor musunuz?		
Yanıtlar	n	%
Evet	270	59,1
Hayır	96	21,0
Fikrim Yok	91	19,9
Toplam	**457**	**100**

Diğer taraftan katılımcıların veri türlerinin sınıflandırılmasına ilişkin farkındalıklarının belirlenmesine yönelik olarak hazırlanan, kişisel ve tüzel kişi verileri bilgisine ilişkin soruya, katılımcıların %69,1'i kişisel ve tüzel kişi verileri hakkında bilgi sahibi olduğunu belirtirken, %15,5'inin bilgisinin olmadığı, %15,3'ünün ise bir fikri olmadığı belirlenmiştir. Tablo 31'de sonuçlara yer verilmiştir. Her iki tablo sonucu değerlendirildiğinde, katılımcıların, kayıt edilen veriler ve türleri ile ilgili olarak bilgi sahibi olmaları, farkındalıkları açısından önemli bulunmuştur.

Tablo 31. Kişisel Veriler ile Tüzel Kişi Verileri Hakkında Bilgi

Kişisel Veriler ile Tüzel Kişi Verileri Hakkında Bilginiz Var mı?		
Yanıtlar	n	%
Evet	316	69,1
Hayır	71	15,5
Fikrim Yok	70	15,3
Toplam	**457**	**100**

Diğer taraftan katılımcılara, kişisel ve tüzel kişiliğe ilişkin verilerin kayıt altına alındığı ortamlar konusunda bilgi sahibi olup olmadıkları sorulmuş, %59,1'i konuya ilişkin bilgi

sahibi olduklarını belirtmişken, %20,1'i hayır cevabını vermiş ve %20,8'i fikri olmadığını belirtmiştir. Sonuçlara Tablo 32'de yer verilmiştir.

Tablo 32. Kişisel ve Tüzel Kişi Verilerinin Muhafaza Ortamı

Kişisel Veriler ile Tüzel Kişi Verilerinin Hangi Ortamlarda (Dijital/Fiziki) Kayıt Altına Alındığı Bilinmekte midir?		
Yanıtlar	n	%
Evet	270	59,1
Hayır	92	20,1
Fikrim Yok	95	20,8
Toplam	**457**	**100**

Veri güvenliğinin sağlanabilmesi için öncelikle yapılması gereken iş, hangi türden verilerin kayıt altına alındığının belirlenmesidir. Bunun için veri envanterinin çıkarılması gerekir. Katılımcılara, veri envanterleri bulunup bulunmadığı sorulduğunda, Tablo 33 sonuçlarına göre, %59,5 (n:272) şirketin veri envanterinin bulunduğu cevabını vermiştir. %21,4'ü (n:98) veri envanteri bulunmadığını belirtmiş ve %19'u (n:87) ise bir fikri olmadığını ifade etmiştir. Katılımcı şirketlerin veri envanterlerini hazırlamış olmaları bilgi güvenliğini sağlamak üzere olumlu bir durumdur. Diğer taraftan veri envanteri hazırlanmış olması tek başına yeterli olmayıp, verilerin risk ve önemine göre sınıflandırılmış olması da gerekmektedir.

Tablo 33.Şirketin Veri Envanteri

Şirketinizin Veri Envanteri Bulunmakta mıdır?		
Yanıtlar	n	%
Evet	272	59,5
Hayır	98	21,4
Fikrim Yok	87	19
Toplam	**457**	**100**

Katılımcılara, verilerin risk ve önemine göre gruplandırılması yapılmış mıdır şeklinde sorulduğunda, Tablo 34 sonuçlarına göre, %47,5'i (n:217) bu gruplandırmanın yapılmadığını, %28,2'si (n:129) gruplandırmanın yapıldığını ve %24,3'ü (n:111) ise bir fikri olmadığını belirtmiştir.

Tablo 34. Şirket Verilerinin Risk ve Önemine Göre Gruplandırılması

Şirketinizde Kayıt Altına Alınan Veriler Risk ve Önemine Göre Gruplandırılmış mıdır?		
Yanıtlar	n	%
Evet	129	28,2
Hayır	217	47,5
Fikrim Yok	111	24,3
Toplam	**457**	**100**

Tablo 35. Şirket Verilerinin İhlalinde Zarar Çalışması

Şirketinizde Kayıt Altına Alınan Verilere Yönelik Risklerin Gerçekleşmesi Halinde Ortaya Çıkabilecek Zararlar Konusunda Çalışma Yapılmış mıdır?		
Yanıtlar	n	%
Evet	133	29,1
Hayır	150	32,8
Fikrim Yok	174	38,1
Toplam	**457**	**100**

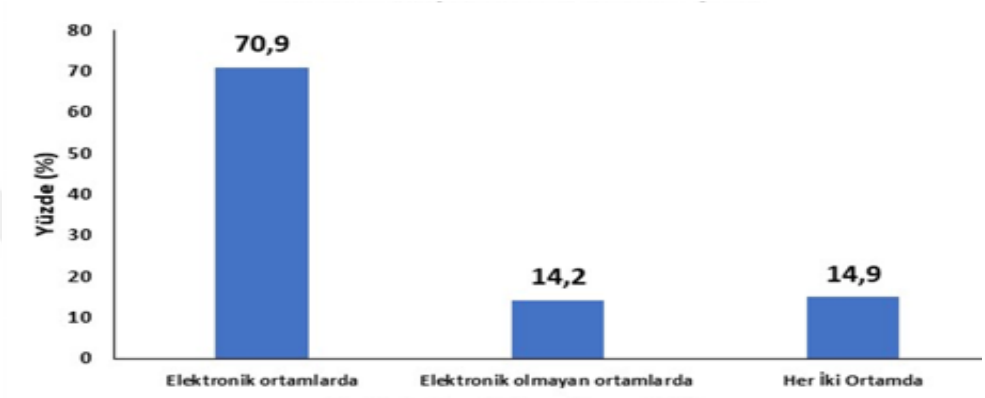
İşlenen verilere yönelik risklerin gerçekleşmesi halinde oluşacak zararlara ilişkin çalışma yapılıp yapılmadığı sorusuna katılımcıların, %32,8'i (n:150) bir çalışma yapılmadığını, %38,1'i (n:174) çalışma yapılması konusunda bir fikri olmadığını, %29,1'i (n:133) ise ortaya çıkabilecek zararlar konusunda çalışma yapıldığını belirtmiştir. Tablo 35'de bulgulara yer verilmiştir. Veri, bir işletmenin can damarıdır ve değerlidir. Veriye yetkisiz kişi/kişilerin erişimi halinde firma iş süreçlerinin aksaması ile birlikte güvenirliğinin zedelenmesi ve itibar kaybı şeklinde diğer zararlar oluşması mümkündür. Tüm bu olumsuzlukların önlenebilmesi için, verilere yönelik risklerin tespiti ile gerçekleşmesi halinde oluşacak zararların öncesinde belirlenerek tedbir alınması için çalışmalar yapılmalıdır.

Tablo 36. Şirket Verilerinin Kayıt Altına Alınması

Veriler Elektronik Ortamlarda mı, Yoksa Elektronik Olmayan Ortamlarda mı Kayıt Altına Alınmaktadır?		
Yanıtlar	n	%
Elektronik Ortamlarda	324	70,9
Elektronik Olmayan Ortamlarda	65	14,2
Her İki Ortamda	68	14,9
Toplam	**457**	**100**

Tablo 36'da yer verilen bulgulara göre, veriler yoğun olarak dijital ortamlarda kayıt edilerek depolanmaktadır. Bu durum, dijitalleşmenin doğal bir sonucudur. Katılımcıların %70,9'u (n:324) şirket verilerinin elektronik ortamlarda kayıt altına alındığını ifade etmiştir. %14,2'si (n:65) elektronik olmayan ortamlarda kayıtlı olup saklandığını ve

%14,9'u da (n:68) her iki ortamda da kayıt altına alındığını belirtmiştir. Bulgulara Şekil 16'da yer verilmiştir. Mevzuat gereği, belirli süreler ile fiziki ortamlarda (elektronik olmayan) saklanması gereken bilgi ve belgeler bulunmaktadır. Elektronik ortamda kayıtlı olsa da bazı verilerin orjinallerinin fiziki olarak saklanması gerekir. Benzer şekilde, bazı hallerde verilerin (ürün formülü gibi), firma için önemine bağlı olarak, elektronik ortamlarda saklanması uygun olmayabilir. Bu tür veriler, firmanın rakiplerine karşı sahip olduğu ticari sırlardır, önem ve risk derecesi yüksektir.



Şekil 16. Şirket Verilerinin Kayıt Altına Alınma Şekline Göre Dağılımı

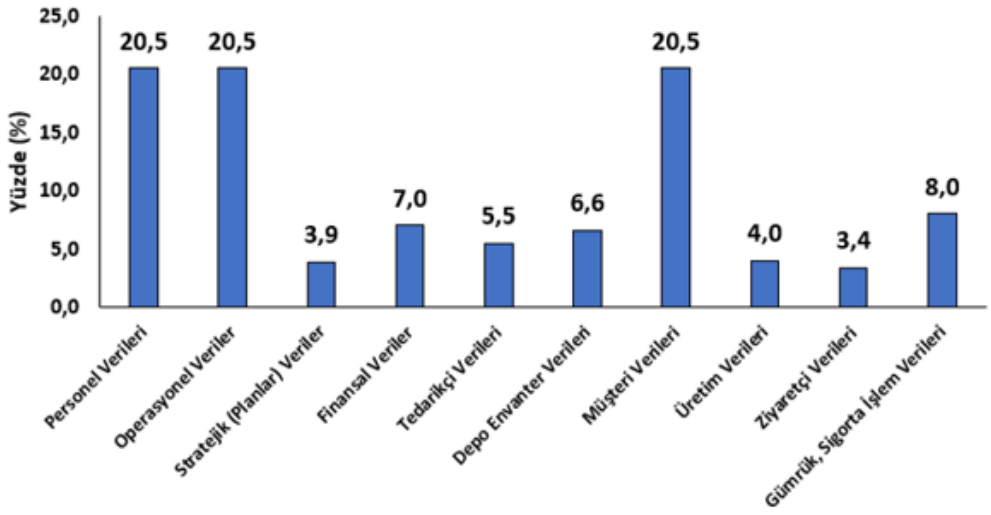
Tablo 37. Şirketin Kayıt Altına Aldığı Veri Türleri

Şirketinizde Hangi Türden Veriler Kayıt Edilmektedir?		
Yanıtlar	n	%
Personel Verileri	457	20,5
Operasyonel Veriler	457	20,5
Stratejik (Planlar) Veriler	88	3,9
Finansal Veriler	155	7,0
Tedarikçi Verileri	123	5,5
Depo Envanter Verileri	147	6,6
Müşteri Verileri	457	20,5
Üretim Verileri	89	4,0
Ziyaretçi Verileri	76	3,4
Gümrük, Sigorta İşlem Verileri	179	8,0
Toplam	**2228**	**100,0**

#Çoklu yanıt verildiğinden cevaplayıcı sayısı örneklem sayısını geçebilir.

Tablo 37 ile katılımcılara, faaliyetlerinde hangi türden verileri kayıt altına aldıkları sorulmuş elde edilen bulgularda, personel verileri ile operasyonel ve müşteri verilerinin yoğun olarak %20,5 oranı ile kayıt edildiği belirlenmiştir. Bu verileri değişen oranlarda olmak üzere, gümrük, sigorta ve finansal veriler ile tedarikçi, depo ve ziyaretçi verileri

takip etmektedir. Üretim bilgileri ile stratejik bilgiler de kayıt altına alınan verilerdendir. Genellikle büyük çaplı imalatçı firmalar lojistik işlemlerini kendileri gerçekleştirmekte ve lojistik faaliyetlerini üretim faaliyetleriyle bütünleşik yapıda gerçekleştirmektedir. Bulgular genel itibariyle, lojistik işletmelerinin sunduğu hizmetlere ilişkin veri türlerini kapsayıcı niteliktedir. Şekil 17'de bulgulara yer verilmiştir.



Şekil 17. Kayıt Altına Alınan Veri Türleri

Tablo 38. Mobil Ağa Bağlı Cihaz Veri Envanteri

Şirketiniz Mobil Ağına Bağlı Olan Cihaz ve Sistemlerin Veri Envanteri Çıkarılmış mıdır?		
Yanıtlar	n	%
Evet	131	28,7
Hayır	108	23,6
Fikrim Yok	112	24,5
Mobil Ağa Bağlı Cihaz ve Sistemimiz Yok	106	23,2
Toplam	**457**	**100**

Mobil ağa bağlı cihaz ve sistemlerin veri envanterine ilişkin Tablo 38' de yer alan bulgularda, katılımcıların %28,7'si evet mobil ağa bağlı cihaz ve sistemlerin veri envanteri bulunmaktadır derken, %23,6'sı hayır, %24,5'i bir fikri olmadığını ve %23,2'si de mobil ağa bağlı cihaz ve sistemleri olmadığını ifade etmiştir.

4.5.1.3 Bilgi güvenliği yönetim sistemine ilişkin bulgular

Bu bölümde anket katılımcısı lojistik şirketlerin Bilgi Güvenliği Yönetim Sistemi uygulamaları, düzenlemeleri ve farkındalıklarına ilişkin bulgulara yer verilmiştir.

Tablo 39. ISO 27001 BGYS Hakkında Bilgi Durumu

ISO 27001 Bilgi Güvenliği Yönetim Sistemi Hakkında Bilginiz Var mıdır?		
Yanıtlar	n	%
Evet	182	39,8
Hayır	144	31,5
Fikrim Yok	131	28,7
Toplam	**457**	**100**

Katılımcılara, ISO 27001 bilgi güvenliği yönetim sistemi hakkında bilgileri olup olmadığı sorulduğunda Tablo 39'da yer verilen cevaplarda, %39,8'i (n:182) bilgisi olduğunu ifade etmiş, diğer taraftan katılımcıların %31,5'i (n:144) bilgi sahibi olmadığını belirtmiştir. %28,7'sinin (n:131) ise bir fikri olmadığı belirlenmiştir.

Tablo 40. Şirketin ISO 27001 BGYS Belgesine Sahip Olma Durumu

Şirketinizin ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi Bulunmakta mıdır?		
Yanıtlar	n	%
Evet	128	28,0
Hayır	119	26,0
Fikrim Yok	210	46,0
Toplam	**457**	**100,0**

Tablo 40'da ki sonuçlara göre, araştırmaya dahil olan katılımcı şirketlerin %28,0'ında (n:128) ISO 27001 BGYS belgesi bulunurken, %26,0'ında (n:119) bu belge mevcut değildir ve %46,0'nın (n:210) konuya ilişkin fikirleri bulunmadığı belirlenmiştir. ISO 27001 bilgi güvenliği yönetim sistemi sertifikası olan şirketler, verilerini kaydetmiş oldukları müşteri, paydaş, çalışan gibi gruplara, kaydedilen bilgilerinin güvende olduğu, korunduğu ve önemsendiği mesajını vermektedir. Bilgi güvenliğini tüm yönleriyle (teknik, idari, hukuki, eğitim) sağladıklarını kabul etmektedirler. ISO 27001 belgesine sahip olan firmaların, bilgi güvenliğine ilişkin politikaları bulunmaktadır, personelleri bilgi güvenliği konusunda eğitimli ve bilinçlidir, şirket üst yönetiminden başlamak üzere, tüm personel hukuki sorumluluklarının farkındadır.

Bilgi güvenliğinin sağlanmasında, şirket üst yönetiminin bilgi sahibi olması ve kararlar almasının büyük önemi bulunmaktadır. Yönetim, güvenliğin sağlanmasına ilişkin olarak

karar almalı ve bütçe ayırmalıdır. ISO 27001 BGYS standart ana maddelerinde şirket idarecilerine bu konuda sorumluluklar yüklenmiştir.

Tablo 41. Bilgi Güvenliğine İlişkin Yıllık Gider

Bilgi Güvenliğine Harcama Yapılan Yıllık Gider		
Yanıtlar	n	%
1 TL. - 50.000 TL.	77	16,8
50.001 TL. - 100.000 TL.	136	29,8
100.001 TL. - 500.000 TL.	89	19,5
500.001 TL. – 1.000.000 TL.	19	4,2
1.000.000 TL'den Fazla	17	3,7
Bir Giderimiz Bulunmamaktadır	119	26
Toplam	**457**	**100**

Katılımcılara, bilgi güvenliğine yapılan yıllık harcama giderleri sorulmuş Tablo 41'de gösterilen elde edilen bulgularda, büyük çoğunluğunun, %29,8 (n:136) ile yıllık olarak 50.001 TL-100.000 TL arasında ve %19,5 (n:89) ile yıllık 100.001 TL-500.000 TL arasında bilgi güvenliğine ilişkin giderleri olduğu belirlenmiştir. Diğer %16,8'nin (n:77) 1 TL-50.000 TL. arasında bir gideri olduğunu, %26'lık (n:119) kesim ise bilgi güvenliğine dair bir gideri bulunmadığını ifade etmiştir. Bir tüzel kişiliğin, yasal zorunluluk bulunmasına ve risklere karşın, bilgi güvenliğine dair bir giderinin bulunmamasının değişik sebepleri olabilir. Ekonomik sebepler, bilgi sahibi olmama, önemli bulmama şeklinde örnekleri saymak mümkündür. Ayrılacak bütçe miktarı, şirketin büyüklüğüne, işlenen verinin çeşit ve sayısı gibi faktörlere göre değişiklik gösterebilecektir.

Bilgi güvenliğinin sağlanabilmesi için şirket üst yönetiminin desteği yanında süreci yönetecek ekibin oluşturulması da önemlidir. 2020 yılı Türkiye Siber Risk Algı Araştırması Raporu'nda; "*Her şirkette bir Siber Güvenlik Komitesi kurulması, bu komitenin insan kaynakları, operasyon, hukuk ve diğer iş birimlerinden yetkilileri barındırması"* gerekliliği belirtilmiştir (Marsh ve TÜSİAD, 2020, s. 29).

Tablo 42. Bilgi Güvenliği Kurul/Komisyon Varlığı ve Kurulu Oluşturan Birimler

Şirketinizde Bilgi Güvenliğinden Sorumlu Bir Kurul/Komisyon/Birim Bulunmakta mıdır?		
Yanıtlar	n	%
Evet	119	26,0
Hayır	183	40,0
Fikrim Yok	155	33,9
Toplam	**457**	**100,0**

Bilgi Güvenliği Kurul/Komisyon/Birimi Aşağıda ki Seçeneklerin Hangilerinden Oluşmaktadır?		
Yanıtlar	n	%
Teknoloji Birimi	13	10,9
Üst Yönetim	32	26,9
Hukuk Birimi	44	37,0
Bölüm Müdürleri	30	25,2
Toplam	**119**	**100**

Tablo 42 sonuçlarına göre, araştırmaya dahil olan katılımcı şirketlerin %26,0'ında bilgi güvenliğinden sorumlu bir kurul/komisyon/birimi bulunurken, %40'ında böyle bir birim olmadığı ve %33,9'unun ise konuya dair bir fikri olmadığı belirlenmiştir. Aynı tabloda, araştırmaya katılan, bilgi güvenliğinden sorumlu bir kurul/komisyon/birim sahibi olanların komisyonlarının, %10.9'unun teknoloji birimi, %26,9'unun üst yönetim, %37'sinin hukuk birimi ve %25,2'sinin bölüm müdürlerinden oluştuğu belirlenmiştir. Bilgi güvenliği komisyonunu oluşturacak temsilci birimler, şirketin büyüklüğüne, yapılanmasına bağlı olarak farklılık gösterebilecektir.

Tablo 43. Personele Bilgi Güvenliğine İlişkin Eğitim Verilme Durumu

Çalışanlara Veriler ve Bilgi Güvenliğine İlişkin Teknik, İdari ve Yasal Hak ve Yükümlülükler Eğitim Verildi mi?		
Yanıtlar	n	%
Evet	131	28,7
Hayır	161	35,2
Fikrim Yok	165	36,1
Toplam	**457**	**100**

Bilgi güvenliği konusunda şirket çalışanlarına eğitimler düzenlenmesine ilişkin Tablo 43'de yer verilen bulgularda katılımcıların, %28,7'si şirketlerinde çalışanlarına eğitim verildiğini belirtmiş, %35,2'si ise böyle bir eğitim verilmediğini ifade etmiştir.

%36,1'inin ise bir fikri olmadığı belirlenmiştir. Bilgi güvenliğinin sağlanmasından tüm personel sorumludur. Personele verilecek eğitimler ile çalışanlarda haklar ve sorumluluklara ilişkin farkındalık geliştirilmesi mümkündür.

ISO 27001:2022 BGYS uygulayan kuruluşlar, standardın 7.2 maddesi gereğince, çalışanlarının bilgi güvenliğine ilişkin yeterliliklerini belirlemekle sorumludur. Gerekli yeterliliğin sağlanması için tecrübeli çalışan istihdam edebileceği gibi, çalışanları için girişimlerde bulunarak, onlara eğitim verilmesi, rehberlik edilmesi şeklinde faaliyetler ile bilinçlenmelerini temin edecektir. Standardın kontrol maddeleri 6.3'de bilgi güvenliği farkındalığı, eğitim ve öğretim konularına yer verilmiştir.

"ISO 27001:2022 Ek-A Maddeleri

6.3: Bilgi güvenliği farkındalığı, eğitim ve öğretim

Kuruluşun personeli ve bağıntılı ilgili taraflar, iş işlevleriyle ilgili olarak, uygun bilgi güvenliği farkındalığı, eğitim ve öğretim ve kuruluşun bilgi güvenliği politikası, konuya özgü politikalar ve prosedürler hakkında düzenli güncellemeler almalıdır" (ISO 27001, 2022).

Tablo 44. ISO 27001 BGYS'nin Şirkete Olumlu Etkileri

ISO 27001 BGYS Belgesine Sahip Olmanın Firmanıza Hangi Açılardan Olumlu Etkileri Olduğunu Düşünüyorsunuz?		
Yanıtlar	n	%
Veriler Koruma Altında Olduğundan Müşteri Güveni Artmıştır	128	33,3
Ticari Rekabete Olumlu Etkisi Bulunmaktadır	48	12,5
ISO 27001 BGYS Belgesi, Firmamızın Tercih Edilmesinde Etkilidir	39	10,2
Ticari İtibarımıza Olumlu Etkisi Bulunmaktadır.	38	9,9
Veri İhlalinden Oluşabilecek Maddi Zararlara Engel Olmaktadır	58	15,1
Hukuki Yükümlülüklere Uyumu Sağlamaktadır	42	10,9
Veri İhlallerine Karşı Koruma Sağlamaktadır	31	8,1
Toplam	**384**	**100,0**

Katılımcılara, ISO 27001 BGYS belgesine sahip olmanın firmalarına etkileri sorulduğunda Tablo 44'de yer alan bulgularda, %33,3'ü, bilgiler koruma altında olduğundan müşteri güvenini artırıcı faydası olduğu ifade edilmiştir. Bunu %15,1'lik oran ile veri ihlalinden oluşabilecek maddi zararlara engel olduğu cevabı takip etmiştir. Devamla, %12,5'ine göre ticari rekabete olumlu etkisi bulunduğu, %9,9'una göre ticari itibarlarına olumlu etkisi bulunduğunu, %10,9'una göre hukuki yükümlülüklere uyumu

sağladığı, %10,2'sine göre ISO 27001 BGYS belgesi, firmanın tercih edilmesinde etkili olduğu, ve %8,1'ine göre de veri ihlallerine karşı koruma sağladığı şeklinde faydaları olduğu belirtilmiştir. Akademik araştırmalar da Mirtsch, Kinne ve Blind (2021), ISO 27001 BGYS belgesine sahip olmanın firma tercihlerinde önemli olduğunu göstermektedir.

Tablo 45. Verilerin İşlenmesi, Saklanması Prosedür ve Politika Varlığı ile Denetim Durumu

Şirketinizdeki Verilerin İşlenmesi, Saklanması, Korunması ve İmhası Konusunda Prosedür ve Politikalar Belirlenmiş midir?		
Yanıtlar	n	%
Evet	68	14,9
Hayır	150	32,8
Fikrim Yok	239	52,3
Toplam	**457**	**100**

Şirketinizdeki Verilerin İşlenmesi, Saklanması ve Korunması Konusunda Denetimler Yapılmakta mıdır?		
Yanıtlar	n	%
Evet	136	29,8
Hayır	163	35,7
Fikrim Yok	158	34,6
Toplam	**457**	**100**

Araştırmaya dahil olan katılımcılara, bilgi güvenliğine ilişkin politikaların varlığına ilişkin olarak yöneltilen soruya verilen cevaplarda, %14,9'u (n:68) şirketlerinde verilerin saklanması, korunması, işlenmesi ve imhası konusunda prosedür ve politikaların belirlendiğini, diğer taraftan %32,8'i (n:150) politikaların belirlenmediğini ve %52,3'ü ise (n:239) konuya ilişkin fikri olmadığını belirtmiştir. Bulgulara Tablo 45'de yer verilmiştir. Aynı tabloda, işlemlerin denetlenmesine ilişkin soruya verilen cevaplarda ise, anket katılımcısı şirketlerin %29,8'inin verilerin işlenmesi, saklanması ve korunması konusunda denetimler yaptığı, %35,7'sinde bu denetimlerin yapılmadığı ve %34,6'sının konu hakkında fikri olmadığı belirlenmiştir.

ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi standardı, bilgi güvenliğine ilişkin politikaların hazırlanması ve tüm şirkete duyurulması yönünde düzenlemeler içermektedir. Politikaların, güncel ihtiyaç ve değişikliklere uygun olarak revize edilmeleri mümkündür. Anket bulgularına göre, katılımcı şirketlerin, verilerin

korunması, işlenmesi, imhası ve saklanması konusunda politikaların hazırlanması ve işlemlerin denetlenmesi bakımından yeterli oldukları söylenemeyecektir.

Tablo 46. Şirketin Bilgi Güvenliğine Yatırım Yapma Nedenleri

Şirketinizin Bilgi Güvenliğine Yatırım Yapmasının Temel Nedenleri Nelerdir?		
Yanıtlar	n	%
Sistemlerimizi Korumak	338	40,05
Çalışan, Tedarikçi, Müşteri ve Paydaşların Verilerini Korumak	121	14,34
Kanun ve Yönetmeliklere Uymak	122	14,45
Dolandırıcılık ve Hırsızlığı Önlemek	95	11,26
Ticari Sırları, Fikri Mülkiyeti ve Diğer Varlıkları (nakit gibi) Korumak	152	18,01
Kesintilerin Önlenmesi ve İş Sürekliliğinin Devamını Sağlamak	16	1,90
Toplam	**844**	**100,0**

#Çoklu yanıt verildiğinden cevaplayıcı sayısı örneklem sayısını geçebilir.

Anket katılımcılarının %40,05'ine göre (n:338) şirketlerinin bilgi güvenliğine yatırım yapmalarının temel nedeni sistemlerini korumak şeklinde olmuştur. %18,01'ine göre ticari sırları, fikri mülkiyeti ve diğer varlıkları (nakit gibi) korumak olduğu belirlenirken, %14,45'ine göre kanun ve yönetmenliklere uymak, %14,34'üne göre verileri korumak, %11,26'sına göre dolandırıcılık ve hırsızlığı önlemek olduğu belirlenmiştir. Son olarak %1,90'na göre kesintilerin önlenmesi ve iş sürekliliğinin devamını sağlamak üzere yatırım yaptıkları belirlenmiştir. Tablo 46'de bulgulara yer verilmiştir. Katılımcı şirketlerin genel itibariyle sistemlerini korumak üzere bilgi güvenliğine yatırım yapmış olmaları farkındalıkları bakımından önemlidir. Ancak, veri ihlali, sadece sistemlere izinsiz erişimle sınırlı değildir. Fiziki ortam güvenliğinin de sağlanması, idari, hukuki ve insan kaynaklarına ilişkin önlemlerin birlikte alınması önemlidir. Diğer taraftan özellikle ticari sırlar bir kurumu rakip firmalar karşısında üstün kılan önemli verilerdir ve özenle korunması gerekir. Katılımcıların %1,90'nı kesintilerin önlenmesi ve iş sürekliliğinin devamını sağlamak üzere bilgi güvenliğine yatırım yaptıklarını belirtmiştir. İş sürekliliğinin kesintisiz devamı her işletme için önemlidir. Ancak bilgi akışının mal akışı kadar önemli olduğu lojistik sektörü açısından kesintisiz bilgi akışı ile iş sürekliliğini sürdürmek, tedarik zincirlerinde yaşanabilecek aksaklıkları önlemek bakımından oldukça önemlidir.

4.5.1.4 Veri ihlaline ilişkin bulgular

Anketin 4. bölümünde katılımcılara veri ihlali ile ilgili sorular yöneltilmiştir.

Tablo 47. Veri İhlali Hakkında Bilgi ve Veri İhlali Yaşanması

Veri İhlali Hakkında Bilginiz Var mıdır?		
Yanıtlar	n	%
Evet	131	28,7
Hayır	159	34,8
Fikrim Yok	167	36,5
Toplam	**457**	**100**

Şirketinizde Veri İhlali Yaşandı mı?		
Yanıtlar	n	%
Evet	39	8,5
Hayır	205	44,9
Fikrim Yok	213	46,6
Toplam	**457**	**100**

Anket katılımcılarına veri ihlali ile ilgili bilgileri sorulduğunda, %34,8'i bilgilerinin olmadığını, %36,5'i ise fikri olmadığını ifade etmiştir. Kalan %28,7'si ise evet cevabı ile veri ihlali hakkında bilgilerinin olduğunu belirtmiştir. Tablo 47'de bulgulara yer verilmiştir.

Diğer taraftan katılımcılara, şirketlerinde veri ihlali yaşanıp yaşanmadığı sorulmuştur. Tablo 47'de gösterilen elde edilen bulgularda, katılımcıların %8,5'i şirketlerinin veri ihlali yaşadığını, %44,9'unun veri ihlali yaşamadığı ve %46,6'sının ise konuya ilişkin fikri olmadığı belirlenmiştir. Firmalar çoğu kez, veri ihlali yaşamış olsalarda, piyasadaki itibarlarının zedelenmemesi, müşteriler nezdinde oluşan güven ortamının sarsılmaması gibi sebeplerle ihlal olayını, dış çevre ile paylaşmamakta ve şirket içinde çözümlemeyi tercih etmektedir.

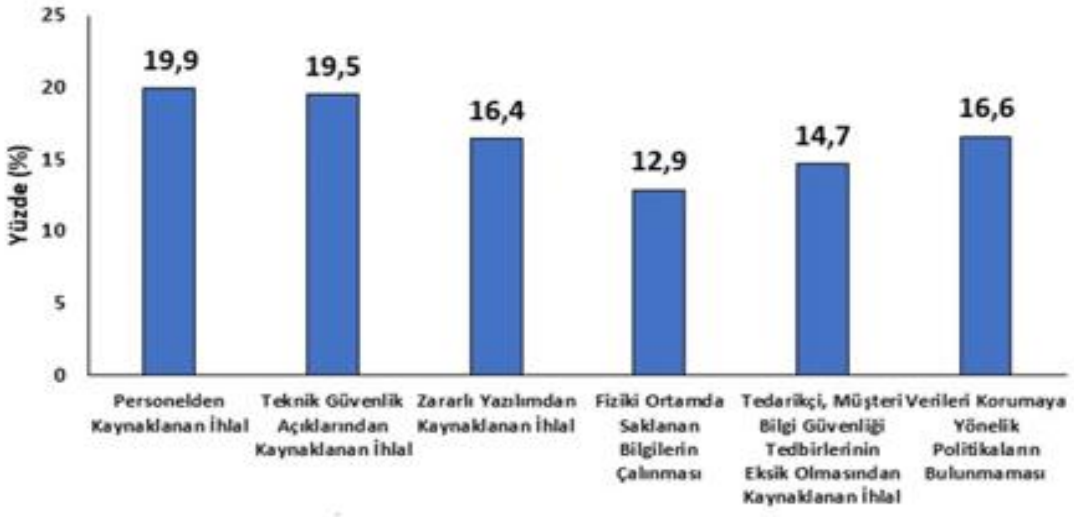
Tablo 48. Veri İhlali Sebepleri

Sizce Veri İhlalleri Aşağıdakilerden Hangileri Kaynaklı Olabilir?		
Yanıtlar	n	%
Personelden Kaynaklanan İhlal	91	19,9
Teknik Güvenlik Açıklarından Kaynaklanan İhlal	89	19,5
Zararlı Yazılımdan Kaynaklanan İhlal	75	16,4
Fiziki Ortamda Saklanan Bilgilerin Çalınması	59	12,9
Tedarikçi, Müşteri Bilgi Güvenliği Tedbirlerinin Eksik Olmasından Kaynaklanan İhlal	67	14,7
Verileri Korumaya Yönelik Politikaların Bulunmaması	76	16,6
Toplam	**457**	**100**

Ankete katılanlara, veri ihlali yaşanmasının sebepleri sorulmuştur. Tablo 48'de gösterilen elde edilen bulgularda, %19,9'u veri ihlallerinin sebebini personel kaynaklı olarak belirtmiştir. Bu sonuç verilen cevaplar içinde en büyük yüzdeye sahip sonuçtur. Çoğu ihlalin temelinde personelin ihmal ya da kasıtlı davranışı bulunmaktadır. İhmal, konu hakkında yeterli bilgi sahibi olmamaktan ya da söz konusu işi doğru yapmamaktan kaynaklanmakta iken kasıt ise bilerek ve isteyerek şirkete zarar verme eylemidir. Şekil 18'de bulgulara yer verilmiştir.

Katılımcıların %19,5'i teknik güvenlik açıklarından kaynaklı bir ihlal olabileceğini, %16,6'sı verileri korumaya yönelik politikaların bulunmamasından kaynaklı olabileceğini, %16,4'ü zararlı yazılımlardan kaynaklanan ihlal olabileceği, %12,9'u fiziki ortamda saklanan bilgilerin çalınması nedeniyle bir veri ihlali olabileceğini belirtilmiştir. %14,7'si ise tedarikçiden kaynaklı sebeplerle veri ihlali yaşanabileceğini ifade etmiştir.

Ernst ve Young (2024), Son beş yılda tehdit aktörlerinin en zayıf halka olarak gördükleri tedarik zincirlerini hedef aldığı görünüyor. Buna göre, günümüzde siber saldırganlar genel olarak tedarikçileri hedef almaktadır. Asıl hedefe ulaşmak için çoğu kez tedarikçiler kullanılmaktadır. Bu nedenle firmaların kendi iç güvenlikleri yanında, veri paylaşımında bulundukları tedarikçi ve iş ortaklarının da kendi bilgi güvenliklerini sağladıklarını araştırması, denetlemesi gerekir. Bu konu, özellikle Kişisel Verileri Koruma Kuruluna intikal eden veri ihlallerinde, özenle araştırılarak incelenmektedir.



Şekil 18. Veri İhlal Kaynakları

Personel kaynaklı veri ihlalleri işletmeler için ortak bir sorundur. Katılımcılara, çalışan kaynaklı veri ihlalleri için uygulanacak disiplin süreci hakkında çalışmalar yapılıp yapılmadığı sorulmuş, elde edilen bulgular Tablo 49'e göre, %22,8'i evet cevabını verirken, %40,9'u disiplin süreci belirlenmediğini, %36,3'ü ise bir fikri olmadığını belirtmiştir. Veri ihlalini önleyici tedbirler alınması esas olmak ile birlikte ihlal yaşanması halinde, sürecin ne şekilde yürütüleceği, uygulanacak prosedürler, personele uygulanacak disiplin ve cezalar hakkında düzenleme yapılmış olması da önemlidir.

Tablo 49. Personele Uygulanacak Disiplin Süreci, Tedarikçilere Uygulanacak Politikalar ve Veri İhlalinde İzlenecek Süreç-Eylem Planı Düzenlemeleri

Personel Kaynaklı Veri İhlalleri İçin Uygulanacak Disiplin Süreci Belirlenmiş midir?		
Yanıtlar	n	%
Evet	104	22,8
Hayır	187	40,9
Fikrim Yok	166	36,3
Toplam	**457**	**100**

Veri Sızıntısında Sorumluluğu Olan, Şirket Bilgi Güvenliği Prosedürlerine Uymayan Tedarikçi, İş Ortakları vb. Uygulanacak Yazılı Politikalar Bulunmakta mıdır?		
Yanıtlar	n	%
Evet	113	24,7
Hayır	163	35,7
Fikrim Yok	181	39,6
Toplam	**457**	**100**

Şirketinizde Veri İhlali Durumunda İzlenecek Süreçler ve Olaya Müdahale Yazılı Eylem Planı Oluşturulmuş mudur?		
Yanıtlar	n	%
Evet	150	32,8
Hayır	158	34,6
Fikrim Yok	149	32,6
Toplam	**457**	**100**

Aynı şekilde katılımcılara, veri ihlalinin oluşmasında tedarikçi ve iş ortaklarının sorumlu olması halinde uygulanacak politikaların bulunup bulunmadığı sorulduğunda, Tablo 49'a göre, katılımcıların %24,7'sinde uygulanacak yazılı politikaların hazır olduğu, %35,7'sinde böyle bir politika olmadığı ve %39,6'sının ise fikri olmadığı belirlenmiştir.

Katılımcılara bir veri ihlali yaşanması halinde izlenecek süreç ve olaylara müdahale eylem planlarının varlığı sorulmuştur. Aynı tabloda gösterilen elde edilen bulgularda katılımcıların %32,8'inin veri ihlali durumunda izlenecek süreçler ve olaya müdahale yazılı eylem planının bulunduğu, %34,6'sında ise bu hazırlığın olmadığı, %32,6'sının konu hakkında fikrinin olmadığı belirlenmiştir.

Bulgulara ilişkin olarak genel bir değerlendirme yapıldığında, lojistik işletmelerinin veri ihlali yaşanması halinde, izlenecek süreçlere ilişkin bir eylem planı olmadığı gibi, ihlale sebep olan kişi/kişiler hakkında uygulanacak prosedüre ilişkin de yeterli hazırlıklarının bulunmadığını söylemek mümkündür.

Tablo 50. Olası Veri İhlallerinin Zamanında Tespit Edilmesine İlişkin Prosedürlerin Varlığı

Olası Veri İhlallerinin Zamanında Tespit Edilebilmesine Yönelik Prosedürler Hazırlanmış mıdır?		
Yanıtlar	n	%
Evet	110	24,1
Hayır	171	37,4
Fikrim Yok	176	38,5
Toplam	**457**	**100**

Katılımcılara, veri ihlalleri yaşanmadan önce, zamanında tespit edilmesine yönelik hazırlıklarının olup olmadığı sorulmuştur. Tablo 50'de elde edilen bulgularda katılımcıların %24,1'inin şirketlerinde olası veri ihlallerinin zamanında tespit edilebilmesine yönelik prosedürler hazır iken, %37,4'ünde hazır olmadığı ve %38,5'inin ise konuya ilişkin fikrinin bulunmadığı belirlenmiştir.

Veri ihlalleri şirketler üzerinde olumsuz etkiler yaratabilmektedir. İş süreçlerinin aksaması ile maddi zararlar oluşabildiği gibi, itibar ve güven kaybı ile manevi zarara sebep olmaktadır. Ayrıca hukuki ve cezai müeyyideler ile karşılaşılması mümkündür.

Tablo 51. Veri İhlalinin Şirkete Etkisi

Şirketinizde Veri İhlali Yaşanır İse Bu Olayın Şirketinize Etkisi Aşağıdakilerden Hangisi Olabilir?		
Yanıtlar	n	%
Şirketin itibarını olumsuz etkilemez, fakat bilgi güvenliği organizasyon yapısını etkiler ya da personel değişikliği yapılır	82	17,9
Şirketin itibarı olumsuz etkilenir	88	19,3
Şirkete bir etkisi olmaz, şirket mevcut organizasyonunu ve itibarını devam ettirir	100	21,9
Şirkete idari para cezası, hukuki tazminat ve ceza yükümlülüğü getirebilir	85	18,6
Fikrim yok	102	22,3
Toplam	**457**	**100**

Araştırmaya dahil olan katılımcılara, veri ihlali yaşanması halinde bu durumun şirkete etkilerinin neler olabileceği sorulmuştur. Katılımcılar çoğunlukla %22,3 oranıyla bir fikri olmadığını belirtmiştir. %21,9'u şirkete bir etkisi olmayıp, şirketin mevcut organizasyonunu ve itibarını devam ettireceğini düşündükleri belirtilmiştir. %19,3'ü ise şirketin itibarının olumsuz etkileneceğini belirtmiştir. Tablo 51'de bulgulara yer verilmiştir. Bulgulara bakıldığında genel olarak, veri ihlalinin şirketin itibarını olumsuz yönde etkilemeyeceği düşünülmekte, hatta oluşturacağı etkiler ile ilgili fikir sahibi olmayan katılımcı sayısının da fazla olduğu görülmektedir.

4.5.1.5 Bilgi güvenliğine ilişkin tedbir ve yükümlülüklere ait bulgular

Anketin 5. bölümünde katılımcılara bilgi güvenliğine ilişkin tedbir ve yükümlülüklere yönelik sorular yöneltilmiştir.

Tablo 52. Şirket Verilerinin Korunmasından Yasal Sorumluluk Durumu

Şirket Verilerinin Korunmasından Yasal Olarak Sorumlu Olduğunuzu Düşünüyor musunuz?		
Yanıtlar	n	%
Evet	239	52,3
Hayır	116	25,4
Fikrim Yok	102	22,3
Toplam	**457**	**100**

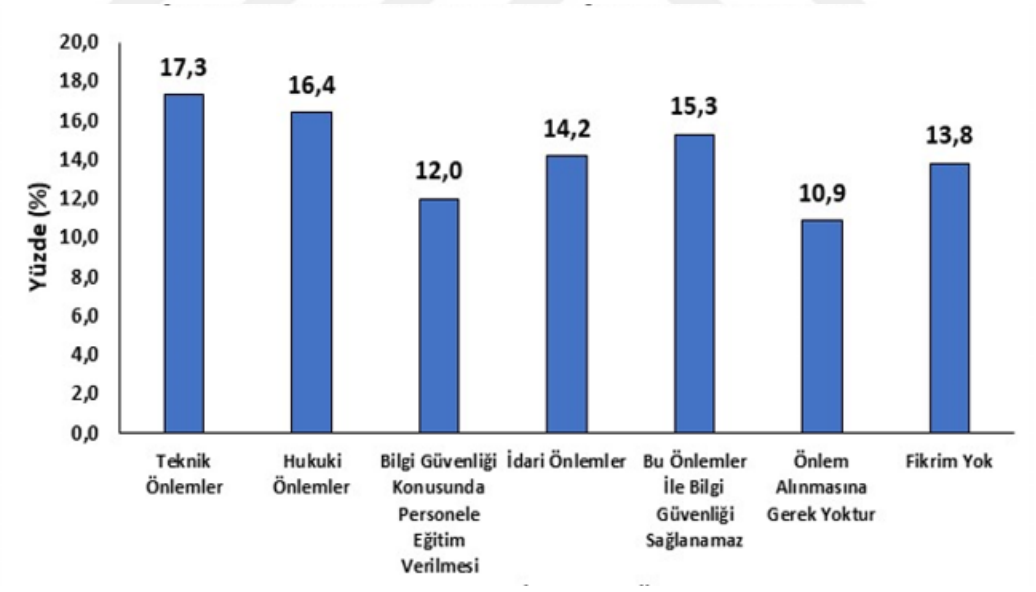
Araştırmaya dahil olan katılımcıların %52,3'ü (n:239) şirket verilerinin korunmasından yasal olarak sorumlu olduklarını belirtmiştir. %25,4'ü (n:116) soruya hayır cevabı vermiş ve %22,3'ünün (n:102) konu hakkında fikri olmadığı belirlenmiştir. Bulgular Tablo 52'de gösterilmiştir. Edinilen bulgular analiz edildiğinde, verilerin korunmasından yasal olarak sorumlu olunduğunun bilinmesi önemlidir, fakat bu tek başına yeterli değildir. Çünkü sorumluluğun eylemlerle somut hale getirilmesi, politikaların oluşturulması ve süreçler ile kuralların belirlenip uygulanması gerekmektedir.

Şirket verilerinin korunması amacıyla alınan önlemler ile bu önlemlerin nasıl uygulandığı da araştırılması gereken konulardandır. Tablo 53'de lojistik şirketlerin verilerin korunmasına ilişkin olarak almış oldukları önlemlere dair bulgulara yer verilmiştir.

Tablo 53. Şirket Verilerinin Korunması İçin Alınan Önlemler

Şirket Verilerinin Korunması İçin Aşağıdaki Önlemlerden Hangileri Alınmaktadır?		
Yanıtlar	n	%
Teknik Önlemler	79	17,3
Hukuki Önlemler	75	16,4
Bilgi Güvenliği Konusunda Personele Eğitim Verilmesi	55	12,0
İdari Önlemler	65	14,2
Bu Önlemler İle Bilgi Güvenliği Sağlanamaz	70	15,3
Önlem Alınmasına Gerek Yoktur	50	10,9
Fikrim Yok	63	13,8
Toplam	**457**	**100**

Alınan önlemlere ilişkin olarak verilen cevaplarda, katılımcıların %17,3'ü teknik önlemler aldıklarını, %16,4'ü hukuki önlem aldıklarını belirtmiştir, %14,2'si İdari önlem ve %12,0'ı personele eğitim verildiğini ifade etmiştir. Katılımcıların %15,3'ü bu önlemler ile bilgi güvenliğinin sağlanamayacağını ve %10,9 ise önlem alınmasına gerek bulunmadığını ve %13,8'inin alınan önlemler hakkında fikri olmadığı belirlenmiştir. Bulgulara Şekil 19'da yer verilmiştir.



Şekil 19. Verilerin Korunması İçin Alınan Önlemler

Tablo 54. Verilerin Korunması İçin Teknik Donanım ve Güvenlik Testlerinin Yapılması Durumu

Şirketiniz, Verilerin Korunması İçin Gerekli ve Yeterli Teknik Donanıma Sahip midir?		
Yanıtlar	n	%
Evet	180	39,4
Hayır	141	30,9
Fikrim Yok	136	29,8
Toplam	**457**	**100**

Cevabınız Evet ise, Teknik Donanımın Yedekleme, Bakım, Güncellemeleri ve Gerekli Güvenlik Testleri Düzenli Olarak Yapılmakta mıdır?		
Yanıtlar	n	%
Evet	84	46,7
Hayır	53	29,4
Fikrim Yok	43	23,9
Toplam	180	100

Tablo 54'de araştırmaya dahil olan katılımcıların %39,4'ünün, bilgilerin korunması için gerekli ve yeterli teknik ekipmana sahip oldukları belirlenirken, %30,9'unun sahip olmadığı ve %29,8'inin bu konuda bir fikri bulunmadığı belirlenmiştir. Tablonun ikinci bölümü incelendiğinde bilgilerin korunması için gerekli ve yeterli teknik ekipmana sahip olan katılımcıların %46,7'sinin yedekleme, bakım, güncelleme ve gerekli güvenlik testlerini düzenli olarak yaptıkları, %29,4'ünün bu işlemleri yapmadığı belirlenirken katılımcıların %23,9'unun ise konuya dair bir fikir beyan edemedikleri tespit edilmiştir. Sonuçlar değerlendirildiğinde, genel olarak bilgi güvenliğine ilişkin teknik önlemlerin alınarak bakım ve güncellenmelerinin yapıldığını söylemek mümkündür. Tedarik zinciri içerisinde çok sayıda lojistik faaliyet yürütüldüğünden tüm firmaların güvenlik tedbirlerini almış olması önemlidir. Ancak bu genel olarak mümkün olmamaktadır. Bu sebeple firmaların teknik tedbirlerini alarak gerekli kontrol ve testleri düzenli ve sık aralıklarla yapıyor olması gerekir.

Katılımcılara, verilerin korunmasına ilişkin mevcut düzenlemeleri ile yetki ve sorumlulukların aktarılmasına ilişkin planları, "Fiziki Ortamların" güvenliğinden sorumlu kişilerin belirlenmesi, "Fiziki Ortamların" hırsızlık, yangın, deprem vb. karşı korunması, kişisel ve tüzel kişi verilerinin muhafaza edildiği "Fiziki Ortamlara" erişebilecek ve "Bilgisayarlara" erişebilecek sorumlu kişilerin belirlenmesine ilişkin

düzenlemelerinin varlığıyla ilgili sorular sorulmuştur. Tablo 55'de bulgulara yer verilmiştir.

Tablo 55. Verilerin Korunmasına İlişkin Düzenlemeler, Sorumlulukların Paylaşılması Durumu

Verilerin Muhafaza Edildiği "Fiziki Ortamların" Hırsızlık, Sel, Yangın, Deprem vb. Olaylarına Karşı Korunma Önlemleri Alınmış mıdır?

Yanıtlar	n	%
Evet	178	38,9
Hayır	.....	.....
Fikrim Yok	279	61,1
Toplam	**457**	**100**

Verilerin Muhafaza Edildiği "Fiziki Ortamların" (Kasa, Kilitli Dolap, Sunucu, Sistem Odaları vb.) Güvenliğinden Sorumlu Kişiler Belirlenmiş midir?

Yanıtlar	n	%
Evet	70	15,3
Hayır	213	46,6
Fikrim Yok	174	38,1
Toplam	**457**	**100**

Kişisel ve Tüzel Kişi Verilerinin Kaydedildiği "Bilgisayarlara" Erişebilecek Sorumlu Kişiler Belirlenerek, Yetkilendirme Prosedürleri Hazırlanmış mıdır?

Yanıtlar	n	%
Evet	70	15,3
Hayır	168	36,8
Fikrim Yok	219	47,9
Toplam	**457**	**100**

Kişisel ve Tüzel Kişi Verilerinin Muhafaza Edildiği "Fiziki Ortamlara" Erişebilecek Sorumlu Kişiler Belirlenmiş Midir?

Yanıtlar	n	%
Evet	113	24,7
Hayır	283	61,9
Fikrim Yok	61	13,3
Toplam	**457**	**100**

Tablo 55'ün ilk sırasında yer alan, verilerin muhafaza edildiği fiziki ortamların, yangın, sel, deprem, hırsızlık gibi olaylara karşı korunma önlemi alınıp alınmadığına ilişkin soruya, araştırmaya dahil olan katılımcıların %38,9'u korunma önlemlerinin alındığını belirtirken, %61,1'i ise bir fikri bulunmadığını ifade etmiştir.

Tablonun ikinci sırasındaki soruya verilen cevaplara bakıldığında ise, şirketlerin %15,3'ü verilerin muhafaza edildiği "fiziki ortamların" (kasa, kilitli dolap, sunucu, sistem odaları

vb) güvenliğinden sorumlu kişilerin belirlendiğini, %46,6'sı ise belirlenmediğini ifade ederken, katılımcıların %38,1'inin bir fikirlerinin bulunmadığı görülmektedir.

Tablonun üçüncü sırasındaki soruya verilen cevaplara bakıldığında ise, şirketlerin %15,3'ünde kişisel ve tüzel kişi verilerinin kaydedildiği "bilgisayarlara" erişebilecek sorumlu kişilerin belirlenerek, yetkilendirme prosedürlerinin hazırlandığı belirlenmişken, %36,8'inde belirlenmediği ve katılımcıların %47,9'unun ise bir fikirlerinin bulunmadığı tespit edilmiştir.

Son sırada bulunan soruya verilen yanıtlarda ise, katılımcıların %24,7'sinde kişisel ve tüzel kişi verilerinin muhafaza edildiği "fiziki ortamlara" erişebilecek sorumlu kişiler belirlenmişken %61,9'unda sorumlu kişilerin belirlenmediği ve katılımcıların %13,3'ünün bir fikirlerinin bulunmadığı belirlenmiştir.

Bulgular değerlendirildiğinde, lojistik şirketlerin, bilgi ve ortamlara erişebilecek yetkili ve sorumlu kişilerin belirlenmesinde yetersiz kaldıkları görülmektedir. Bilgi güvenliği, tüm tedbirlerin birlikte alınması ve uygulanması ile sağlanabilir. ISO 27001 ana maddeler 5.3 maddesinde "*Üst yönetim, bilgi güvenliği ile ilgili roller için sorumlulukların ve yetkilerin atanmasını (belirlenmesini) ve kuruluş içinde duyurulmasını sağlamalıdır"* düzenlemesi ile üst yönetim tarafından alınması gereken yetkilendirme tedbirleri belirtilmiştir (ISO/IEC, 2022). Şirket içinde verilerin korunmasına yönelik yetkilendirme ve sorumluluk dağılımının yapılmamasından kaynaklanan ihtilaflara ilişkin yargı kararları bulunmaktadır.

Tablo 56. Bilgi Güvenliği İçin Şirket Üst Yönetiminin Desteği

Bilgi Güvenliğinin Sağlanması Konusunda Şirket Üst Yönetimi Destek Olmakta mıdır?		
Yanıtlar	n	%
Evet	32	7,0
Hayır	347	75,9
Fikrim Yok	78	17,1
Toplam	**457**	**100**

Tüzel kişilerde bilgi güvenliğinin sağlanması, şirket üst yönetiminin alacağı karar ve bütçe ayırarak destek olması ile mümkün olabilir. Katılımcılara, şirket idarecilerinin bilgi güvenliğinin sağlanması konusunda destek olup olmadıkları sorulmuştur. Tablo 56'da katılımcı cevaplarına yer verilmiştir. Buna göre, katılımcı şirketlerin %7,0'ında bilgi

güvenliğinin sağlanması konusunda şirket üst yönetimi destek olurken, %75,9'unda destek olmadığı ve katılımcıların %17,1'inin bu konuya ilişkin fikirlerinin bulunmadığı belirlenmiştir.

Tablo 57. Yurt Dışına Kişisel Veri Aktarımına İlişkin Düzenlemelerin Varlığı

Şirketinizde Yurt Dışı ile İşlem Yapılıyor ise, Yurt Dışına Kişisel Veri Aktarımı Konusunda Yazılı Düzenlemeler Yapılmış mıdır?		
Yanıtlar	n	%
Evet	78	41,3
Hayır	56	29,6
Fikrim Yok	55	29,1
Toplam	**189**	**100**

Tablo 57 incelendiğinde, yurt dışı ile işlem yapan şirketlerin %41,3'ünün yurt dışına kişisel veri gönderimi ile ilgili olarak yazılı düzenlemelerini yaptığı, %29,6'sının bu düzenlemeleri yapmadığı ve katılımcıların %29,1'inin konuya ilişkin fikir beyan edemedikleri belirlenmiştir.

Tablo 58. Veri Paylaşılan İş Ortaklarının ISO 27001 BGYS Sahip Olmasının Önemi

Veri Paylaşımında Bulunduğunuz Tedarikçi, İş Ortakları gibi, ISO 27001 BGYS Belgesine Sahip Olması Şirketiniz İçin Önemli midir?		
Yanıtlar	n	%
Evet	162	35,4
Hayır	157	34,4
Fikrim Yok	138	30,2
Toplam	**457**	**100**

Anket katılımcılarına, tedarikçiler ile paydaşlarınızın ISO 27001 BGYS belgesine sahip olmasının önemli olup olmadığı sorulmuştur. Bulgulara Tablo 58'de yer verilmiştir. Buna göre, şirketlerin %35,4'üne göre veri paylaşımında bulundukları tedarikçi, iş ortakları, hizmet alınan firmaların, ISO 27001 bilgi güvenliği yönetim sistemi belgesine sahip olması önemli iken, %34,4'üne göre önemli olmadığı ve katılımcıların %30,2'sinin bir fikrinin olmadığı belirlenmiştir.

Tedarik zinciri, çeşitli lojistik faaliyetlerden oluşur ve bu zincir içinde pek çok aktör bulunur ve çok sayıda veri paylaşımı yapılır. Bilgi paylaşımı yapılan tedarikçi, iş ortağı ve hizmet alınan firmaların bilgi güvenliğini sağlamış olmaları ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi belgesine sahip olmaları göz önünde bulundurulmalıdır. Tedarik zincirin herhangi bir noktasında meydana gelen bilgi kesintisi diğer halkaları da etkileyebileceğinden verilerin özenle korunması gerekir.

Tablo 59. ‘’Personel Sözleşmeleri" ve İş Ortakları İle Yapılan Sözleşmelerde’’ Bilgi Güvenliği Düzenlemelerine Yer Verilme Durumu

Şirket Çalışanlarınız ile" Aranızdaki Sözleşmelerde, Bilgi Güvenliği, Gizlilik ve Sır Saklama Yükümlülüğüne İlişkin Hükümlere Yer Verilmiş midir?		
Yanıtlar	n	%
Evet	182	39,8
Hayır	138	30,2
Fikrim Yok	137	30,0
Toplam	**457**	**100,0**

Tedarikçi ve İş Ortaklarınız ile Aranızda ki Sözleşmelerde Bilgi Güvenliği, Gizlilik ve Sır Saklama Yükümlülüğüne İlişkin Hükümlere Yer Verilmiş midir?		
Yanıtlar	n	%
Evet	89	19,5
Hayır	188	41,1
Fikrim Yok	180	39,4
Toplam	**457**	**100**

Bu bölümde anket katılımcılarına, personel ile birlikte tedarikçiler ve hizmet sağlayıcılar gibi üçüncü şahıslarla yapılan sözleşmelerde gizlilik, sır saklama ve bilgi güvenliği ile ilgili düzenlemelerin bulunup bulunmadığı sorulmuştur. Tablo 59’da yer verilen bulgularda, şirketlerin %39,8’i çalışanlarıyla aralarındaki sözleşmelerde, gizlilik, bilgi güvenliği ve sır saklama yükümlülüğü ile ilgili düzenlemeye yer verirken, %30,2’sinin yer vermediği ve katılımcıların %30,0’nın ise bu konuda fikirlerinin bulunmadığı belirlenmiştir. Tablonun ikinci bölümünde yer alan bulgularda da, şirketlerin %19,5’u tedarikçi ve iş ortakları ile aralarındaki sözleşmelerde gizlilik, bilgi güvenliği ve sır saklama yükümlülüğüne ilişkin hükümlere yer verirken, %41,1’inin yer vermediği ve katılımcıların %39,4’ünün ise fikirlerinin bulunmadığı belirlenmiştir.

Bulgular değerlendirildiğinde, firmaların tedarikçi, hizmet alınan firma gibi üçüncü kişiler ile arasındaki sözleşmelerde bu düzenlemelere yer vermemesi, lojistik işletmenin risk seviyesini artırdığı gibi, tedarik zincirini de olumsuz şekilde etkileyecek niteliktedir. Aynı şekilde personel ile arasındaki sözleşmelerde de bu düzenlemelere yer verilmesi önemlidir.

Tablo 60. Verilere Erişim Yetkisi Bulunan Personelin Görev Değişikliğinde Yapılacak İşlem Durumu

Verilere Erişim Yetkisi Bulunan Personelin Görev Değişikliği ya da İşten Ayrılması Halinde, Verilere Erişim Yetkileri İvedi Olarak Sonlandırılmakta mıdır?		
Yanıtlar	n	%
Evet	164	35,9
Hayır	144	31,5
Fikrim Yok	149	32,6
Toplam	**457**	**100**

Anket katılımcılarına, verilere erişim yetkisi verilen personelin işten ayrılması halinde uygulanacak prosedürlere ilişkin soru yöneltilmiştir. Tablo 60'da yer alan cevaplarda, katılımcıların %35,9'u, verilere erişim yetkisi bulunan personelin görev değişikliği ya da işten ayrılması halinde, erişim yetkilerinin ivedi olarak sonlandırıldığını, %31,5'inin ise yetkileri sonlandırmadığı ve katılımcıların %32,6'sının bu konuda fikirlerinin bulunmadığı belirlenmiştir.

Elde edilen bulgular değerlendirildiğinde, lojistik işletmelerinin ihtiyaç halinde personelin verilere erişim yetkisini sonlandırma konusunda çok fazla özen ve gayret gösterdikleri söylenemeyecektir. Verilen yetkinin ivedilikle sona erdirilmemesinin sonuçlarına ilişkin olarak, Kişisel Verileri Korunma Kurulu ve Yargıtay tarafından verilen kararlar bulunmaktadır.

> "(…)Şirketinde..çalışan sanığın işten çıkarılması üzerine şirkete ait ticari işletmenin işleyişine ilişkin özel belgeler olan ve ticari sır niteliğindeki formlarını(…) İşletmesine götürerek verdiği iddiasıyla sanık hakkında ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması suçundan kamu davası açıldığı ve mahkemece atılı suçtan sanığın mahkumiyetine karar verildiği anlaşılmıştır(…)" (Yargıtay 5.CD, 2023).

Benzer durum 3. kişi firmalar ile sonlandırılan iş ilişkisi akabinde, verilen yetkilerin ivedilikle sonlandırılmaması halinde de söz konusudur. "V*eri sorumlusunun, veri işleyenin muhafaza ettiği kişisel verilerin imhasına yönelik olarak aralarındaki ticari ilişkinin sonlanmasını müteakip gerekli girişimlerde bulunması gerekirken bunu ihlalden sonra yaptığı;(...)veri sorumlusunun veri işleyen ile ilişkilerin yönetimi noktasında özensiz davrandığı"* şeklindedir (Kişisel Verileri Koruma Kurulu Kararı, 2021).

Örnek kararlardan da anlaşıldığı üzere, gerekli hallerde, verilere erişim yetkilerinin derhal sona erdirilerek yetkisiz kişilerin şirket verilerine izinsiz erişimine engel olunması gerekmektedir.

Tablo 61. Verilerin Korunmasında İdari ve Hukuki Düzenlemeler ve Politika Uygulanmalarının Denetlenmesi, Teknik Destek Hizmet Alma Durumu

Şirketiniz, Verilerin Korunması Konusunda İdari ve Hukuki Düzenlemelere Sahip midir?

Yanıtlar	n	%
Evet	108	23,6
Hayır	223	48,8
Fikrim Yok	126	27,6
Toplam	**457**	**100**

Bilgi Güvenliğini Sağlamaya İlişkin Politika ve Prosedürlerin Şirket İçinde Tam Olarak Uygulandığı Denetlenmekte midir?

Yanıtlar	n	%
Evet	154	33,7
Hayır	135	29,5
Fikrim Yok	168	36,8
Toplam	**457**	**100**

Bilgi Güvenliği Konusunda Dışarıdan Teknik Destek Hizmeti (Bakım, Proje vs) Alıyor musunuz?

Yanıtlar	n	%
Evet	166	36,3
Hayır	127	27,8
Fikrim Yok	164	35,9
Toplam	**457**	**100**

Tablo 61 ilk bölüm sonuçları incelendiğinde, ankete katılan şirketlerin %23,6'sı verilerin korunması konusunda idari ve hukuki düzenlemelere sahipken, %48,8'inin sahip olmadığı ve %27,6'sının konu hakkında fikir beyan edemedikleri belirlenmiştir.

Aynı tablonun ikinci bölümünde araştırmaya katılanlara, şirket bilgi güvenliği politika uygulamalarının denetlenip denetlenmediği sorulmuştur. Katılımcıların %33,7'si bilgi güvenliğini sağlamaya ilişkin politika ve prosedürlerin şirket içinde uygulanmasının denetlendiğini, %29,5'i denetlemediğini ve %36,8'i fikirlerinin olmadığını belirtmiştir.

Firmalar çoğu zaman dijital sistemlerinin kurulumu, bakımı gibi konular için şirket dışı firmalardan teknik destek hizmeti alabilmektedir. Tablo 61 üçüncü bölümde, katılımcılara teknik destek hizmeti alıp almadıkları sorulduğunda, şirketlerin %36,3'ünün

bilgi güvenliği konusunda dışarıdan teknik destek hizmeti (bakım, proje vs) aldıkları, %27,8'inin destek almadıkları ve katılımcıların %35,9'unun konu hakkında fikir beyan edemedikleri belirlenmiştir. Gerçek ve tüzel kişiler ihtiyaç duyduklarında dış kaynak firmalardan destek alabilmektedirler. Burada göz önünde bulundurulması gereken nokta, teknik destek hizmeti sağlayan kuruluş veya çalışanlarının, hizmet alan tarafın verilerine zarar verme riskine karşı gerekli önlemlerin alınmış olmasıdır.

Tablo 62 ve Tablo 63'de, katılımcı şirketlerin yasal düzenlemeler çerçevesindeki sorumluluklarına ilişkin tespitlere yer verilmiştir.

Tablo 62. "Tüzel Kişi Veriler" ile İlgili Sorumluluğa İlişkin Yasal Düzenlemeler

Şirketinizde Kayıtlı "Tüzel Kişi Verileri" ile İlgili Hangi Yasal Düzenlemeler Gereğince Sorumlu Olduğunuzu Düşünüyorsunuz?		
Yanıtlar	n	%
Kişisel Verilerin Korunması Kanunu	457	43,6
Türk Ceza Kanunu	222	21,2
Sorumlu Olduğumu Düşünmüyorum	235	22,4
Türk Ticaret Kanunu	133	12,7
Toplam	**1047**	**100,0**

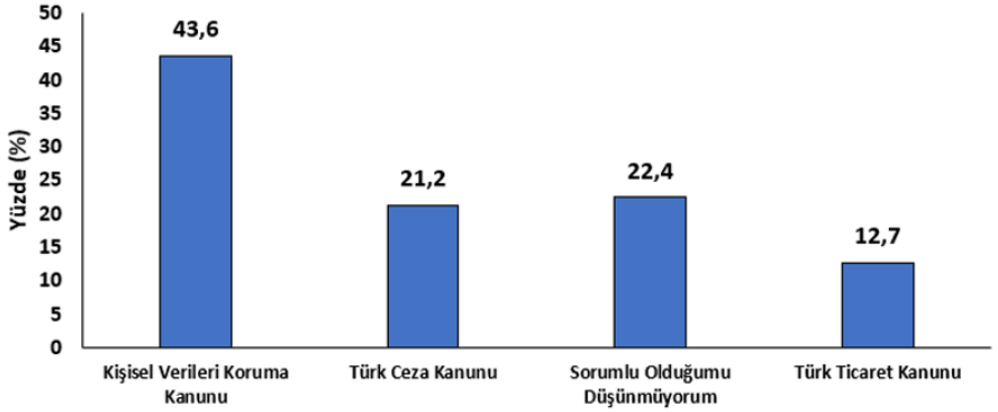
#Çoklu yanıt verildiğinden cevaplayıcı sayısı örneklem sayısını geçebilir.

Anket katılımcılarına, kayıt edilen tüzel kişi verileri ile ilgili hangi yasal düzenlemeler gereğince sorumlu olduklarına dair, çoktan seçmeli 6 seçenekli bir soru sorulmuştur. Elde edilen bulgular Tablo 62'de yer verilmiş olup buna göre, Tüzel kişi verilerinin korunmasıyla ilişkili olarak katılımcıların yarıya yakını Kişisel Verilerin Korunması Kanunu %43,6 ile, %21,2'si Türk Ceza Kanunu ile ve %12,7 ile Türk Ticaret Kanunu çerçevesinde sorumlu olduklarını düşünmektedir. %22,4'i ise yasal düzenlemeler gereğince sorumlu olduklarını düşünmediklerini belirtmiştir. Sonuçlara Şekil 20'de yer verilmiştir.

Bulgular değerlendirildiğinde dikkat edilmesi gereken nokta, katılımcıların %22,4'ünün tüzel kişi bilgilerinin korunmasına ilişkin hukuki düzenlemelerden sorumlu olmadığını düşünmesidir. Bunun çeşitli sebepleri olabilir. Şirket içi düzenlenecek eğitimlerle hak ve sorumluluklar konusunda farkındalık oluşturulması mümkündür.

Diğer taraftan, katılımcıların büyük bir kısmı, tüzel kişi verileri ile ilgili olarak Kişisel Verilerin Korunması Kanunu kapsamında sorumlu olduklarını belirtmişlerdir. Bu kanun, sadece gerçek kişi verilerini koruma altına alan düzenlemeler içermektedir. Halbuki tüzel

kişilerin, ticari sırlar ve diğer tüzel kişiliğe ilişkin verileri de bulunmaktadır. KVKK tüzel kişilerin bu türden verilerine uygulanmamaktadır. Özel bir düzenleme olan KVKK'nın katılımcılar tarafından bilinmesi ve kısmen de olsa Türk Ceza Kanunu ve Türk Ticaret Kanunu gereğince sorumluluğun farkında olunması, hukuk bilincinin oluşması ve farkındalık bakımından önemli bulunmuştur.



Şekil 20. Tüzel Kişi Verileri İle İlgili Sorumluluğa İlişkin Yasal Düzenleme

Tablo 63. "Kişisel Verilerin" İhlalinde Uygulanması Gereken Prosedür Durumu

"Kişisel Verilerin İhlal Edilmesi" Halinde Aşağıda Sayılanlardan Hangileri Yapılmalıdır?		
Yanıtlar	n	%
Kişisel Verileri Koruma Kuruluna Bildirimde Bulunma	457	65,4
Şirket Üst Yönetimine Haber Verme	242	34,6
Toplam	**699**	**100,0**

#Çoklu yanıt verildiğinden cevaplayıcı sayısı örneklem sayısını geçebilir.

Bu bölümde de kişisel verilerin ihlal edilmesi durumunda yapılması gereken idari ve yasal tedbirleri içeren çoktan seçmeli olarak 5 seçenekli bir soru sorulmuştur. Tablo 63'de bulgulara yer verilmiştir. Katılımcıların %65,4'ü kişisel verilerin ihlal edilmesi halinde kişisel verileri koruma kuruluna bildirimde bulunulması gerektiğini, %34,6'sı ise şirket üst yönetimine haber verilmesi gerektiğini belirtmişlerdir. Elde edilen bulgular, katılımcı firmaların kişisel verileri korumakla ilgili yasal düzenlemelerin farkında olduğunu göstermesi bakımından önemlidir.

5. BULGULAR VE TARTIŞMA

Bu bölümde, lojistik şirketlerine uygulanan anket sonucu edinilen bulgular; mevcut durum, yapılan uygulamalar, farkındalık ve hazırlanarak geliştirilecek bilgi güvenliği politikası bakımından değerlendirilerek analiz edilmiş, lojistik işletmelerin bilgi güvenliği riskleri ele alınmıştır. Ayrıca araştırma hipotezi bulguları ve çözümlenmesine yer verilmiştir.

5.1 Bilgi Güvenliği ve Risk Yönetimi

Veri güvenliğinin sağlanmasında güvenlik risk analizi oldukça önemlidir. Risk analizindeki amaç, firmanın işleyişindeki risk seviyesini düşürmektir. Bu analiz ile, firmaların karşılaşabileceği güvenlik riskleri çıkarılmakta, bilgi varlıklarına yönelik tehditler belirlenmekte, firmalar önceliklerini belirleyerek gerekli bilgi güvenliği önlemlerini zamanında alabilmektedir (Çek, 2017).

Firmalarda işlenen verilere ilişkin risk seviyelerinin belirlenebilmesi için öncelikle veri envanterinin (dijital ortamdaki veriler, basılı ve yazılı veriler gibi) oluşturulması, sınıflandırılması, önem düzeylerine göre detaylandırılması (az, orta ve çok önemli), kayıt altına alındığı ortamların ve kayıt edenlerin belirlenmesi gerekmektedir. Bu süreç, bilgi güvenliğinin en kritik aşamalarından biridir. İşletmelerin kayıt altına aldığı verilerin türünü, önem derecesini ve nerede muhafaza edildiğini bilmesi ve uygun önlemleri alması önemlidir. Bu süreç, veriye erişimi kontrol ederek, erişim izinlerini yönetmeyi ve ihlalleri önlemeyi amaçlar. Veri envanteri hazırlığı sürecinde, kişisel veriler ve işletmenin tüzel kişiliğe ilişkin verileri ayrı ayrı değerlendirilir. Veri kayıt süreci sürekli devam eden bir işlem olduğundan, gerekli güncellemelerin yapılması da büyük önem taşımaktadır.

Bilgi varlıkları belirlenip değerlendirilmesi yapıldıktan sonra risk değerlendirmesi yapılmalıdır. Böylece korunacak bilgi varlıklarına karar verilir, muhtemel riskler belirlenir. Bu işlemler sonrasında hazırlanan bilgi güvenliği politikası, belirlenen tehditlerin ne şekilde kontrol edileceğini göstermesi bakımından, risk yönetimi ile bilgi güvenliğini sağlama sürecinin önemli bir aşamasıdır. Riskler ancak, yasal düzenlemeler,

uluslararası standartlar ve bilgi güvenliği politikaları ile etkin şekilde yönetilebilecektir (Henkoğlu, 2015).

Bu süreçte, tüzel kişi verileri ile kişisel verilerin kayıt edildiği ve korunduğu alanlara yetkisiz kişilerin erişiminin engellenebilmesi için alınacak önlemler belirlenirken, verileri kaydeden ve muhafaza eden personelin eğitimi de önem taşımaktadır. Riskler belirlendikten sonra, riskin gerçekleşmesi durumunda karşılaşılabilecek zararlar konusunda da çalışma yapılmalıdır. Yaşanabilecek bir veri ihlali vakası karşısında olaylara ne şekilde müdahale edileceğini gösteren eylem planları da hazır olmalıdır. Bu sayede veri ihlali halinde hızlı ve etkili müdahale yapılabilecektir.

5.1.1 Lojistik şirketlerinde veri güvenliği ve risk yönetimine bakış

Literatür çalışmaları, siber saldırı riskinin sürekli olarak arttığını göstermektedir. Cheung, Bell ve Bhattacharjya (2021), internet tabanlı teknolojilerin benimsenmesi, lojistik ortamındaki saldırı yüzeyini artırmıştır. Bu durumda, zincirin tüm kademelerinde hizmet veren lojistik işletmelerinin, risk yönetimi konusunda hazırlıklı olmaları ve müşteri ile tedarikçilerin verilerini korumak üzere gerekli önlemleri almaları gerekir.

Lojistikte bilgi sistem güvenliğinin görevi, bilginin üç önemli unsuru olan gizliliğinin, bütünlüğünün, erişilebilirliğinin korunması, yok olmasının engellenmesidir. Firma çalışanlarının etkin davranışları lojistik bilgi sistem güvenliğinin sağlanmasında oldukça önemlidir. Bir lojistik firmada bilgi sistem güvenliği kültürünün oluşması için, lojistik bilgi güvenliği organizasyonunun varlığı, politikaların oluşturulması, sistemlerin fiziki ortam güvenliğinin sağlanması, erişim denetimlerinin yapılması ve veri ihlal süreç yönetiminin sağlanmış olması gerekir. Çalışanların bilgi güvenliğine uygun ve yapıcı hareketleri bilgi güvenliği etkinliğini artırır (Avci ve Karataş, 2017).

Türkiye'de bulunan lojistik işletmelerin bilgi güvenliği uygulamaları, firmalara uygulanan anket sonucu elde edilen bulgularla değerlendirilmiştir. Bu analize göre, katılımcı şirketlerin genel olarak veri güvenliği konusunda bilgilerinin bulunduğu, ancak pratikte alınan tedbirlerin genel olarak yeterli olmadığı belirlenmiştir.

Tablo 64. Risk Yönetimine İlişkin Sonuçlar

	EVET		HAYIR		FİKRİM YOK	
	N	*%*	*N*	*%*	*N*	*%*
Şirketinizin Veri Envanteri Bulunmakta mıdır?	*272*	*59,5*	*98*	*21,4*	*87*	*19,1*
Şirketinizde Kayıt Altına Alınan Veriler Risk ve Önemine Göre Gruplandırılmış mıdır?	*129*	*28,2*	*217*	*47,5*	*111*	*24,3*
Şirketinizde Kayıt Altına Alınan Verilere Yönelik Risklerin Gerçekleşmesi Halinde Ortaya Çıkabilecek Zararlar Konusunda Çalışma Yapılmış mıdır?	*133*	*29,1*	*150*	*32,8*	*174*	*38,1*

Tablo 64'ten anlaşıldığı üzere, firmaların genel olarak, kayıt altına aldıkları verilerin envanterini çıkardıkları tespit edilmiştir. Ancak, bu verilerin risk ve önemlerine göre gruplandırılma işlemlerinin çoğunlukla yapılmadığı belirlenmiştir. Katılımcılar bu soruya, %28,2 oranında evet cevabını verirken %47,5 hayır cevabını vermiş ve %24,3 ise fikri olmadığını belirtmiştir. Aynı şekilde, verilere yönelik risklerin gerçekleşmesi halinde ortaya çıkabilecek zararlara ilişkin olarak çalışma yapan şirket sayısının da yeterli olmadığı belirlenmiştir. Katılımcıların %29,1'i zararlar konusunda çalışma yapıldığını belirtirken, %32,8 çalışma yapılmadığını, %38,1 fikri olmadığını ifade etmiştir.

Avrupa Birliği Siber Güvenlik Ajansı (ENISA) tarafından, Ulaşım Alanına Yönelik Siber Tehdit raporu 21 Mart 2023 tarihinde yayınlanmıştır. Bu yeni rapor, 2021 Ocak ayından 2022 Ekim ayına kadar olan dönemi kapsayan havacılık, deniz, demiryolu ve karayolu taşımacılığı ile ilgili siber olayları analiz etmektedir. Rapor, ulaşım sektörünün siber tehditlerine ilişkin bilgiler vererek, birincil tehditlerin belirlenmesi ve olayların analizini içermektedir. Raporda, ulaştırmanın ekonomideki öneminden, kişisel ve profesyonel yaşantıda kilit bir sektör olduğundan sözedilmektedir. Taşımacılık sektörünü etkileyen başlıca tehditler şu şekilde sıralanmıştır;

> Fidye yazılımı saldırıları; verilerle ilgili tehditler; kötü amaçlı yazılım; kimlik avı; tedarik zinciri saldırıları şeklindedir. Fidye yazılımı saldırıları , 2021'de %13'ten, 2022'de %25'e çıkarak neredeyse ikiye katlanarak 2022'de sektöre yönelik en önemli tehdit haline gelmiştir(…).Siber suçlular kar amacıyla kimlik bilgilerini, çalışan ve müşteri verilerini ve fikri mülkiyeti hedeflemektedir. Karayolu sektöründeki tehditler ağırlıklı olarak fidye yazılımı saldırıları,

verilerle ilgili tehditler ve kötü amaçlı yazılımlardır. Otomotiv endüstrisi, tedarikçiler, üretim kesintilerine yol açan fidye yazılımlarının hedefi olmuştur(…)Verilerle ilgili tehditler, öncelikle müşteri ve çalışan verilerini ve özel bilgileri elde etmek için BT sistemlerini hedeflemektedir. Denizcilik sektörünü hedef alan tehditler arasında liman yetkililerine, liman operatörlerine ve üreticilere yönelik fidye yazılımları, kötü amaçlı yazılımlar ve kimlik avı saldırıları yer alır (Bilgi Teknolojileri ve İletişim Kurumu, 2023, s. 64-66).

5.2 Lojistik Şirketlerinde Veri Güvenliği Farkındalık ve Uygulamalar

1- Avrupa ülkelerinde şirketler, Genel Veri Koruma Tüzüğü (GDPR) kapsamında kişisel verilerin korunmasına ilişkin gizlilik politikalarına uymakla yükümlüdür ve bu verilere ilişkin bilgilere web sitelerinde yer vermektedir. Ülkemizde de Kişisel Verilerin Korunması Kanunu ile veri sorumlularına benzer yükümlülükler getirilmiştir. Ancak, yapılan analizde, incelenen lojistik işletmelerinin çoğunun web sitelerinde, kanunla ilgili düzenlemelere yer verilmediği belirlenmiştir.

Avrupa ülkelerinde lojistik işletmelerinin, tedarikçilerinden ISO 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasına sahip olmalarını talep ettiklerine dair akademik çalışmalar bulunmaktadır.

“Firmaların yalnızca kendilerinin bilgi güvenliği sertifikası aramadığını, aynı zamanda web sitelerinde bilgi güvenliği sertifikası olan ortaklara başvurduğunu göstermiştir. Sonuç olarak, daha büyük ve daha yenilikçi firmaların ISO/IEC 27001 sertifikası alma olasılığının daha yüksek olduğu gözlenmiştir” (Mirtsch, Kinne ve Blind, 2021).

Lojistik işletmeler ile yapılan anket çalışmasında, katılımcıların ISO 27001 Bilgi Güvenliği Yönetim Sistemine ilişkin bilgileri sorgulanmış ve edinilen bulgular Tablo 65’de gösterilmiştir. Buna göre, firmaların %39,8’i soruya evet cevabı verirken, %31,5 hayır cevabını vermiş, %28,7’ si ise bir fikri bulunmadığını belirtmiştir.

Tablo 65. ISO 27001 BGYS Hakkında Bilgi Sahibi Olunmasına İlişkin Sonuçlar

	EVET		HAYIR		FİKRİM YOK	
	N	*%*	*N*	*%*	*N*	*%*
ISO 27001 Bilgi Güvenliği Yönetim Sistemi Hakkında Bilginiz Var mıdır?	*182*	*39,8*	*144*	*31,5*	*131*	*28,7*

Bilgi güvenliği politikalarında amaç, bilgiyi koruyacak güvenlik önlemlerinin planlanması, bilinçlendirmenin sağlanarak zararlı girişimlerin engellenmesi ve iş birliğinin geliştirilerek veri ihlallerine karşı mücadele edilmesini sağlamaktır. Bilgi güvenliği politikasının uygulanabilir olması için, gerekli tüm önlemlerin alınması için yeterli bütçenin ayrılması, kullanıcıların bilgilendirilip bilinçlendirilmesinin sağlanması, ihtiyaç duyulan yasal düzenlemelerin yapılması gereklidir (Henkoğlu ve Yılmaz, 2013).

Şekil 21'de ankete katılan şirket ölçekleri (büyüklükleri) gösterilmiştir. Buna göre, katılanların %92,1 küçük ve orta ölçekli işletme olup kalan %7,9 luk oran ise büyük ölçekli işletmedir. Araştırmalara göre, küçük ve orta ölçekli işletmeler daha fazla sayıda siber saldırıya maruz kalmaktadır. Sektörün genellikle bu ölçekteki işletmelerden oluştuğu göz önüne alındığında, riskin de büyük olduğu söylenebilecektir.



Şekil 21. Araştırmaya Dahil Olan Şirketlerin Büyüklüğüne Göre Dağılımları

2-Anket katılımcısı firmalara, bünyelerinde bilgi güvenliğinden sorumlu bir birim olup olmadığı sorulduğunda Tablo 66, %40,0'ı hayır cevabı vererek bilgi güvenliğinden sorumlu birim bulunmadığını belirtmiş, %26,0'ı evet cevabı vermiştir. Yine katılımcılara, şirketlerinde, verilerin saklanması ve imhasına yönelik prosedür ve politikaların bulunup

bulunmadığı sorulduğunda %32,8'i hayır cevabını vermiş, %52,3'ü ise fikri olmadığını ifade etmiştir.

Diğer taraftan, 2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkındaki Yönetmelik gereğince veri sorumluları siciline kayıt olması zorunlu olan veri sorumlularının, veri saklama ve imha politikalarını hazırlama yükümlülüğü bulunmaktadır.

Ticari sırlar değişik türden saldırılar ile ele geçirilebilmektedir. Bunlar, kötüniyetli yazılımlar, sistemlere yetkisiz erişim, taşınabilir cihazlara siber saldırılar şeklinde olabilmektedir. İşletme sahipleri bilgi güvenliğine önem vermelidir. Bu itibarla, bilgi güvenliği konusundaki yasal ve teknik gelişmeler takip edilerek politikalar geliştirilmelidir (Yüksel, 2018).

ISO 27001 Bilgi Güvenliği Yönetim Sistemi'ni uygulayan firmalar, standart gerekliliklerine uygun olarak, bilgi güvenliğinden sorumlu birimleri oluşturmak, yetkilendirmeleri yapmak ve standart tarafından zorunlu görülen politikaları hazırlayıp uygulamak ve şirket çalışanlarına duyurmakla yükümlüdürler. Aynı şekilde, kişisel verilerin korunması yasası gereğince, kişisel verilerle ilgili benzer düzenlemelerin yapılması gerekli ve zorunludur.

Katılımcılara, verilerin korunması konusunda bilgi güvenliğine ilişkin eğitim verilip verilmediği sorulduğunda ise %28,7 evet cevabı verirken, %35,2'i hayır cevabını vermiş, %36,1 de fikri olmadığını belirtmiştir. Elde edilen bulgulara Tablo 66' da yer verilmiştir. Anket bulguları, eğitim çalışmalarının firmalar tarafından yeterli şekilde yapılmadığını ortaya koymaktadır.

Tablo 66. Bilgi Güvenliği Politikalar, Eğitim ve Kurul/Komisyon Varlığına İlişkin Sonuçlar

	EVET		HAYIR		FİKRİM YOK	
	N	*%*	*N*	*%*	*N*	*%*
Şirketinizde Bilgi Güvenliğinden Sorumlu Bir Kurul/Komisyon /Birim Bulunmakta mıdır?	119	26,0	183	40,0	155	33,9
Şirketinizdeki Verilerin İşlenmesi, Saklanması, Korunması ve İmhası Konusunda Prosedür ve Politikalar Belirlenmiş midir?	68	14,9	150	32,8	239	52,3
Şirketinizin Çalışanlarına Veriler ve Bilgi Güvenliğine İlişkin Teknik, İdari ve Yasal Hak ve Yükümlülükler Eğitim Verildi mi?	*131*	*28,7*	*161*	*35,2*	*165*	*36,1*

3- Katılımcılara, şirket üst yönetiminin, bilgi güvenliğinin sağlanması konusundaki davranış ve destekleri ile ilgili soru yöneltilmiştir. Elde edilen bulgularda Tablo 67, şirketlerin %7,0'ı bilgi güvenliğinin sağlanması konusunda şirket üst yönetiminin destek olduğunu, %75,9'u ise hayır cevabı vererek destek olmadığını belirtmiştir. Katılımcıların %17,1'inin bir fikirlerinin bulunmadığı belirlenmiştir.

TS ISO/IEC 27001:2022 BGYS standardın 5. ve 9. madde düzenlemelerinde, üst yönetimin bilgi güvenliği yönetim sistemine ilişkin olarak yerine getirmesi gereken konular düzenlenmiştir. Buna göre, üst yönetimin şirkete liderlik ve bağlılık göstermesi gerektiği, bir bilgi güvenliği politikası oluşturması, bilgi güvenliğinin sağlanmasına ilişkin roller için sorumlu ve yetkililerin atanmasını ve duyurulmasını temin etmesi gerektiği belirtilmiştir. Ayrıca, planlı aralıklarla uygulamaları gözden geçirmesi ve bilgi güvenliği yönetim sistemi için gerekli olan kaynakları tedarik etmesi görevleri arasında sayılmıştır. Bu çerçevede, şirket üst yönetiminin destek ve kararları önemlidir ve bilgi güvenliğine yönelik yatırım kararı, şirket için stratejik bir karar olarak değerlendirilmektedir.

Tablo 67. Bilgi Güvenliğine İlişkin Şirket Üst Yönetiminin Desteğine Dair Sonuçlar

	EVET		HAYIR		FİKRİM YOK	
	N	*%*	*N*	*%*	*N*	*%*
Bilgi Güvenliğinin Sağlanması Konusunda Şirket Üst Yönetimi Destek Olmakta mıdır?	*32*	*7,0*	*347*	*75,9*	*78*	*17,1*

5.3 Bilgi Güvenliğini Sağlamak Üzere Alınan Teknik, Hukuki ve İdari Tedbirler

Anket katılımcılarına, bilgi güvenliği konusundaki teknik ve idari tedbirler ile yasal sorumluluklara ilişkin sorular yönlendirilmiş ve bulgulara Tablo 68 'de yer verilmiştir. Tablo verilerine göre, katılımcıların %52,3'ünün verilerin korunmasından yasal olarak sorumlu olduklarını bildiği görülmektedir. Çoğunluğun bu bilince sahip olması önemlidir, bu durum, bilgi güvenliğiyle ilgili yasal yükümlülüklerin belirli bir kitleye ulaştığını göstermektedir. Yine, sayıca çok fazla olmamakla birlikte, katılımcı şirketlerin %39,4'nün verilerin korunmasıyla ilgili teknik önlemleri aldıkları gözlemlenmektedir. Ancak literatür çalışmalarında belirtildiği üzere, bilgi güvenliği için yalnızca teknik tedbirlerin alınmış olması yeterli değildir. Diğer yönlerin (idari, hukuki, insan kaynakları) de dikkate alınması gerekmektedir. Safa, Maple ve Watson (2017), bilgi güvenliği için teknik yönlerin önemli olduğu ancak yeterli olmadığı, bilgi güvenliğinin tüm yönlerine dikkat edilmesi gerektiği belirtilmiştir. Aynı tabloda, katılımcıların bilgi güvenliği için alınması gereken hukuki ve idari tedbirlere ilişkin verdikleri cevaplara da yer verilmiştir.

Elde edilen anket bulguları Tablo 68'de katılımcılar, bilgi güvenliğine ilişkin çalışanlara eğitim verilmesi ile ilgili soruya %35,2'si hayır eğitim verilmedi şeklinde cevap verirken, %28,7'si eğitim verildiğini ve %36,1'i ise bir fikirlerinin olmadığını belirtmiştir.

Tablo 68. Bilgi Güvenliğinin Sağlanmasına Yönelik Tedbirlere İlişkin Sonuçlar

	EVET		HAYIR		FİKRİM YOK	
	N	%	N	%	N	%
Şirketiniz, Verilerin Korunması İçin Gerekli ve Yeterli Teknik Donanıma Sahip midir?	180	39,4	141	30,9	136	29,8
Şirket Verilerinin Korunmasından Yasal Olarak Sorumlu Olduğunuzu Düşünüyor musunuz?	239	52,3	116	25,4	102	22,3
Şirketinizdeki Verilerin İşlenmesi, Saklanması, Korunması ve İmhası Konusunda Prosedür ve Politikalar Belirlenmiş midir?	68	14,9	150	32,8	239	52,3
Verilerin Muhafaza Edildiği "Fiziki Ortamların" (Kasa, Kilitli Dolap, Sunucu, Sistem Odaları vb.) Güvenliğinden Sorumlu Kişiler Belirlenmiş midir?	70	15,3	213	46,6	174	38,1
Kişisel ve Tüzel Kişi Verilerinin Muhafaza Edildiği "Fiziki Ortamlara" Erişebilecek Sorumlu Kişiler Belirlenmiş midir?	113	24,7	283	61,9	61	13,3
Kişisel ve Tüzel Kişi Verilerinin Kaydedildiği "Bilgisayarlara" Erişebilecek Sorumlu Kişiler Belirlenerek, Yetkilendirme Prosedürleri Hazırlanmış mıdır?	70	15,3	168	36,8	219	47,9
Şirketinizin Çalışanlarına Veriler ve Bilgi Güvenliğine İlişkin Teknik, İdari ve Yasal Hak ve Yükümlülükler Eğitim Verildi mi?	131	28,7	161	35,2	165	36,1

Kişisel ve tüzel kişi verilerinin muhafaza edildiği fiziki ortamlara erişebilecek sorumluların belirlenmesine ilişkin soruya katılımcıların % 61,9'u hayır belirlenmedi cevabını vermistir. Aynı soru bilgisayarlara erişebilecek sorumlularının belirlenmesi için de sorulmuş ve katılımcıların % 36,8'i hayır cevabını verirken, %47,9'u fikri olmadığını ve sadece %15,3'ü evet belirlenmiştir şeklinde cevap vermiştir.

Verilerin muhafaza edildiği fiziki ortamların (kasa, kilitli dolap gibi) güvenliğinden sorumlu kişilerin belirlenip belirlenmediğine ilişkin soruya da katılımcıların %46,6'sı hayır cevabını vermiştir.

Katılımcılara yöneltilen bu sorular, bilgi güvenliğini sağlamak üzere yapılması gerekli olan hukuki ve idari tedbirlerle ilgilidir. Anket sonuçları, lojistik işletmelerinin bilgi güvenliği konusunda teknik önlemlerin yanı sıra gerekli olan idari ve hukuki önlemleri yeterince almadığını göstermektedir.

Kişisel verileri koruma kurulunun, firmaların idari ve hukuki tedbirlerdeki eksikliklerinden kaynaklanan kararları bulunmaktadır. Ayrıca, firmaların teknik önlemler aldıkları halde gerekli güncelleme ve denetimleri yapmamaları sebebiyle oluşan

mağduriyetlere ilişkin kararları bulunmaktadır. Benzer şekilde, yeterli ve özenli yetkilendirmelerin yapılmaması ve sorumluların belirlenmemesi nedeniyle ortaya çıkan ihtilaflarda verilmiş olan Yargıtay kararları da mevcuttur;

Yargıtay 5 Ceza Dairesi (2017), *"(...) çalışmakta olan sanığın, şirketin ana bilgisayarına, güvenlik sistemini devre dışı bırakıp uzaktan girerek kendi bilgisayarına veri transferi yaptığı(...)*". Anılan kararda, sanığın şirketin ana bilgisayar güvenlik sistemini devre dışı bırakarak veri transferi yapması ele alınmaktadır. Şirket, sisteme giriş yetkilendirmelerini özenli ve yeterli şekilde yapmadığı, gerekli önlemleri almadığı için böyle bir olayla karşılaşmıştır. Bilgi güvenliği politikalarının hazırlanması sürecinde, şirket verilerine kimlerin, ne zaman, ne şekilde erişebileceğine ilişkin ayrıntılı düzenlemelere yer verilmesi mümkündür. Bu politikaların varlığı, uygulanması ve denetimi, risklerin önlenmesi açısından önemlidir.

ISO 27001:2022 BGYS standart ana maddeler 7.md. kapsamında farkındalık ve yetkinlik düzenlemesine yer verilmiştir;

" ISO 27001:2022 Ana Maddeleri

7 Destek

7.2 Yetkinlik

Kuruluş aşağıdakileri yapmalıdır:

a) Bilgi güvenliği performansını etkileyen kendi kontrolü altında çalışan kişinin/kişilerin gerekli yetkinliğini belirlemeli,

b)Bu kişilerin uygun eğitim, öğretim veya deneyim temelinde yetkin olmalarını sağlamalı,

c) Uygun olduğu durumlarda, gerekli yeterliliği elde etmek için önlemler almalı ve alınan önlemlerin etkinliğini değerlendirmeli ve

d) Yeterliliğin kanıtı olarak uygun yazılı bilgileri muhafaza etmelidir.

7.3 Farkındalık

Kuruluşun kontrolü altında çalışan kişiler aşağıdaki hususların farkında olmalıdır:

a) Bilgi güvenliği politikası,

b) İyileştirilmiş bilgi güvenliği performansının faydaları da dâhil olmak üzere, bilgi güvenliği yönetim sisteminin etkinliğine katkıları ve

c) Bilgi güvenliği yönetim sistemi gerekliliklerine uymamanın sonuçları" (ISO/IEC, 2022).

Standartın çalışanlara yüklediği sorumlulukların yerine getirilmesi, onların bilgilendirilmeleri, hak ve yükümlülükleri konusunda eğitim verilmesi ile sağlanabilir. Ancak, Tablo 68 sonuçları incelendiğinde, lojistik işletmelerinin genel olarak, çalışanlarına bilgi güvenliği konusunda teknik, idari ve hukuki haklar ve yükümlülükler ile ilgili eğitim verilmesinde yetersiz kaldıkları görülmektedir. Akademik araştırmalar veri ihlal sebepleri içinde insan kaynaklı ihlalleri ilk sırada göstermektedir. Ayrıca, işletme içerisinden kaynaklı veri ihlallerine ilişkin olarak fazla sayıda yargı kararı bulunmaktadır.

5.3.1 Veri ihlaline yönelik tedbirler

Tablo 69.Veri İhlaline İlişkin Hukuki ve İdari Tedbirler

	EVET		**HAYIR**		**FİKRİM YOK**	
	N	%	N	%	N	%
Veri İhlali Hakkında Bilginiz Var mıdır?	131	28,7	159	34,8	167	36,5
Şirketinizde Veri İhlali Durumunda İzlenecek Yazılı Eylem Planı Oluşturulmuş mudur?	150	32,8	158	34,6	149	32,6
Veri Sızıntısında Sorumluluğu Olan, Bilgi Güvenliği Prosedürlerine Uymayan Tedarikçi vb. Üçüncü Kişilere Uygulanacak Politikalar Var mıdır?	113	24,7	163	35,7	181	39,6

Katılımcılara veri ihlali, ihlalin gerçekleşmesi halinde izlenecek eylem planı ile ilgili sorular yöneltilmiştir. Katılımcıların, %28,7'si veri ihlali hakkında bilgilerinin bulunduğunu, %34,8'i ise bilgisinin olmadığını belirtmiştir. %36,5'i ise fikrinin bulunmadığını ifade etmiştir.

Tablo 69'da yer verilen, veri ihlali halinde izlenecek bir eylem planı bulunup bulunmadığına ilişkin soruya katılımcıların, %34,6'sı eylem planı olmadığını ve %32,6'sı ise fikrinin bulunmadığını belirtmiştir.

Aynı tabloda yer verilen, veri sızıntısında sorumluluğu olan ve şirketin bilgi güvenliği politikalarına uymayan iş ortakları, tedarikçiler, hizmet alınan firmalara bu kusurlu davranışları sebebi ile uygulanacak politikaların mevcut olup olmadığı sorulduğunda ise katılımcıların, %35,7 hayır mevcut değildir cevabını verirken, %39,6'sı bir fikrinin bulunmadığını belirtmiştir.

Veri ihlali yaşanması durumunda ortaya çıkacak doğal sonuçlardan biri, iş akışlarının kesintiye uğramasıdır. Lojistik hizmetlerin sunulmasında iş süreçlerinin durması, tedarik zinciri içerisinde birçok hizmetin aksamasına ve dolayısıyla zarar oluşmasına sebep olacaktır.

Katılımcı firmaların cevapları değerlendirildiğinde, genel olarak, veri ihlali yaşanması durumunda ortaya çıkabilecek olaylara ilişkin eylem planlarının mevcut olmadığı görülmektedir. Benzer şekilde, ihlal olayında sorumluluğu bulunan tedarikçilere, iş ortaklarına ve hizmet sağlayıcı firmalara yönelik uygulanacak prosedürlere ilişkin bir politikalarının da genel olarak mevcut olmadığı anlaşılmaktadır.

Çok sayıda tedarikçisi olan firmaların denetimi güçlendirilmelidir; çünkü bu tür firmalar, bilgi ifşa etme ihlalleri yapma konusunda daha yüksek bir motivasyon seviyesine sahip olabilir ve tedarikçilerin denetimi ve firma yönetiminin etkinliği genellikle daha zayıftır. Özetle, dış denetimin güçlendirilmesi, bilgi ifşası ihlali vakalarının azaltılmasına yardımcı olur (Li, Lai ve Zhong, 2024).

5.3.2 Üçüncü kişilerden kaynaklanan ihlallere yönelik tedbirler

Tablo 70. Hukuki ve İdari Tedbirler

	EVET		HAYIR		FİKRİM YOK	
	N	%	N	%	N	%
Bilgi Güvenliği Konusunda Dışarıdan Teknik Destek Hizmeti (Bakım, Proje vs) Alıyor musunuz?	166	36,3	127	27,8	164	35,9
Veri Paylaşımında Bulunduğunuz Tedarikçi, İş Ortakları, Hizmet Alınan Firmalar'ın, ISO 27001 BGYS Belgesine Sahip Olması Şirketiniz İçin Önemli midir?	162	35,4	157	34,4	138	30,2
Tedarikçi ve İş Ortaklarınız İle Aranızda ki Sözleşmelerde Bilgi Güvenliği Gizlilik ve Sır Saklama Yükümlülüğüne İlişkin Hükümlere Yer Verilmiş midir?	89	19,5	188	41,1	180	39,4

Katılımcılara, bilişim sistemlerinin güvenliği, bakımı gibi durumlar için dış kaynaktan teknik destek hizmeti alıp alınmadıkları sorulmuş ve %36,3'ü destek aldıklarını ifade etmiştir. Destek hizmeti almadığını belirtenler ise %27,8 dir. Destek hizmetlerinin (bakım, proje gibi) firma bünyesinde kurulacak bir birim tarafından verilmesi imkanı bulunduğu gibi, bazı hallerde dış kaynak kullanılarak firma dışından tek seferlik ya da sürekli destek veya yerel iş ağları aracılığı ile bilgi alışverişi şeklinde hizmet alınması mümkündür. Önemli olan, alınacak hizmet için uyulması gereken kural ve sorumlulukların belirli prosedürlere bağlanmış olmasıdır. Hizmeti verecek üçüncü kişi firma, hizmet talep eden firmanın bilgi güvenliğine ilişkin prosedür ve politikalarına uymalıdır. Bunun sağlanabilmesi için, öncelikle hizmeti alan lojistik şirketinin bir bilgi güvenliği politikasına sahip olması gereklidir. Karşılıklı iki firma arasında akdedilecek sözleşme ile, hizmet verecek firma personelinin, lojistik şirketinin dijital sistemlerine girerek verilere zarar verme riski azaltılabilecektir. Sözleşmede, gizlilik, bilgi güvenliği ve sır saklamaya ilişkin hükümlere yer verilmeli, uyulması gereken hususlar açık ve net olarak belirlenmelidir.

Tablo 70 bulgularında katılımcılara, tedarikçi ve iş ortakları ile aralarındaki sözleşmelerde, veri güvenliği ile ilgili düzenlemelere yer verilip verilmediği sorulmuş, %41,1'i Hayır cevabını vermiştir. %39,4'ü fikri olmadığını belirtmiş, %19,5'lik bir katılımcı ise evet cevabını vermiştir. Diğer taraftan katılımcılara bilgi güvenliği ihlal

sebeplerinin neler olabileceği sorulduğunda ise, Tablo 71'de yer verilen sonuçlara göre, %14,7 oranı ile tedarikçi, iş ortakları ve müşteri bilgi güvenliği tedbirlerinin eksik olmasından kaynaklanan ihlal, sebepler arasında gösterilmiştir. Sonuçlar değerlendirildiğinde, ihlal sebebi olarak gösterilen bir konuda firmaların yeterli bilgi güvenliği tedbiri almayarak yanlış uygulamalara devam ettikleri görülmektedir. Düzenlemelerin eksik ve yetersiz olması, veri ihlallerinin ortaya çıkmasında etkili olmaktadır. Bu durumda, lojistik işletmelerinin veri güvenliği için ihtiyaç duyulan hukuki ve idari önlemleri aldığı söylenemeyecektir.

Tedarik zincirlerine yönelik saldırılar bir ve daha fazla tedarikçiye yönelik olabildiği gibi aynı zamanda müşteri varlıklarını da hedeflenmektedir:

> Tedarik zinciri saldırılarının yaşam döngüsüne göre, saldırının, bünyesinde iki gelişmiş sürekli tehdit saldırısını barındırdığı görülebilir. İlk saldırı, bir veya daha fazla tedarikçiyi hedeflerken; ikinci saldırı, müşterilerin varlıklarını hedef alır. Müşteriler halihazırda tedarikçilere güvendiği için bu tür siber saldırıların tespit edilmesi daha zordur(…).Tek bir tedarikçiye yapılan bir saldırının tetiklediği zincirleme reaksiyon bütün bir sağlayıcı ağını tehlikeye atabilmektedir (Aselsan, 2022, s. 24).

Çoğu zaman firmalara ait ticari sırlar, ticari sözleşmeler kapsamında da ifşa edilebilmektedir. Tedarikçiler ile akdedilen sözleşmelere yazılacak gizlilik maddelerinde ticari sır tanımı kapsamının geniş tutulması önemlidir. Ayrıca yükümlülükler kapsamı açık ve net belirlenmelidir. Sözleşmeye, gizlilik yükümlülüğünün tarafların çalışanları, temsilcileri ve danışmanları için de geçerli olacağı maddesi eklenebilir.

Anket araştırmasında katılımcılara, veri paylaşımında bulundukları tedarikçi ve iş ortaklarının ISO 27001 BGYS belgesine sahip olmasının önemli bulunup bulunmadığı da sorulmuştur. Tablo 70 bulgularına bakıldığında, katılımcıların %35,4'ü evet önemli cevabını verirken %30,2'si fikrinin olmadığını belirtmiş ve %34,4'ü ise hayır cevabını vermiştir.

Diğer taraftan, yapılan araştırmalarda, siber saldırı risklerinden korunmanın, doğru ve etkin bir güvenlik stratejisi sayesinde gerçekleşebileceği, bunu gerçekleştirmek için de tüm paydaşların sürece dahil olmasının öneminden sözedilmektedir.

Siber güvenlik stratejisi oluşturarak güvenlik riskleri ile mücadele edilebilir. Stratejinin uygulanması ancak, tüm paydaşların yönetim proseslerine katılmasını sağlayarak mümkün olabilir (Savaş ve Karataş, 2022).

Tedarik zincirleri siber risklerin yayılması için verimli ortamlardır. Geçmişte, bu saldırılar ana hedeflerine açıkça odaklanırken, günümüzde failler yetkili erişimlerini elde etmek için tedarik zincirine hizmet veren firmalara/kişilere saldırmaya başlamıştır. Örneğin, 2018'de Maersk, BİT sisteminin sağlayıcısı olan yan kuruluşu aracılığıyla ihlal yaşamıştır. Tüm tedarik zinciri katılımcılarının veya taşeronlarının siber riskler için tam koruyucu önlemler uyguladığını varsaymak mümkün değildir (Filho, Rego ve Claro, 2021).

Bir diğer araştırmaya göre, firmalar çoğu kez, tedarikçi seçimlerinde ISO 27001 bilgi güvenliği belgesi sahibi firmaları tercih etmektedir.

Yapılan çalışma, firmaların bilgi güvenliği sertifikası olan ortaklara başvurduğunu göstermiştir (Mirtsch, Kinne ve Blind, 2021).

5.3.3 Personel kaynaklı veri ihlalleri

Çalışan kaynaklı veri ihlali çoğu işletmenin yaşadığı bir sorundur. İşçiler, bazı hallerde bilmeden ya da ihmalkar davranışları ile bazı hallerde de kasıtlı olarak şirkete zarar verilebilmektedir.

Araştırmalar, veri ihlallerinin genellikle şirket içinden, insan kaynaklı olduğunu ortaya koymaktadır. Verizon raporu (2023), raporda en dikkat çekici istatistik insan ile ilgilidir. 16.312 vaka ve 5.199 küresel veri ihlalinin %74'ünde insan kaynaklı hatalar bulunmaktadır. Bu durumun çeşitli sebepleri olabilir; en önemlisi, yeterli düzeyde bilinçlendirme ve farkındalık olmamasıdır.

Anket katılımcılarına, veri ihlal sebeplerinin neler olabileceğine ilişkin olarak çoktan seçmeli bir soru sorulmuştur. Verilen cevaplarda (Tablo 71) en fazla oran %19,9 ile

Personelden kaynaklanan ihlal şeklinde olmuştur. %16,6 oranı ile verileri korumaya yönelik politikaların bulunmaması ve %12,9 oranı ile Fiziki ortamda saklanan bilgilerin çalınması da sebepler arasında sayılmıştır. Bunları değişik oranlarda başkaca sebepler izlemiştir.

Tablo 71. Veri İhlali Sebeplerine İlişkin Bulgular

Sizce Veri İhlalleri Aşağıdakilerden Hangileri Kaynaklı Olabilir?		
Yanıtlar	n	%
Personelden Kaynaklanan İhlal	91	19,9
Teknik Güvenlik Açıklarından Kaynaklanan İhlal	89	19,5
Zararlı Yazılımdan Kaynaklanan İhlal	75	16,4
Fiziki Ortamda Saklanan Bilgilerin Çalınması	59	12,9
Tedarikçi, İş Ortakları, Müşteri Bilgi Güvenliği Tedbirlerinin Eksik Olmasından Kaynaklanan İhlal	67	14,7
Verileri Korumaya Yönelik Politikaların Bulunmaması	76	16,6
Toplam	**457**	**100**

Diğer taraftan katılımcılara, çalışan kaynaklı veri ihlali halinde uygulanacak disiplin süreçlerinin olup olmadığı sorulduğunda Tablo 72 sonuçlarına göre, %40,9'u hayır cevabını vermiş, %36,3 fikrinin olmadığını belirtmiş ve %22,8'i evet cevabını vermiştir.

Tablo 72. Personel Kaynaklı İhlallere Karşı Disiplin Süreci Belirleme Durumu

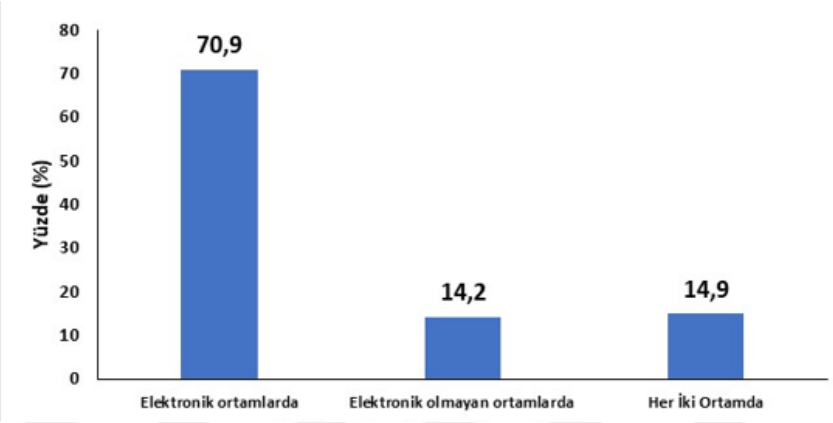
	EVET		**HAYIR**		**FİKRİM YOK**	
	N	%	N	%	N	%
Personel Kaynaklı Veri İhlalleri İçin Uygulanacak Disiplin Süreci Belirlenmiş midir?	104	22,8	187	40,9	166	36,3

Borçlar Kanunu madde 396'a göre; "*İşçi, iş gördüğü sırada öğrendiği, özellikle üretim ve iş sırları gibi bilgileri, hizmet ilişkisinin devamı süresince kendi yararına kullanamaz veya başkalarına açıklayamaz. İşverenin haklı menfaatinin korunması için gerekli olduğu ölçüde işçi, hizmet ilişkisinin sona ermesinden sonra da sır saklamakla yükümlüdür"* (Türk Borçlar Kanunu, 2011).

Mevzuat gereğince, işçinin iş gördüğü sırada öğrendiği bilgileri, çalışırken hatta iş akdi sona erdikten sonra da kullanması ve açıklaması yasaktır. Kanun düzenlemesi işverenin haklarını işçinin zararlı, kasti davranışlarına karşı korumakla birlikte işveren tarafından da şirket içi yasal ve idari tedbirlerin alınması gereklidir. Anket bulguları birlikte

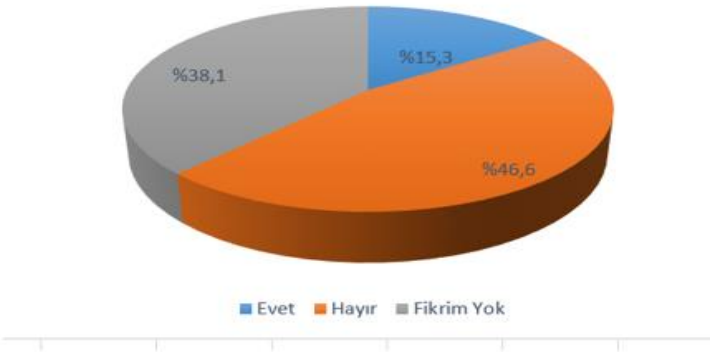
değerlendirildiğinde, katılımcı şirketlerin personelden kaynaklı ihlal sorunlarının farkında oldukları, ancak ihlal ve sonrasında takip edilecek plan ve disiplin süreci ile ilgili düzenlemeleri genel olarak yapmadıkları görülmektedir. Aynı şekilde bulgular, çalışanlara yönelik bilgi güvenliğine ilişkin eğitim çalışmalarının yeterince yapılmadığını göstermektedir.

Şekil 22'de yer verilen anket sonuçlarına göre, dijitalleşme ile birlikte verilerin yoğun olarak elektronik ortamlarda kayıt altına alındığı görülmektedir.



Şekil 22. Verilerin Kayıt Edildiği Ortamlara İlişkin Bulgular

Anket çalışmasında katılımcılara, verilerin muhafaza edildiği fiziki ortamların güvenliğinden sorumlu kişilerin belirlenip belirlenmediği sorulmuş, katılımcıların %46,6'sı Hayır belirlenmedi şeklinde cevap vermiştir. %15,3 evet derken, %38,1 fikri bulunmadığını ifade etmiştir. Bulgular Şekil 23'de gösterilmiştir.



Şekil 23. Verilerin Korunduğu "Fiziki Ortamların" Güvenliğinden Sorumlu Olanların Belirlenmesi

Diğer taraftan, verilerin muhafaza edildiği bilgisayarlara erişebilecek sorumlu kişilerin belirlenmesine ilişkin soruya katılımcılar, %36,8 ile Hayır cevabını vermiştir. %15,3 evet derken, %47,9 fikri bulunmadığını ifade etmiştir. Bulgular Tablo 73'de gösterilmiştir.

Tablo 73. Bilgisayarlara Erişebilecek Yetkili Kişilerin Belirlenme Oranı

Kişisel ve Tüzel Kişi Verilerinin Kaydedildiği "Bilgisayarlara" Erişebilecek Sorumlu Kişiler Belirlenerek, Yetkilendirme Prosedürleri Hazırlanmış mıdır?		
Yanıtlar	n	%
Evet	70	15,3
Hayır	168	36,8
Fikrim Yok	219	47,9
Toplam	**457**	**100**

Elde edilen bulgular birlikte değerlendirildiğinde, lojistik işletmeler, şirket içi kaynaklı veri ihlal sebeplerini başlıca sorun olarak belirtmektedir. Diğer taraftan ise, personele yeterli eğitim verilmediği gibi, ihlale sebep olan personele uygulanacak disiplin düzenlemelerinin de yapılmadığı görülmektedir. Veriler genel olarak dijital ortamlarda kayıt altına alındığından, bilgi sistemleri ile birlikte fiziki ortam güvenliğinin de sağlanması gerekir iken bu prosedürlerin uygulanmadığı, gerekli yetkilendirmelerin yeterince yapılmadığı anlaşılmaktadır. Bu durumda, lojistik işletmelerinin bilgi güvenliğine ilişkin olarak idari ve hukuki tedbirlerinin yetersiz olduğunu söylemek mümkündür. Bilgi güvenliği, hukuki, idari, teknik ve insan kaynakları alanlarını kapsayan çok yönlü bir disiplindir, dolayısıyla bu unsurların hepsinin etkili bir şekilde birlikte değerlendirilmesi gerekmektedir.

Verizon tarafından yayımlanan 2022 Veri İhlali Soruşturma Raporunda, 2021 yılında fidye yazılımı saldırılarında artış yaşandığı, 5 saldırıdan üçünün tedarik zincirlerini etkilediği ve saldırıların %82'sinin insan faktöründen kaynaklandığı belirtilmiştir (Digital Report, 2022).

Verizon 2023 tarihli raporunda en dikkat çekici istatistik insan ile ilgilidir. İnsan kaynaklı hataların yüksek seviyede olması sosyal mühendislik saldırılarına zemin hazırlayan kasıtsız davranışlarla da ilgilidir (Kron Teknoloji, 2023).

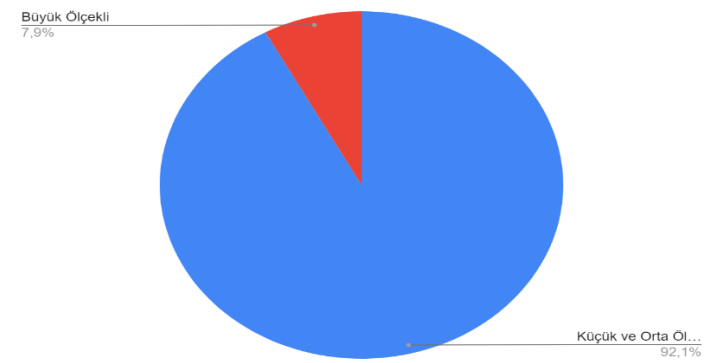
Yasal düzenlemeler genel itibari ile veri sorumlularının, kayıt altına aldıkları verileri korumak üzere her türlü önlemi almaları gerektiğini belirtmektedir. KVKK madde 12/c'de "V*eri sorumlularının, kişisel verilerin muhafazasını sağlamak, amacıyla uygun*

güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda oldukları" belirtilmiştir.

KVKK düzenlemesi sicile kayıt madde 16-3/e fıkrası; "*(3) Veri Sorumluları Siciline kayıt başvurusu aşağıdaki hususları içeren bir bildirimle yapılır:(...) e) Kişisel veri güvenliğine ilişkin alınan tedbirler"* şeklindedir. Kişisel Verilerin Korunması Kanunu düzenlemesine göre, kanun koyucu tarafından kişisel veri güvenliğine ilişkin alınan tedbirlerin, sicile kayıt başvurusunda açıklanması gerekir. Buna göre, kanun koyucu sadece hangi türden verilerin işlendiği ile ilgilenmemekte ayrıca, bu verilerin korunması için gerekli olan tedbirlerin alınıp alınmadığını da incelemektedir.

5.3.4 Bilgi güvenliği ve mali durum açısından değerlendirilmesi

Şekil 24'e göre anket çalışmasına her büyüklükte (ölçekte) lojistik şirketi katılım göstermiştir. Katılımcı şirketlerin %92,1 küçük ve orta ölçekli işletmelerden, %7,9' u da büyük ölçekli işletmelerden oluşmaktadır.



Şekil 24.Şirket Büyüklüğü

Anket çalışması kapsamında, katılımcı şirketlerin son mali yıla ait yıllık geliri ile bilgi güvenliğine ayrılan yıllık giderleri arasındaki ilişki incelenmiş ve elde edilen bulgulara Tablo 74'de yer verilmiştir. Tablo incelendiğinde, son mali yıla ait yıllık gelir ile bilgi güvenliğine dair yıllık gider arasındaki ilişkinin incelenmesi ile aralarındaki ilişkinin anlamlı olduğu (χ^2:607,200; p=0,001<0,05), şirket mali durumunun, bilgi güvenliğine yönelik harcama yapılmasında etkili olduğu belirlenmiştir.

Tablo 74. Son Mali Yıla Ait Yıllık Gelir ile Bilgi Güvenliğine İlişkin Yıllık Gider İlişkisi

Son Mali Yıla Ait Yıllık Geliriniz (Şirket Cirosu)		Bilgi Güvenliğine Dair Yıllık Gider						**Toplam**	**χ^2**	**p**
		1 TL. - 50.000 TL.	50.001 TL. - 100.000 TL.	100.001 TL. - 500.000 TL.	500.001 TL. – 1.000.000 TL.	1.000.000 TL'den Fazla	Bir Giderimiz Bulunmamaktadır			
5 Milyon TL altında	n	47	53	16	0	0	56	172	607,2	0,001*
	%	27,3%	30,8%	9,3%	0,0%	0,0%	32,6%	100,0%		
5-50 Milyon TL	n	28	57	43	0	0	47	175		
	%	16,0%	32,6%	24,6%	0,0%	0,0%	26,9%	100,0%		
50-250 Milyon TL	n	2	26	30	0	0	16	74		
	%	2,7%	35,1%	40,5%	0,0%	0,0%	21,6%	100,0%		
250 Milyon Üzeri	n	0	0	0	19	17	0	36		
	%	0,0%	0,0%	0,0%	52,8%	47,2%	0,0%	100,0%		
*p<0.05; Ki-kare analizi yapılmıştır. Yüzdeler satıra göre verilmiştir.										

Şirketlerin mali durumu bilgi güvenliğine bütçe ayrılmasında etkilidir. Bu durumda, sektörün büyük ölçüde küçük ve orta ölçekli işletmelerden oluştuğu dikkate alındığında, bilgi güvenliğinin istenen seviyede sağlanamamasının ardında mali konuların da etkili olduğu söylenebilecektir.

Küçük ve orta ölçekli işletmeler, esas olarak büyüklükleri, bölgesel kapsamları ve finansal kaynakları nedeniyle bilgi güvenliği ve siber güvenlik yönetiminde kör nokta olarak görülmektedir (Antunes, Maximiano, Gomes ve Pinto, 2021)**.**

Küçük ve orta ölçekli firmalar, siber tehditlere karşı en savunmasızdır. Siber saldırılara maruz kalan işletmeler, varlıkları üzerinde ciddi etkilerle karşı karşıya kalmaktadır (Pawar ve Palivela, 2022).

Verizon 2022 Veri İhlali Soruşturma Raporu, siber saldırganlar, küçük ve orta ölçekli firmaların bilişim sistemlerinin daha savunmasız olduğunu bilerek saldırılarını bu firmalara yöneltmektedir. Siber saldırıların hedefi olmamak için şirket büyüklüğü ne ölçüde olursa olsun tüm firmalar bilgi güvenliğine bütçe ayırmalı, yatırım yapmalıdır (Dijital Report, 2022).

Dijital alandaki gelişmeler, her ölçekten firma için bilgi güvenliği açısından risk oluşturmaya devam etmektedir. Kişisel verileri koruma kurulunun yeni tarihli son

kararlarında, siber saldırı gerçekleştirenlerin veri sorumlusundan fidye talebinde bulunduğu görülmektedir.

"Veri sorumlusu sıfatını haiz olan (...)Plastik Sanayi ve Ticaret Limited Şirketi tarafından Kurum'a gönderilen yazıda özetle; İhlalin, veri sorumlusu sistemlerine yapılan siber saldırı sonucunda gerçekleştiği(...)şirket verilerinin bir kısmının şifrelendiği...veri sorumlusundan fidye talep edildiği" (Kişisel Verileri Koruma Kurulu Kararı, 2024).

Akademik araştırmalar, anket sonucu elde edilen bulgular, kurul kararları birlikte değerlendirildiğinde, gelecekte de siber saldırıların tedarik zincirlerini hedef almaya devam edeceği görülmektedir. Risk her ölçekten firma için söz konusudur. Ancak daha savunmasız ve zayıf halka olarak görünmelerinden ötürü özellikle küçük ve orta ölçekli firmalar siber saldırıların hedefindedir.

Literatür, ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardının, her ölçekten firma için bilgi güvenliğini sağlamada en iyi uygulama olduğunu göstermektedir.

Bu makalede elde edilen sonuçlar, bilgi güvenliği yönetiminin küçük ve orta ölçekli firmalara önemli faydalarını göstermiştir. Küçük ve orta ölçekli firmalarda bilgi güvenliği denetimine uygulanabilecek başka çerçeveler de vardır (örneğin, NIST Siber Güvenlik Çerçevesi), ancak ISO-27001:2013 çerçevesi, literatürde KOBİ'lerde bilgi güvenliğinin söz konusu olduğu en iyi uygulama olarak tanımlanmıştır (Antunes, Maximiano, Gomes ve Pinto, 2021).

5.4 Araştırma Hipotezi Bulguları ve Çözümlenmesi

Anket verileri SPSS 25.0 programı ile analiz edilmiştir. Her bir soruya verilen yanıtların dağılımlarının incelenmesinde frekans ve yüzde analizi yapılmış olup, araştırma hipotezlerin test edilmesi için kategorik değişkenler arasındaki ilişkinin incelenmesi için %95 güven düzeyinde ki-kare analizleri yapılmıştır.

5.4.1 Araştırma hipotezi bulguları

H1: Mali Durum, ISO 27001 Belgesi Sahibi Olunmasında Etkilidir.

Tablo 75. Şirket Mali Durumları ile ISO 27001 Belgesi Sahibi Olma Durumu İlişkisi

Son Mali Yıla Ait Yıllık Geliriniz (Şirket Cirosu)		Şirketinizin ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi Bulunmakta mıdır?			**Toplam**	χ^2	**p**
		Evet	Hayır	Fikrim Yok			
5 Milyon TL altında	n	26	56	90	172		
	%	15,1%	32,6%	52,3%	100,0%		
5-50 Milyon TL	n	38	47	90	175		
	%	21,7%	26,9%	51,4%	100,0%		
50-250 Milyon TL	n	28	16	30	74		
	%	37,8%	21,6%	40,5%	100,0%		
250 Milyon Üzeri	n	36	0	0	36		
	%	100,0%	0,0%	0,0%	100,0%	114,31	0,001*
*p<0.05; Ki-kare analizi yapılmıştır. Yüzdeler satıra göre verilmiştir.							

Tablo 75 incelendiğinde, Mali Durum ile ISO 27001 belgesi sahibi olma durumu arasındaki ilişkinin anlamlı olduğu belirlenmiştir (χ^2:114,31; p=0,001<0,05). Son mali yıla ait yıllık cirosu 5 Milyon TL altında olan firmalarda ISO 27001 Bilgi Güvenliği Yönetim Sistemi bulunma oranı %15,1 iken 5-50 Milyon TL arasında cirosu olanlarda bu oran %21,7, 50-250 Milyon TL arasında cirosu olanlarda bu oran %37,8 ve 250 Milyon üzeri cirosu olan şirketlerde ise bu oranın %100'ünün ISO 27001 belgesi sahibi olduğu belirlenmiştir. Bu sonuç araştırmanın "**H_1: Mali Durum, ISO 27001 Belgesi Sahibi Olunmasında Etkilidir**." Hipotezinin desteklendiğini göstermektedir.

H2: ISO 27001 Belgesi Sahibi Firmalar, Tedarikçi ve Müşterilerinin de ISO 27001 Belgesine Sahip Olmasının Öneminin Farkındadırlar.

Tablo 76. ISO 27001 Belgesi Sahibi Firma ile Tedarikçide ISO 27001 Belgesi Olmasının Önemi

Şirketinizin ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi Bulunmakta mıdır?		Tedarikçi ve Müşterilerin ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesine Sahip Olması Şirketiniz İçin Önemli midir?			**Toplam**	χ^2	**p**
		Evet	Hayır	Fikrim Yok			
Evet	n	62	35	31	128	14,513	0,006*
	%	48,4%	27,3%	24,2%	100,0%		
Hayır	n	34	49	36	119		
	%	28,6%	41,2%	30,3%	100,0%		
Fikrim Yok	n	66	73	71	210		
	%	31,4%	34,8%	33,8%	100,0%		
*p<0.05; Ki-kare analizi yapılmıştır. Yüzdeler satıra göre verilmiştir.							

Tablo 76 incelendiğinde, ISO 27001 BGYS belgesi sahibi firmalar ile bu firmaların tedarikçi ve müşterilerinin de ISO 27001 BGYS belgesine sahip olmasının öneminin farkında olması arasındaki ilişkinin anlamlı olduğu belirlenmiştir (χ^2:14,513; p=0,006<0,05). ISO 27001 Bilgi Güvenliği Yönetim Sistemi belgesi bulunanlar %48,4 oran ile tedarikçi ve müşterilerinin de ISO 27001 belgesine sahip olmasının öneminin farkında iken, ISO 27001 belgesi olmayan firmalarda bu oranın %28,6 ve konu hakkında fikri olmayanlarda ise bu oranın %31,4 olduğu görülmektedir. Bu sonuç araştırmanın "**H_2: ISO 27001 Belgesi Sahibi Firmalar, Tedarikçi ve Müşterilerinin de ISO 27001 Belgesine Sahip Olmasının Öneminin Farkındadırlar**" Hipotezinin desteklendiğini göstermektedir.

H3: Eğitim, Veri İhlalleri Konusunda Farkındalık Oluşumunda Etkilidir.

Tablo 77. Bilgi Güvenliği Eğitimi ile Veri İhlali Hakkında Bilgi Sahibi Olma İlişkisi

Şirketinizin Çalışanlarına Veriler ve Bilgi Güvenliğine İlişkin Teknik, İdari ve Yasal Hak ve Yükümlülükler Eğitim Verildi mi?		Veri İhlali Hakkında Bilginiz Var mıdır?			**Toplam**	**χ^2**	**p**
		Evet	Hayır	Fikrim Yok			
Evet	n	131	0	0	131	457,42	0,001*
	%	100,0%	0,0%	0,0%	100,0%		
Hayır	n	0	81	80	161		
	%	0,0%	50,3%	49,7%	100,0%		
Fikrim Yok	n	0	78	87	165		
	%	0,0%	47,3%	52,7%	100,0%		
*p<0.05; Ki-kare analizi yapılmıştır. Yüzdeler satıra göre verilmiştir.							

Tablo 77 incelendiğinde, şirketin tüm çalışanlarına veriler ve bilgi güvenliğine ilişkin idari, teknik ve yasal hak ve yükümlülükler ile ilgili olarak eğitim verilmesi ile veri ihlali hakkında bilgi sahibi olunması arasındaki ilişkinin anlamlı olduğu belirlenmiştir (χ^2:457,42; p=0,001<0,05). Çalışanlarına, veriler ve bilgi güvenliğine ilişkin idari, teknik ve yasal hak ve yükümlülükler eğitimi verenlerin %100 oranında veri ihlali hakkında bilgisi bulunurken, eğitim almayanlarda veri ihlali hakkında bilgisi olmadığı görülmektedir. Bu sonuç araştırmanın "**H_3: Eğitim, Veri İhlalleri Konusunda Farkındalık Oluşumunda Etkilidir**" Hipotezinin desteklendiğini göstermektedir.

H4: Bilgi Güvenliğine Harcama Yapan Firmalar, Veri İhlali Etkilerinin Farkındadırlar.

Tablo 78. Bilgi Güvenliği Yıllık Giderleri ile Veri İhlalinin Şirkete Etkisi

Bilgi Güvenliğine Dair Yıllık Gider		Şirketinizde Veri İhlali Yaşanır ise Bu Olayın Şirketinize Etkisi Aşağıdakilerden Hangisi Olabilir?					**Toplam**	χ^2	**p**
		Şirketin itibarını olumsuz etkilemez, bilgi güvenliği yapısını etkiler	Şirketin itibarı olumsuz etkilenir	Şirkete bir etkisi olmaz, şirket mevcut organizasyonunu ve itibarını devam ettirir	Şirkete idari para cezası, hukuki tazminat ve ceza yükümlülüğü getirebilir	Fikrim yok			
1 TL. - 50.000 TL.	n	16	12	18	17	14	77	18,330	0,566
	%	20,8%	15,6%	23,4%	22,1%	18,2%	100,0%		
50.001 TL. - 100.000 TL.	n	20	32	30	19	35	136		
	%	14,7%	23,5%	22,1%	14,0%	25,7%	100,0%		
100.001 TL. - 500.000 TL.	n	14	14	21	14	26	89		
	%	15,7%	15,7%	23,6%	15,7%	29,2%	100,0%		
500.001 TL. – 1.000.000 TL.	n	2	5	6	3	3	19		
	%	10,5%	26,3%	31,6%	15,8%	15,8%	100,0%		
1.000.000 TL'den Fazla	n	3	4	3	5	2	17		
	%	17,6%	23,5%	17,6%	29,4%	11,8%	100,0%		
Bir Giderimiz Bulunmamaktadır	n	27	21	22	27	22	119		
	%	22,7%	17,6%	18,5%	22,7%	18,5%	100,0%		

Ki-kare analizi yapılmıştır. Yüzdeler satıra göre verilmiştir.

Tablo 78 incelendiğinde, bilgi güvenliğine dair yıllık gider ile bilgi güvenliği (veri) ihlali yaşanır ise bu olayın şirkete etkisi arasındaki ilişkinin incelenmesi arasındaki ilişkinin anlamlı olmadığı belirlenmiştir (χ^2:18,330; p=0,566>0,05). Bu sonuç araştırmanın "**H_4: Bilgi Güvenliğine Harcama Yapan Firmalar, Veri İhlali Etkilerinin Farkındadırlar**" Hipotezinin red edildiğini göstermektedir.

H5: Mali Durum, Bilgi Güvenliğine Yönelik Harcama Yapılmasında Etkilidir.

Tablo 79. Son Mali Yıla Ait Yıllık Gelir ile Bilgi Güvenliğine Dair Yıllık Gider İlişkisi

Son Mali Yıla Ait Yıllık Geliriniz (Şirket Cirosu)		Bilgi Güvenliğine Dair Yıllık Gider						**Toplam**	χ^2	**p**
		1 TL. - 50.000 TL.	50.001 TL. - 100.000 TL.	100.001 TL. - 500.000 TL.	500.001 TL. – 1.000.000 TL.	1.000.000 TL'den Fazla	Bir Giderimiz Bulunmamaktadır			
5 Milyon TL altında	n	47	53	16	0	0	56	172	607,2	0,001*
	%	27,3%	30,8%	9,3%	0,0%	0,0%	32,6%	100,0%		
5-50 Milyon TL	n	28	57	43	0	0	47	175		
	%	16,0%	32,6%	24,6%	0,0%	0,0%	26,9%	100,0%		
50-250 Milyon TL	n	2	26	30	0	0	16	74		
	%	2,7%	35,1%	40,5%	0,0%	0,0%	21,6%	100,0%		
250 Milyon Üzeri	n	0	0	0	19	17	0	36		
	%	0,0%	0,0%	0,0%	52,8%	47,2%	0,0%	100,0%		
*p<0.05; Ki-kare analizi yapılmıştır. Yüzdeler satıra göre verilmiştir.										

Tablo 79 incelendiğinde, son mali yıla ait yıllık gelir ile bilgi güvenliğine dair yıllık gider arasındaki ilişkinin incelenmesi arasındaki ilişkinin anlamlı olduğu belirlenmiştir (χ^2:607,200; p=0,001<0,05). Son mali yıla ait yıllık cirosu 5 Milyon TL altında cirosu olan firmaların %32,6 oranında bilgi güvenliğine dair bir giderleri bulunmadığı belirlenirken, 5-50 Milyon TL arasında cirosu olanlarda bu oran %26,9, 50-250 Milyon TL arasında cirosu olanlarda bu oran %21,6 ve 250 Milyon üzeri cirosu olan şirketlerde ise bu oranın %0 olduğu görülmektedir. Aynı zamanda Yıllık cirosu 250 milyon üzerinde olanların bilgi güvenliğine dair yıllık gideri %52,8 oranıyla 500.001 TL-1.000.000 TL arasında olduğu görülmektedir. Bu sonuç araştırmanın "**H_5: Mali Durum, Bilgi Güvenliğine Yönelik Harcama Yapılmasında Etkilidir**." Hipotezinin desteklendiğini göstermektedir.

H6: Veri Güvenliğinden Yasal Sorumlu Olunduğunun Farkında Olunması, Veri Güvenliğinin Korunmasına Yönelik Önlem Alınmasında Etkilidir.

Tablo 80. Verilerin Korunmasından Yasal Olarak Sorumlu Olduğunu Düşünme ile Şirket Verilerinin Korunması İçin Alınan Önlemler Arasındaki İlişkinin İncelenmesi

Şirket Verilerinin Korunmasından Yasal Olarak Sorumlu Olduğunuzu Düşünüyor musunuz?		Şirket Verilerinin Korunması İçin Aşağıdaki Önlemlerden Hangileri Alınmaktadır?							**Toplam**	**χ^2**	**p**
		Teknik Önlemler	Hukuki Önlemler	Bilgi Güvenliği Konusunda Personele Eğitim Verilmesi	İdari Önlemler	Bu Önlemler ile Bilgi Güvenliği Sağlanamaz	Önlem Alınmasına Gerek Yoktur	Fikrim Yok			
Evet	n	51	44	31	32	29	25	27	239	24,350	0,018*
	%	21,3%	18,4%	13,0%	13,4%	12,1%	10,5%	11,3%	100,0%		
Hayır	n	14	13	12	25	17	15	20	116		
	%	12,1%	11,2%	10,3%	21,6%	14,7%	12,9%	17,2%	100,0%		
Fikrim Yok	n	14	18	12	8	24	10	16	102		
	%	13,7%	17,6%	11,8%	7,8%	23,5%	9,8%	15,7%	100,0%		
*p<0.05; Ki-kare analizi yapılmıştır. Yüzdeler satıra göre verilmiştir.											

Tablo 80 incelendiğinde, verilerin korunmasından yasal olarak sorumlu olduğunu düşünme ile şirket verilerinin korunması için alınan önlemler arasındaki ilişkinin anlamlı olduğu belirlenmiştir (χ^2:24,350; p=0,018<0,05). Şirket verilerinin korunmasından yasal olarak sorumlu olduğunu düşünenlerin %21,3 oranı ile en fazla teknik önlemler aldıkları görülürken, şirket verilerinin korunmasından yasal olarak sorumlu olduğunu düşünmeyenlerin en fazla %21,6 ile idari önlemler aldıkları ve konu hakkında fikri olmayanların en fazla %23,5 ile bu önlemlerle bilgi güvenliğinin sağlanamayacağını düşündükleri belirlenmiştir. Bu sonuç araştırmanın "**H_6: Veri Güvenliğinden Yasal Sorumlu Olunduğunun Farkında Olunması, Veri Güvenliğinin Korunmasına Yönelik Önlem Alınmasında Etkilidir**." Hipotezinin desteklendiğini göstermektedir.

H7: Veri Güvenliğinden Yasal Sorumlu Olunduğunun Farkında Olunması, Bilgi Güvenliğine Bütçe Ayrılmasında Etkilidir.

Tablo 81. Verilerin Korunmasından Yasal Olarak Sorumlu Olduğunu Düşünme ile Bilgi Güvenliğine Dair Yıllık Gider Arasındaki İlişkinin İncelenmesi

Şirket Verilerinin Korunmasından Yasal Olarak Sorumlu Olduğunuzu Düşünüyor musunuz?		Bilgi Güvenliğine Dair Yıllık Gider						χ^2	p
		1 TL. - 50.000 TL.	50.001 TL. - 100.000 TL.	100.001 TL. - 500.000 TL.	500.001 TL. – 1.000.000 TL.	1.000.000 TL'den Fazla	Bir Giderimiz Bulunmamaktadır		
Evet	n	37	58	47	19	17	61	39,884	0,001*
	%	48,05%	42,65%	52,81%	100,00%	100,00%	51,26%		
Hayır	n	22	39	21	0	0	34		
	%	28,57%	28,68%	23,60%	0,00%	0,00%	28,57%		
Fikrim Yok	n	18	39	21	0	0	24		
	%	23,38%	28,68%	23,60%	0,00%	0,00%	20,17%		
Toplam	n	77	136	89	19	17	119		
	%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%		
*p<0.05; Ki-kare analizi yapılmıştır. Yüzdeler sütuna göre verilmiştir.									

Tablo 81 incelendiğinde, verilerin korunmasından yasal olarak sorumlu olunduğunun düşünülmesi ile bilgi güvenliğine dair yapılan yıllık gider arasındaki ilişkinin anlamlı olduğu belirlenmiştir (χ^2:39,884; p=0,001<0,05). Bilgi güvenliğine dair yıllık gideri 500.001 TL ve üzerinde olanların tamamının şirket verilerinin korunmasından yasal olarak sorumlu olduğunu düşünürken, bilgi güvenliğine dair yıllık gideri 100.001-500.000 TL arasında olanlarda bu oranın %52,81, 50.001-100.000 TL arasında bilgi güvenliğine yıllık gideri olanlarda bu oranın 42,65 ve 50.000 TL veya altında bilgi güvenliğine dair yıllık gider harcayanlarda bu oranın %48,05 olduğu görülmektedir. Bu sonuç araştırmanın "**H_7: Veri Güvenliğinden Yasal Sorumlu Olunduğunun Farkında Olunması, Bilgi Güvenliğine Bütçe Ayrılmasında Etkilidir**." Hipotezinin desteklendiğini göstermektedir.

H8: Bilgi Güvenliğinden Sorumlu Komisyon Kurulmuş Olması, Verilere İlişkin Prosedür ve Politikaların Oluşturulmasında Etkilidir.

Tablo 82. Bilgi Güvenliğinden Sorumlu Bir Kurul/Komisyon/Birim Bulunması ile Verilerin İşlenmesi, Saklanması, Korunması ve İmhası Konusunda Prosedür ve Politikalar Belirlenmesi Arasındaki İlişkinin İncelenmesi

Şirketinizde Bilgi Güvenliğinden Sorumlu Bir Kurul/Komisyon/Birim Bulunmakta mıdır?		Şirketinizdeki Verilerin İşlenmesi, Saklanması, Korunması ve İmhası Konusunda Prosedür ve Politikalar Belirlenmiş midir?			**Toplam**	χ^2	**p**
		Evet	Hayır	Fikrim Yok			
Evet	n	41	0	78	119	99,848	0,001*
	%	34,5%	0,0%	65,5%	100,0%		
Hayır	n	16	80	87	183		
	%	8,7%	43,7%	47,5%	100,0%		
Fikrim Yok	n	11	70	74	155		
	%	7,1%	45,2%	47,7%	100,0%		
*p<0.05; Ki-kare analizi yapılmıştır. Yüzdeler satıra göre verilmiştir.							

Tablo 82 incelendiğinde, şirketlerde bilgi güvenliğinden sorumlu bir kurul/komisyon/birim bulunması ile verilerin saklanması, korunması, işlenmesi ve imhası konusunda prosedür ve politikalar belirlenmesi arasındaki ilişkinin anlamlı olduğu belirlenmiştir (χ^2:99,848; p=0,001<0,05). Bilgi güvenliğinden sorumlu bir birim bulunduranların %34,5 oranıyla verilerin korunması, işlenmesi, saklanması ve imhası konusunda prosedür ve politikaları belirlediği, birim bulundurmayanlarda bu oranın %8,7'ye düştüğü, fikri olmayanlarda ise bu oranın %7,1 olduğu belirlenmiştir. Bu sonuç araştırmanın **"H_8: Bilgi Güvenliğinden Sorumlu Komisyon Kurulmuş Olması, Verilere İlişkin Prosedür ve Politikaların Oluşturulmasında Etkilidir.."** Hipotezinin desteklendiğini göstermektedir

H9: Şirket Personeline Bilgi Güvenliğine İlişkin Eğitim Veren Firmalar, Personel Sözleşmelerine Bilgi Güvenliği, Sır Saklama Yükümlülüğe İlişkin Hüküm Koyulması Gerektiğinin Farkındadırlar.

Tablo 83. Şirket Çalışanlarına Veriler ve Bilgi Güvenliğine İlişkin Eğitim Verilmesi ile Şirket Çalışanlarının İş Sözleşmelerinde, Bilgi Güvenliği Hükümlerine Yer Verilmesi Arasındaki İlişki

Şirketinizin Çalışanlarına Veriler ve Bilgi Güvenliğine İlişkin Teknik, İdari ve Yasal Hak ve Yükümlülükler Eğitim Verildi mi?		Şirket Çalışanlarınız ile Aranızdaki Sözleşmelerde, Bilgi Güvenliği, Gizlilik ve Sır Saklama Yükümlülüğüne İlişkin Hükümlere Yer Verilmiş midir?			**Toplam**	χ^2	**p**
		Evet	Hayır	Fikrim Yok			
Evet	n	70	32	29	131	16,943	0,002*
	%	53,4%	24,4%	22,1%	100,0%		
Hayır	n	52	49	60	161		
	%	32,3%	30,4%	37,3%	100,0%		
Fikrim Yok	n	60	57	48	165		
	%	36,4%	34,5%	29,1%	100,0%		
*p<0.05; Ki-kare analizi yapılmıştır. Yüzdeler satıra göre verilmiştir.							

Tablo 83 incelendiğinde, şirket çalışanlarına veriler ve bilgi güvenliği konusunda eğitim verilmesi ile personel sözleşmelerinde bilgi güvenliği, gizlilik ve sır saklamaya ilişkin düzenlemelere yer verilme durumu arasındaki ilişkinin anlamlı olduğu belirlenmiştir (χ^2:16,943; p=0,002<0,05). Eğitim veren firmaların %53,4 oranıyla şirket çalışanları ile aralarındaki sözleşmelerde, gizlilik, bilgi güvenliği ve sır saklama yükümlülüğüne ilişkin hükümlere yer verdiği belirlenirken, eğitim vermeyen firmalarda bu oranın %32,3'e düştüğü, fikri olmayanlarda ise bu oranın %36,4 olduğu belirlenmiştir. Bu sonuç araştırmanın **"H9: Şirket Personeline Bilgi Güvenliğine İlişkin Eğitim Veren Firmalar, Personel Sözleşmelerine Bilgi Güvenliği, Sır Saklama Yükümlülüğe İlişkin Hüküm Koyulmasının Farkındadırlar."** Hipotezinin desteklendiğini göstermektedir.

6. BİLGİ GÜVENLİĞİ POLİTİKA ÖNERİSİ

Firmalar, lojistik faaliyetlerini gerçekleştirirken bireylerden, işletme ve/veya kurumlardan edindikleri bilgileri kayıt ederek depolamakta ve gerektiğinde üçüncü taraf kişi, işletme ve/veya kurumlar ile paylaşmaktadır. Firmanın bilgi varlıklarının gizliliği, erişilebilirliği ve bütünlüğü temel prensip olarak korunmalıdır. Bu koruma, yasal düzenlemeler gereğince de zorunludur.

Bilgi güvenliği politikaları, işletmeler için, önemli bilgilerinin yönetimi, korunması ve dağıtımı ile kritik görevlerin korunmasını sağlayan kurallar ve yönergelerdir (Yılmaz, 2018).

Çalışma kapsamında, lojistik işletmeler için öneri olarak oluşturulan bu model, bilgi güvenliği politikasının uygulanabilir olması için, ülke genelinde faaliyet gösteren 5413 lojistik işletmesi araştırma evreni olarak belirlenmiştir. Ankete tutarlı geri dönüşler incelendiğinde araştırmanın örneklemi 457 firmadan oluşmaktadır. Anket bulgularından hukuki, teknik ve idari yönleri ile yararlanılmıştır. Çalışma kapsamında, verilerin korunmasına ilişkin yasal düzenlemeler, uluslararası bilgi güvenliği standartları, yargı ve kurul kararları, örnekler ve literatür araştırmaları dikkate alınmıştır. Bilgi güvenliğinin sağlanmasında firma üst yönetiminin desteği önemlidir ve tüm şirket birimlerine sorumluluk yükleyen, denetlenebilen bu bilgi güvenliği politikasında, lojistik işletmeler ile veri sahipleri ve üçüncü kişiler ve kurumların uyması istenilen hususlar düzenlenmektedir.

6.1 Amaç

Madde 1-

Bu politika ile, lojistik işletme tarafından kaydedilen bilgi varlıklarını korumak üzere, idari, hukuki ve teknik önlemleri kapsayan, yasal düzenleme ve sözleşmelere bağlı yükümlülükleri belirleyerek, şirket çalışanları ile diğer ilgili tarafların uyacakları hak ve sorumlulukları tanımlayan ve yasal düzenlemeleri dikkate alarak, düzenli şekilde güncellenmesini hedefleyen, bir model bilgi güvenliği politikası oluşturulması amaçlanmıştır.

6.2 Kapsam

Madde 2-

1- Bilgi güvenliği politikası, lojistik işletmesi ana merkez, şube, depo, acente, saha, mağaza gibi tüm bağlı bina ve tesisleri, tüm bağlı birimleri ve lokasyonlarında yürütülen tüm faaliyetlere ve faaliyetler sırasında kayıt altına alınan, fiziki ve dijital ortamda depolanan, saklanan, kullanılan, paylaşılan ve imha sürecinde olan kişisel veri ve tüzel kişi veri tüm bilgi varlıklarını, tüm bilgi sistemlerini, bilişim ağları ve altyapısı, yazılımları, bilgi işlenen tüm süreçleri ve üst yönetim ile tüm personeli, lokasyon içi ve dışı müşteri, tedarikçi, proje ortakları, yükleniciler ile üçüncü kişi olarak bilişim sistemlerine ve fiziki bilgi ortamlarına erişim sağlayan kullanıcıları ve bilişim sistemlerine teknik destek hizmeti sağlamakta olan yazılım, donanım veya hizmet sağlayıcıları olan tüm kişi ve kurumları kapsar.

2- Yukarıda kapsamı belirtilen şirketin üst yönetim kademesi ve tüm çalışanları, politikada belirtilen hak ve sorumluluklar ile öngörülen kuralları bilmek ve bunlara uymakla yükümlüdür. Politika, farklı türdeki sözleşmeler aracılığıyla lojistik şirket birimlerinde kayıt altına alınan verilere erişim yetkisi tanınan, üçüncü taraf şirket personeli ve/veya diğer üçüncü kişiler ile bilgi paylaşımında bulunulan tedarikçi, paydaş, yüklenici gibi kişileri de kapsamaktadır. Bu kişiler de, politika düzenlemesine uymak zorundadır.

3-Yönetim, şirket içi yapı ve rol dağılımı;

Şirket üst yönetimi altında faaliyet gösteren kapsam içindeki birimler; Gümrük, Sigorta, Stok Yönetimi, Satınalma, Mali ve İdari İşler, Depo Hizmetleri, Antrepo Hizmetleri, Ulusal ve Uluslararası Taşımacılık, Muayene ve Gözetim, İnsan Kaynakları Müşteri Hizmetleri, Kurumsal İletişim ve İş Geliştirme, Hukuk, Finans, Satış, İhracat, İthalat, Bilgi Teknolojileri, Pazarlama, Katma Değerli Hizmetler Paketleme, Kargo, Proje Yönetimi.

6.3 Tanımlar ve Kısaltmalar

Madde 3- Bu politikada adı geçen;

a- Bilgi Güvenliği: Bilginin gizliliği, bütünlüğü ve erişilebilirliğinin risklere karşı korunmasıdır.

b- Kişisel Veri : 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.

c- Tüzel kişi verileri: Tüzel kişiliğe dair her türlü bilgidir.

d- Bilgi varlığı: Şirketin kayıt altına aldığı, depoladığı ve paylaştığı, faaliyetlerini kesintisiz sürdürebilmesi için kritik öneme sahip varlıklardır.

e- Bilgi Güvenliği Politikası: Bilgiyi kötü niyetli girişimlere ve gizliliğine, bütünlüğüne ve kullanılabilirliğine zarar verebilecek eylemlere karşı korumak amacıyla hazırlanan politikadır.

f-Veri sorumlusu: 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

g- Veri işleyen: 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.

h- Bilgi sistemleri : Bilgilerin kaydedildiği, depolandığı ve paylaşıldığı elektronik ortamlar ve ekipmanlar, bilgisayarlar, sunucular, akıllı telefon, disket, kartuşlar, yedekleme birimleri, faks makineleri, yazıcılar gibi elektronik sistemlerle ilişkili ve bunlarla ilgili tüm yazılım, uygulama ve programlardır.

i-Bilgi Güvenliği Komisyonu: Bilgi güvenliği politikalarının oluşturulması, uygulanıp izlenmesi süreçleri için üst yönetim temsilcisi, hukuk, bilişim, finans, idari personel gibi temsilcilerden oluşan, bilgi güvenliği yönetim sisteminin uygulanması ve denetlenmesine ilişkin yetkilere ve sorumluluklara sahip, şirket yönetimi tarafından belirlenen komisyondur.

j- Bilgi Güvenliği Yönetim Sistemi: Bilginin mahremiyeti, tamlığı ve ulaşılabilirliğini temin etmek için planlanmış, yönetilebilir ve belgelenmiş, uluslararası bilgi güvenliği standartlarının temel alındığı bir dizi faaliyetler bütünüdür.

k- Veri envanteri: Şirket tarafından elektronik ve/veya fiziksel ortamlarda kayıt altına alınan tüm bilgi varlıkları ile bu bilgilerin hangi birim ve ortamlarda kayıt altına alındığını gösterir belge.

l- Şirket Üst Yönetimi: Şirketin en üst organı genel kurul ya da şirket ölçeğine göre şirketin sahibidir.

m- Anonim hâle getirme: 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan, kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

n- Siber Saldırı: Bilgisayarlarda ve bilgisayar ağlarında gerçekleşen saldırılar, bir bilgi varlığını ifşa etme, değiştirme, işlevsiz hale getirme, yok etme, ve/veya yetkisiz erişim sağlama veya yetkisiz kullanımı teşvik etme girişimidir.

o- İlgili kişi: 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan kişisel verisi işlenen gerçek kişi.

ö- Üçüncü Kişi: Veri işleyen ile veri sorumlusu haricindeki bireyler ve kurumlardır.

p- Risk değerlendirilmesi: Bir bütün olarak risk belirleme, risk analiz etme ve risk değerlendirme faaliyetidir.

r- Veri Sahibi: Verisi işlenen gerçek ya da tüzel kişilerdir.

s- Gizlilik dereceli bilgi: Şirket menfaatleri açısından sakıncalı görüldüğü için, yetkili kişiler haricindekilere açıklanması veya iletilmesi yasaklanan ve önem derecelerine göre "Çok gizli", "Gizli", "Özel" şeklinde sınıflandırılan bilgiler.

KVKK : Kişisel Verilerin Korunması Kanunu

TCK : Türk Ceza Kanunu

6.4 Bilgi Güvenliği Organizasyon Yapısı

Madde 4-

Şirket bünyesinde bir bilgi güvenliği organizasyon yapısı bulunmaktadır. Bu yapı da gerekli hallerde güncellemeler yapılır.

Bilgi güvenliğini sağlamak üzere, şirket bünyesinde bu konuda görevli ve üst yönetime bağlı bir komisyon kurulur. Komisyon, şirket üst yönetiminden temsilci ile hukuk, insan kaynakları, bilişim, operasyon sorumluları ve diğer idari birimlerin temsilcilerinden oluşur. Komisyon, şirket bilgi varlıklarının gizliği, bütünlüğü ve erişilebilirliği temel unsurlarının korunmasından ve bilgi güvenliği politikalarının uygulanmasından sorumludur.
Her birim yetkilisi, kendi birim çalışanlarının şirket bilgi güvenliği prosedür ve politikalarına uygun davranmalarını sağlamak, denetim ve takibinden sorumludur. Birimler nezdindeki verilere ve verilerin kayıt altına alındığı ortam ve sistemlere erişim yetkilendirmeleri ile rol ve sorumluluk dağıtımı, birim yöneticileri tarafından belirlenerek komisyon onayına sunulur. Komisyon onayı ile yetkilendirmeler yapılarak uygulamalar takip edilir.

6.5 Yetki ve Sorumluluklar

6.5.1 Şirket üst yönetim kademesinin yetki ve sorumlulukları

Madde 5-

Şirket üst yönetim kademesi, şirkete liderlik ve bağlılık göstermek üzere, bilgi güvenliği yönetim sistemi çerçevesinde aşağıdaki hususları yerine getirmekle sorumludur.

1- Bilgi güvenliği politikası oluşturulmalı ve firmanın stratejik hedefleriyle uyumlu hale getirilmelidir. Bu amaçla, üst yönetimin sorumluluğunda ve üst düzey yönetici temsilcilerinin de katılacağı bir bilgi güvenliği komisyonu kurulmalıdır. Komisyonun üye yapısı, üye sayısı, görev süresi ve toplantı sıklığı, şirket birimleriyle istişareler sonucunda üst yönetim tarafından belirlenir.

2- Şirket üst yönetimi, bilgi güvenliği yönetim sistemi kapsamında gerekli olan kaynakların erişilebilirliğinin temin edilmesi ve bütçe tahsisinden sorumludur. Bilgi güvenliği politikasının şirket içinde duyurulması üst yönetimin sorumluluğundadır. Üst yönetim bu görevini, bilgi güvenliği komisyonuyla birlikte veya şirket içinden yetkilendireceği birim yöneticileri aracılığı ile yerine getirebilir. Bilgi güvenliği yönetim sisteminin uygulanmasından ve denetlenmesinden ise komisyon ile birlikte sorumludur.

3- Üst yönetim, çalışanların bilgi güvenliği yönetim sisteminin performansına katkıda bulunmalarını teşvik etmekten, sürekli iyileştirmenin sağlanması ve desteklenmesinden sorumludur. Bilgi güvenliğinin sağlanmasıyla ilgili olarak sorumluluk ve yetkililerin atanması ve şirket içinde duyurulması görevini, komisyon ile birlikte yerine getirir.

4- Üst yönetim, bilgi güvenliği politikalarının uygulanması için gerekli olan koordinasyonu sağlama yetkisine sahiptir. Üst yönetimin liderliği ve katılımı, bilgi güvenliği kültürünün oluşturulması ve devam ettirilmesinde önemli bir rol oynamaktadır.

5- Üst yönetim, kişisel, tüzel kişi verileri ve kayıt edilen diğer verilerin yasal düzenlemelere aykırı olarak elde edilmesi, paylaşılması, değiştirilmesi, yetkisiz olarak açıklanması veya aktarılmasına engel olmak üzere her türlü hukuki, teknik ve idari tedbirleri almakla sorumludur.

6- Üst yönetim, bilgi güvenliği yönetim sisteminin şirket açısından uygun ve yeterli olup olmadığını ve etkinliğini sağlamak amacıyla belirli aralıklarla planlanan kontrol etme faaliyetlerini yerine getirme sorumluluğundadır. Bu görevini komisyon aracılığı ile yerine getirebilir.

7- Üst yönetim, bilgi güvenliği politikalarının uygulanması, süreçlere etkileri, çalışanların uyumu, aksayan yönler, iyileştirme çalışmalarının takibi şeklindeki işlemleri, bilgi güvenliği komisyonu ile birlikte yapabileceği gibi sadece kendisi de yapabilir. Bilgi güvenliği ile ilgili alınacak nihai kararlar, öngörülen değişiklikler, yenilemeler üst yönetimin onayına sunulacaktır. Komisyon belli aralıklarla üst yönetime rapor sunmakla sorumludur.

8- Komisyon tarafından sunulan raporlarla ilgili gerekli önlem ve aksiyonları alarak gerekli revizyonları planlamak üst yönetimin sorumluluğundadır.

9- Üst yönetim üyelerinin, bilgi güvenliğine ilişkin olarak süreç içerisinde elde edilen bilgi varlıklarını başkalarına bildirmeme, kendi menfaatine olacak şekilde kullanmama sorumluluğu ve yükümlülüğü bulunmaktadır. Bu yükümlülük üst yönetim üyelerinin görevden ayrılmaları durumunda da devam eder.

Üst yönetim üyeleri dahil olmak üzere tüm şirket personeli ve bilgi paylaşılan tedarikçi, iş ortakları gibi üçüncü kişiler bilgi güvenliği politikasına uymakla yükümlüdür. Aksi davranışlara ilişkin yaptırımlar komisyon tarafından belirlenerek uygulanacaktır.

10- Üst yönetim tarafından alınan kararlar, yapılan değişiklikler, şirkete bağlı tüm birimlere duyurulur.

6.5.2 Bilgi güvenliği komisyonunun yetki ve yükümlülükleri

Madde 6- Bilgi güvenliği komisyonu;

1- Şirket üst yönetiminin liderliğinde, şirket birim temsilcileri ve üst yönetim temsilcisinin katılımı ile oluşur. Komisyon, şirketin amaç, ihtiyaç ve hedeflerine uygun bilgi güvenliği politikalarının planlanması, oluşturulması, uygulanması, güncellenmesi, yeniden değerlendirilmesi ve iyileştirilmesinden sorumludur. Verilerin ne şekilde işleneceği, saklanarak korunacağı ve imha edileceği konusunda prosedür ve politikaların hazırlanması ve denetimlerinin yapılmasından sorumludur. Komisyon, kişisel verilerin korunması kanunundan kaynaklı özel düzenlemelere uyulması ve uygulatılmasından sorumludur. Yasaya ilişkin düzenlemelere politikada yer verilecektir. Bilgi güvenliği politikası uygulamalarının denetiminden komisyon sorumludur.

2- Bilgi güvenliği komisyonu, şirketin tüm birimleri arasında bilgi güvenliği sorumluluklarının paylaşılması ve politikaların uygulanması için ihtiyaç duyulan koordinasyonu sağlama yetkisine sahiptir.

3- Komisyon, şirket bünyesinde ve bağlı birimler nezdinde bilgi varlık envanterlerinin çıkarılması, risk ve önemine göre sınıflandırılması, derecelendirilmesi, risk belirleme, risk analiz ve risk değerlendirilmesi çalışmalarına rehberlik eder, uygulamaları denetler. Risklerin gerçekleşmesi halinde ortaya çıkabilecek zararlar konusunda birimler bünyesinde çalışmalar yapılmasını denetler ve hazırlanan zarar raporlarını inceler. Tüm

yapılan çalışmaları rapor halinde üst yönetimin bilgi ve onayına sunmak komisyonun görevidir.

4- Şirket birimleri tarafından iletilen bilgi varlıklarında, veri güvenliği risklerini değiştirecek bir durum ortaya çıktığında, risklerin yeniden değerlendirilmesi için yetkili birimleri görevlendirmekle sorumludur. Lojistik işletme, genel olarak, kişisel veriler yanında, müşteri verileri, ticari sırlar ile işletme kayıtları, yönetimsel bilgiler, sektör verileri, sürdürülen operasyonlara ilişkin veriler, sipariş verileri, sigorta, finansal veriler, gümrük, depo, taşıma bilgileri gibi çok çeşit ve sayıda veri işlemekte ve saklamaktadır. Bilgi varlıklarında meydana gelebilecek değişiklerin takibi ile yenilerin envantere eklenerek derecelendirilmesi ve imha edilenlerin envanterden çıkarılma işlemi komisyonun görevlendirmesi ile yapılacaktır.

5- Komisyon, kamuya açık olan ve şirket içinde paylaşılmasına izin verilen bilgi belgeler ile çok gizli (yüksek gizlilik seviyeli) ve gizli bilgi ve belgeleri belirler. Ticari sır kapsamında olan belge ve bilgileri çalışanlar açısından belirgin hale getirir.

6- Komisyon, şirket bilgi güvenliğini sağlamaya yönelik olarak yapılacak yetkilendirmeler ve sorumlu görevli ataması, rol ve görevlerin dağılımı, denetimi ve koordinasyonundan sorumludur. Şirketin her birimi, kendi bölümüne ait verilerin muhafaza edildiği fiziki ortamlara, veri depolama alanları, bilgi sistem ortamları ve bilgisayarlara erişebilecek ve güvenliğini sağlayabilecek sorumlu kişilerin belirlemesinden sorumludur. Belirlenen kişiler komisyona sunularak, komisyon tarafından onaylandıktan sonra rol, görev ve yükümlülükler ilgili personele bildirilecektir. Bildirim, birim yetkilisi tarafından yapılacaktır.

7- Veri depolama alanlarının ve bilgi sistem ortamlarının hırsızlık, izinsiz giriş, deprem, sel, yangın, su baskını gibi olaylara karşı fiziksel güvenlikleri, komisyon öncülüğünde birim yetkililerinin belirleyeceği kişiler tarafından sağlanacaktır. Bu alanlara girişlerde kayıt alınması ve bunların korunması sağlanacaktır.

8- Komisyon, bilgi güvenliğini sağlamaya ilişkin politika ve prosedürlerin şirket birimlerinde uygulanmasını izler, tam olarak uygulanmasını denetler, gerekli hallerde

müdahalelerde bulunur, iletilen aksaklık ve başvurulara ilişkin olarak birim temsilcileri ile değerlendirmeler yaparak karar alma yetkisine sahiptir. Bilgi paylaşılan, şirket adına veri işleyen, hizmet alınan vb. diğer üçüncü kişilerin bilgi güvenliği uygulamalarının şirket bilgi güvenliği politikalarına uygunluğunun takip edilmesi ve denetimi şirket birimleri aracılığı ile komisyonun sorumluluğundadır. Komisyonun, bilgi güvenliği uygulamalarını belirli aralıklarla üst yönetime raporlama sorumluluğu bulunmaktadır.

9- Bilgi güvenliğiyle ilgili yasal değişiklikleri, teknik yenilikleri takip etmek ve gerektiğinde şirket bilgi güvenliği politikasında gerekli değişiklikleri yapmakla sorumludur. Ayrıca teknik donanımların yedekleme, bakım, güncellemeleri ve gereken bilgi güvenliğini sağlamaya yönelik deneme testlerinin organize şekilde düzenli olarak yapılmasını sağlamakla yükümlüdür. Bu hizmetin şirket içinden ya da dışından alınması mümkündür. Şirket dışından alınacak hizmetlerde akdedilecek sözleşme içeriğinde, hizmeti verenlerin, gizlilik, sır saklama ve şirket bilgi güvenliği politikalarına uygun davranacağına ilişkin düzenlemelere yer verilecektir.

10- Komisyon, belli aralıklarla yapacağı iç denetimler ile, bilgi güvenliği yönetim sisteminin, şirket gereklerine ve uluslararası standartlara uygun ve verimli bir şekilde uygulanmakta ve sürdürülmekte olup olmadığını denetlemekle yükümlüdür. Şirket, bilgi güvenliği yönetim sisteminin etkinlik, yerindelik ve yeterliliğini sürekli olarak geliştirmekle yükümlüdür.

11- Komisyon, sistemlere uzaktan erişim ile ilgili riskleri tanımlayarak, uzaktan erişim hakkının kimlere verileceğine karar verme yetkisine sahiptir. Uzaktan erişim yetkilendirilmesi öncesinde, riskler ayrıntılı bir biçimde incelenecek ve gereken güvenlik önlemleri alınacaktır.

12- Komisyon, şirket çalışanlarına veriler ve bilgi güvenliğine dair teknik, idari ve hukuken sahip oldukları haklar ve sorumluluklar konusunda eğitim düzenlenmesi, sonuçların ölçümlenmesi ve değerlendilmesinden sorumludur. Gerekli hallerde verilen lojistik hizmete özel, şirketin ihtiyaçlarına uygun bilgi güvenliği eğitimleri düzenlenecektir. Komisyon, çalışanların uymak zorunda olduğu, temiz alan ve ekran kurallarını hazırlayarak çalışanlara duyurmakla sorumludur.

13- Komisyon, veri ihlali yaşanmasını önleyecek tüm tedbirleri almakla yükümlüdür. Buna ilişkin sözleşmelerin düzenlenmesi, personel ve üçüncü taraflarca imzalanmasının sağlanması komisyonun takip ve denetimindedir. Bilgi güvenliğine ilişkin olarak alınacak tüm idari, hukuki, teknik önlemlerin uygulamalarının takibi, denetimi, iyileştirilmesi komisyonun sorumluluğundadır. Komisyon, kişisel verilerin korunması kapsamında, mevzuat gereğince gerekli olan tedbirleri alacaktır.

Olası veri ihlallerinin zamanında tespit edilebilmesine yönelik prosedürlerin hazırlanması komisyonun görevidir. Veri ihlali halinde izlenecek süreçler ve olaya müdahale planlarının oluşturulması ve alınacak diğer tedbirler ile ilgili olarak gerekli düzenlemeleri yerine getirmekten sorumludur. Bu görevlerini birim yetkilileri ile birlikte koordineli çalışarak yapabilir.

14- Komisyon, personel kaynaklı veri ihlallerinde uygulanacak disiplin sürecini belirlemekle sorumludur. İş akdi sona eren ya da görev değişikliği yapılan çalışanlara ilişkin yürütülecek bilgi güvenliği tedbirlerini belirlemek ve uygulamaları denetlemek komisyonun sorumluluğundadır. Aynı durum veri ihlalinde sorumluluğu olan, şirket bilgi güvenliği prosedürlerine uymayan tedarikçi, iş ortakları, destek hizmeti verenler gibi üçüncü kişilere karşı uygulanacak tedbirler için de geçerlidir.

15- Herhangi bir konuda şirket dışındaki kişi/kişiler/kurum'dan alınan hizmetlerde, hizmeti sunan taraf ile sözleşme imzalanacaktır. Veri işleyen, veri sorumlusu lojistik şirketinin talimatlarına uymak zorundadır. Kişisel veriler ile ilgili olarak, kişisel verilerin korunması mevzuatına uygun şekilde hareket etmek zorundadır. Kişisel verileri kayıt etme, saklama ve imha politikası ile sır saklama yükümlülüğüne uymak ve veri ihlallerini derhal veri sorumlusuna iletmek zorundadır. Veri sorumlusu lojistik şirketi, kişisel veri içeren sistem üzerinde denetim yapma/yaptırma hak ve yetkisi ile veri işleyenin bilgi güvenliği uygulamalarını denetleme yetkisine sahiptir. Komisyon tarafından hazırlanacak sözleşmede bu hususların tümüne yer verilecektir.

16- Veri ihlali durumunda gerekli idari ve yasal girişimlerde bulunmak komisyonun görevidir. Kişisel verilerin ihlali halinde, durum kişisel verileri koruma kuruluna bildirilecektir. İlgililer hakkında yasal ve idari girişimlerde bulunulacaktır. Veri ihlali

komisyon üyelerinden kaynaklı ise, bu halde o üye/üyelerin ivedi olarak yetkileri sonlandırılacak ve yasal, idari işlem başlatılacaktır. Komisyon durumu bir rapor halinde üst yönetime iletmekle yükümlüdür.

17- Komisyon, tespit edilen bilgi güvenliği ihlalleri, sistem açıkları, idari ve hukuki eksiklikler, yetkisiz erişim ve kötü niyetli yazılımlar ile ilgili düzenli olarak rapor hazırlayarak üst yönetime sunmakla yükümlüdür.

18- Komisyon üyeleri, faaliyetleri ve denetim süreçlerinde edindikleri bilgileri, üst yönetim ve şirketin yetkili bölümlerinden başkasına açıklamama ve kendi menfaatine kullanmama yükümlülüğü altındadırlar. Bu yükümlülükleri, komisyon üyelerinin görevden ayrılmaları durumunda da devam edecektir.

19- Komisyonun bilgi güvenliği ile ilgili aldığı kararlar ve gerekli durumlarda yapılan değişiklikler, şirkete bağlı tüm birimlere duyurulur.

6.5.3 Şirket personeli ve diğer üçüncü kişilerin yükümlülükleri

Madde 7- Tüm şirket çalışanları;

1- Bilgi güvenliğinin sağlanması, yasal düzenlemelere ve şirketin bilgi güvenliği politikasına uygun hareket etmek ve uygulamakla yükümlüdür.

2- Şirketin düzenleyeceği bilgi güvenliği eğitimlerine, seminer ve toplantılara katılmakla yükümlüdür. Etkinlik bitiminde yapılacak olan değerlendirmelere katılacaklardır. Aynı zamanda çalışanlar yönetimden, bilgi güvenliği eğitimi verilmesini, yasal düzenlemeler konusunda bilgi verilmesini, bunun için de eğitici seminer ve toplantılar düzenlenmesini talep etme hakkına sahiptir.

3- Bilgi güvenliği ihlali ile karşılaştıklarında durumu birim müdürüne bildirmekle yükümlüdür. İhlalin birim müdürü tarafından yapılması halinde durumu, zaman kaybetmeksizin şirket bilgi güvenliği komisyonuna bildirmekle yükümlüdür.

Çalışanlar, bilgi güvenliği politikasına aykırı hareket edildiği hallerde durumu birim müdürüne bildirmekle yükümlüdür. Bilgi güvenliği politikasına aykırı harekette bulunan birim müdürü ise, bu halde çalışanlar durumu zaman kaybetmeksizin şirket bilgi güvenliği komisyonuna bildirmekle yükümlüdür.

Sözkonusu ihlaller, belirli sözleşmeler ile şirket verilerine ulaşma ve paylaşım yapabilme yetkisi tanınmış üçüncü kişiler tarafından yapılması halinde durum, derhal birim müdürlerine bildirilecektir.

4- Çalışanların sır saklama ve gizliliğe uyma borçları gereğince, öğrenmiş oldukları şirket bilgi ve belgelerini paylaşmama, kendisi için kullanmama, gizliliğe uyma sorumluluğu bulunmaktadır.

5- Çalışanların, yetkili olmadıkları sürece, verilerin kayıtlı olduğu sistem ve bilgisayarlar ile fiziksel ortamlara erişim hakkı ve fiziksel ortamlarda bulunma hakkı bulunmamaktadır. Bu alanlara ancak birim müdürünün önerisi ve komisyonun onayı ile yetkilendirilen kişi/kişiler erişebilecektir. Dijital sistem ve fiziki ortamlara girebilecek kişiler, komisyon onayı sonrasında kesinleşerek rol, görev ve yükümlülükler ilgili personele bildirilecektir.

6- Bilgi sistemleri ve fiziki ortamlara giriş yetkisi bulunan çalışanlar, şifreleri ile giriş ekipmanlarını korumak ve bu ortamlara izinsiz olarak erişimi önlemekle yükümlüdür. Çalışanlar, kendilerine tahsis edilen kullanıcı kimliği ve şifreleri, özel olduğundan kimseyle paylaşmamalıdır. Kullanıcı kimlikleri ile şifrelerin güvenliğinden şüphelenildiğinde, durum birim yetkilisine bildirilerek şifrelerin değiştirilmesi sağlanmalıdır. Yetkili çalışan, bilgi sistem ve fiziki ortamlarda çalışmaları sona erdiğinde, teknik ekip tarafından bildirilen tüm güvenlik talimatlarına uymakla yükümlüdür.

7- Çalışanların işleri bittiğinde, kişisel ve şirkete ait bilgiler içeren belge ve dökümanlar ile şifre, kullanıcı adı yazılı materyalleri çalışma ortamlarında bırakmamak ve bunları kilitli alanlarda korumak yükümlülüğü bulunmaktadır. Birim yetkilileri uygulamaları belirli aralıkla denetleyerek uymayanlar hakkında idari işlem başlatacaktır.

8- Çalışanlar, şirkete ait ve kamunun erişimine kapalı olan bilgi ve belgeleri amir onayı olmadan başkaları ile paylaşamaz. Komisyon tarafından belirlenen kurallara uymakla yükümlüdür. Yasa gereğince kurumların bilgi ve doküman isteğinde bulunması durumunda, durumu birim yetkilisine bildirmek zorundadır. Birim yetkilileri, komisyonun yazılı izni ile talep edilen bilgileri, yetkili makamlara tam ve doğru olarak iletme sorumluluğundadır.

9- Çalışanlar, gönderim yeri belirsiz ve bilmedikleri adreslerden gönderilen ek dosyaları ve mailleri açmamalı, diğer hiçbir mail adresine göndermemelidir.

Şirketin bilgi paylaşımda bulunduğu ve bilgilere erişim yetkisi tanınmış olan üçüncü kişiler;

1- Şirket dışından teknik destek hizmeti veya başkaca hizmetlerin alınması durumda, bilgi paylaşımında bulunulan ve hizmet gereğince bilgilere erişim yetkisi bulunan üçüncü taraf firma ve çalışanları ile diğer ilgili kişiler, şirketin bilgi güvenliği politikasına uymakla yükümlüdür. Hizmet alınan firma gibi üçüncü taraf firma ve kişiler ile yapılacak sözleşmelerde, sır saklama, gizliliğe uyma ve şirket bilgi güvenliği düzenlemelerine uygun davranılacağına ilişkin hükümlere yer verilecektir.

2- Aynı şekilde, lojistik hizmetlerin sunulması esnasında bilgi paylaşımında bulunulan tedarikçi, paydaş gibi üçüncü kişi ve firmalar ile işçileri ve diğer kişiler için de 1 nolu madde de yer verilen düzenlemeler geçerlidir.

6.6 Bilgi Güvenliği Risk Yönetimi

6.6.1 Risk yönetim sürecinde öncelikli yapılması gerekenler

Madde 8-

Bilgi güvenliği yönetim sistemi çerçevesinde, bilginin gizlilik, tamlık ve ulaşılabilirlik kayıpları ile tehlikelerin tespit edilebilmesi için, bilgi güvenliği risklerinin analizi ve değerlendirilmesi süreci uygulanmalıdır. Ardından, risk işleme ve değerlendirme takip işlemleri sırasıyla gerçekleştirilmelidir.

1- Risk yönetim sürecinin başlangıcında öncelikli olarak bilgi varlıkları belirlenerek veri envanteri çıkarılmalıdır. Bilgi varlıkları değerlendirilmeli sonrada sınıflandırılmalıdır. Basılı ve dijital ortamlarda üretilen, aktarılan, depolanan veya sözlü olarak paylaşılan tüm bilgiler, şirketin bilgi varlıkları kapsamında değerlendirilir. Verilerin paylaşılması, erişilmesi, işlenmesi, depolanması ve iptal edilmesi sürecinde kullanılan uygulamalar, program, ekipman ve yazılımlar da bilgi varlıkları olarak kabul edilmektedir.

Şirket veri envanteri, komisyon önderliğinde, tüm birim yetkililerinin yönlendirmesi ile birimlerin sahip olduğu bilgi varlıklarının tespit edilerek listelenmesi ile yapılacaktır. Bilgi varlıkları türlerine ve kayıt şekillerine (dijital varlıklar, fiziksel varlıklar, yazılımsal varlıklar, servisler gibi) göre gruplandırılacaktır.

2- Envanteri çıkarılan bilgi varlıkları, önceliklerine ve önem derecelerine göre değerlendilmeli ve sınıflandırılmalıdır (Kişisel veri, tüzel kişiliğe ilişkin çok gizli, gizli, herkese açık veri gibi). Bilgi varlıklarına yönelik tehditler, riskler ve açıklar ile bunların şirket birimlerinde yaratacağı etkiler ve zararlar analiz edilmelidir. Bunların şirket iş süreçleri ve itibarı ile ekonomisi üzerinde olası etkileri değerlendirilmeli ve risk değerleri hesaplanmalıdır.

3- Risklerin önceliklendirme işlemi yapılmalıdır. Güvenlik eksikliklerinin tespit edilmesini takiben, eksikliklerden oluşabilecek risklerin kontrol edilebilmesi ve risk seviyesinin düşürülebilmesi amacıyla risk yönetim stratejisi oluşturulmalıdır. Risk analiz ve risk yönetimi süreçleri düzenli aralıklarla uygulanmalıdır. Bilgi varlıklarını koruma masrafları ile değerleri arasındaki dengeyi gözeten bir çalışma yapılmalıdır.

4- Şirket hedeflerine uygun olarak kapsam belirlenmelidir.

6.6.2 Risk yönetimi kapsamında uygulanacak genel unsurlar

Madde 9-

1- Uygulanacak güvenlik seviyelerinin tespiti için bilgi güvenliği komisyonu tarafından değerlendirmeler yapılmalıdır. Ticari sırları, kişisel verileri ve diğer önemli bilgileri barındıran veri depolama alanlarının ve bilgi sistem ortamlarının fiziksel güvenliği ile ilgili riskler değerlendirilmeli ve olası tehditlerin tanımlanması yapılmalıdır. İzinsiz erişim, hırsızlık, yangın, elektrik kesintileri ve doğal felaketler gibi potansiyel risklerin belirlenmesi ve bunların olası sonuçları değerlendirilmelidir.

2- Elektronik sistemlerin güncellenmesi öncesi, potansiyel yeni riskler değerlendirilmeli ve uygun önlemler ile sistem yedekleri alınmalıdır.

3- Şirket dışı bağlantıların, kişisel veriler ve kurumsal kimliğe ait önemli bilgilerin yer aldığı sistemler üzerindeki riskleri değerlendirilmelidir. Uzaktan erişim riskleri belirlenmeli, erişim yetkisi tanınmadan önce gerekli önlemler alınmalıdır. Şirket ve bağlı birimlerde, mail, ileti, dosya gönderimi ile ilgili kısıtlama ve virus tarama önlemleri uygulanmalıdır.

4- Şirketin ticari verileri ile kişisel bilgilerin depolandığı alanlarla ilgili olarak, personelin erişim ve kullanım yetkilerine bağlı riskler belirlenmeli ve personelin kullanım kayıtları düzenli olarak tutulmalıdır.

5- Şirkete teknik destek veya diğer hizmetleri sağlayan firmaların, şirket verilerine erişiminden kaynaklanan potansiyel riskler tespit edilmeli ve gerekli tedbirler alınmalıdır.

6- Şirketin veri paylaşımında bulunduğu ve/veya verilere erişim yetkisi bulunan üçüncü kişilerin yeterli bilgi güvenliği önlemine sahip olup olmadıkları araştırılmalı, tehditler belirlenmeli ve gerekli durumlarda, faaliyetlerin durdurulması ve/veya sonlandırılması seçeneği değerlendirilmelidir.

7- Ticari sır ve kişisel verilerin işlendiği birimlerde taşınabilir cihazların ve sistemlere yönelik kötü amaçlı yazılımların yaratabileceği riskler incelenerek değerlendirilmeli ve gerekli önlemler alınmalıdır.

6.7 Bilgi Güvenliği Önlemleri

6.7.1 Fiziksel güvenlik önlemleri

Madde 10-

1- Kişisel veriler ile tüzel kişiliğe ilişkin gizli nitelikli bilgilerin muhafaza edildiği fiziki ortamların korunması için güvenlik sınırları tanımlanmalıdır. Bu alanlar uygun giriş kontrolleri ile korunmalı, alarm ve kamera sistemleri ile izlenmeli, alanlara girebilecek erişim yetkilileri belirlenmelidir. Yetkisiz fiziksel erişime karşı bu alanlar sürekli olarak izlenmelidir.

Bu alanların yangın, deprem, su baskını gibi çeşitli türden çevresel tehditlere, hırsızlık ve elektrik kesintisi gibi teknik tehditlere karşı korunması planlanmalı ve önlemler alınmalıdır.

2- Fiziksel ortam güvenliği açısından, işyeri çalışma alanlarında veri içeren belgelerin, taşınabilir depolama cihazlarının, şifre ve kullanıcı adı yazılı materyallerin, açık bırakılan bilgisayarlar gibi veriye izinsiz erişimi kolaylaştırabilecek ortamlar oluşturulmamalıdır. Çalışma saatlerinin sonunda, fiziksel ortamdaki bilgisayarlar kapatılmalı, diğer materyallerden temizlenmiş bir şekilde ve belgeler kilitli dolaplarda muhafaza edilecek şekilde bırakılmalıdır.

3- Gizlilik dereceli verilerin bulunduğu bilgisayarlara sistem yöneticileri dışındaki kişilerin fiziksel erişimi yasaklanmalıdır. Bu alanlara, kayıt cihazları ile girilmesi yasaklanmalıdır. Yapılacak teknik ya da başka türden çalışmalara nezaret edilmelidir.

Gizlilik derecesi yüksek ve kişisel verilerin depolandığı bilgisayar ve alanlara, yetkililer dışında erişimin yasak olduğunu belirten uyarılar asılmalıdır.

4- Dinleme faaliyetlerine karşı, gizlilik derecesi yüksek verilerin işlendiği bilgisayar ve sistem odaları gibi bölgelerde gerekli güvenlik önlemleri alınmalıdır.

5- Veri ihlali durumunda, bu alanlara erişim ve alınacak önlemler ile süreçlere ilişkin prosedürler hazırlanmalıdır.

6- Kişisel verilerin korunması için, Kişisel Verilerin Korunması Kanunu hükümleri ile kanunun uygulanmasına ilişkin olarak yayımlanan yönetmelik, idari tedbirlere ilişkin rehber ve diğer tüm düzenlemelere uygun davranılacaktır.

6.7.2 Teknik kontroller

Madde 11-

1- Şirketin kayıt altına aldığı, depoladığı ve paylaşılan verilerin güvenliğinin temin edilmesi için gerekli ve yeterli ölçüde teknik donanım sağlanmalıdır. Güncel değişiklik ve yenilikler takip edilmeli, yeni oluşan risklere karşı teknik önlemler ivedilikle alınmalıdır.

2- Dijital sistemlerin bakım, güncelleme, güvenlik testleri ile teknik donanım yedeklemeleri düzenli olarak yapılmalıdır. Bilgi koruma sistemleri ve ekipmanları düzenli bakım ve güvenlik testlerine tabi tutulmalıdır. Bilgi sistemlerinin varsa teknik açıklıkları tespit edilmeli gerekli önlemler alınmalıdır. Sistemler, ağlar ve diğer tüm cihazlar için düzenli olarak veri sızıntısı testleri gerçekleştirilmeli, risk taraması yapılmalı ve risk ile sızıntıyı önleme tedbirleri alınmalıdır. Potansiyel güvenlik açıkları azaltılmalıdır.

3- Arızalanan ya da bakım için üçüncü kişi kurumlara gönderilen cihazların bakım ve onarım işlemi öncesinde, verilerin güvenliğini sağlamak üzere, cihazlardaki veri saklama bölümü çıkarılarak ayrı bir yerde saklanmalıdır. Sadece arızalı parçalar gönderilmelidir. Verilerin bulunduğu diskler arızalı ise bilgiler yedeklenerek içindeki veriler geri getirilemeyecek şekilde imha edilerek arızalı disk gönderilmelidir.

Bakım ve onarım gibi amaçlarla şirket dışından üçüncü kişinin gelmesi durumunda, verilerin kopyalanarak şirket dışına çıkartılmasını önleyici gerekli tedbirler alınacaktır. Dışarıdan teknik destek alınan durumlarda, işlemler, görevlendirilen şirket çalışanı bir kişinin gözetimi altında yapılmalıdır.

4- Verilerin, yazılım ve sistemlerin yedek kopyaları korunmalı ve oluşturulacak yedekleme politikasına uygun olarak düzenli aralıklarla test edilmelidir. Yedeklenen veriler sadece komisyon tarafından erişilebilir şekilde muhafaza edilecektir. Yedeklerin fiziksel güvenliği sağlanacaktır.

Bilgi sistemleri, cihazlar gibi ortamlarda saklanan bilgilerin kullanılmadığının belirlenmesi amacıyla komisyon tarafından gerçekleştirilen tespitin ardından, veri imha politikasına uygun olarak veriler imha edilecektir.

Kişisel veriler bakımından ise, veri sorumluları, işleme amaçları bakımından depolanan kişisel verilere ihtiyaç olup olmadığını değerlendirecektir. Değerlendirme sonucuna göre, ihtiyaç duyulmayan kişisel verilerin, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yönetmeliğine ve veri saklama ve imha politikasına uygun şekilde ve güvenli bir biçimde imha edilmesi sağlanacaktır.

5- Çalışanlara, yaptıkları iş ve görevler ile bağlantılı, verilen yetki ve sorumluluklar kapsamında, gerekli olduğu ölçüde erişim yetkisi tanınacaktır. Her bir kullanıcı, kullanıcı adı ve şifresi ile sadece yetkili oldukları sistemlere erişim sağlayacaktır. Şifre ve parolaların düzenli aralıklarla değiştirilmesi sağlanacaktır. Çalışanlara tahsis edilen kullanıcı kimliği ve şifreler kişiye özel olduğundan kimseyle paylaşılmamalıdır. Güvenli olduklarından şüphelenildiğinde, durum birim yetkilisine bildirilerek şifrelerin değiştirilmesi sağlanacaktır.

Personelin bilgi sistemlerinde ve fiziki ortamlarda çalışmaları sona erdiğinde, teknik ekip tarafından bildirilen güvenlik talimatlarına uyma ve uygun davranma yükümlüğü bulunmaktadır. Uyulması gereken teknik kurallar bilişim departmanı tarafından hazırlanacaktır.

Verilerin depolandığı sistemlere giriş yetkisi bulunan çalışanlar, çalışmalarının bitmesi ile birlikte, teknik ekip tarafından bildirilen güvenlik talimatlarına uygun olarak sistemden çıkacak ve güvenlik talimatlarına uyacaklardır.

6- Şirket ana bilgisiyar sistemine girişler, birden fazla personelin birlikte hareket etmesi ve şifre paylaşımı ile (giriş şifresinin bölünmesi) sağlanacaktır. Giriş şifresinin bir örneği üst yönetim yetkilisinde bulunacaktır. Şirket ana bilgisayarlarına yetkisiz müdahaleyi önlemek için, sistem izleme ekibi ve bu ekibi haberdar edecek alarm sistemleri kurulacaktır. Veri ihlali veya şifrenin kırılması gibi durumlar içinde alarm sistemi devreye girecek ve teknik personelin derhal olaya müdahale etmesi sağlanacaktır.

7- Sistemlere ayrıcalıklı erişim tahsisi ve kullanımı sınırlandırılacaktır. Şirket üst yönetiminin belirlediği bilgi, belge ve diğer ilgili varlıklara erişimler üst yönetim tarafından kısıtlanabilecektir.

8- Çalışanların kişisel elektronik makinelerinin bilgi sistem ağına bağlanması, riski yükseltebildiğinden, kişisel cihazların ağa erişimine ilişkin kontrol ve kısıtlamalar yapılmalıdır. Bulutta depolanan verilerin tanımlanması, yedeklenmesi ve uzaktan erişim için çift aşamalı kimlik doğrulama kontrolü yapılmalıdır. Ağ güvenliği önlemleri alınmalıdır. Tüm kullanıcıların işlem hareket kayıtları düzenli şekilde tutulmalıdır.

9- Risk derecesi yüksek ticari veriler, kişisel veriler ile gizlilik dereceli diğer veriler, şirket birimlerindeki bilgisayarlar dışında kayıt altına alınmamalı, depolanmamalıdır.

10- Verilerin güvenliğinin temin edilmesi için, çok faktörlü kimlik doğrulama yönteminin kullanılması, depolanan ve iletilen verilerin şifrelenmesi, ayrıca verilere ulaşılmasını engellemek üzere güçlü şifreler belirlenmesi, şifre deneme sayılarının kısıtlanması şeklinde teknik önlemler alınmalıdır.

11- Kişisel verilerin korunması için, Kişisel Verilerin Korunması Kanunu hükümleri ile kanunun uygulanmasına ilişkin olarak yayımlanan yönetmelik, teknik tedbirlere ilişkin rehber ve diğer tüm düzenlemelere uygun davranılması zorunludur.

12- Komisyon tarafından saptanan bilgi güvenliği ihlalleri, sistem açıkları, yetkisiz erişim ve kötü niyetli yazılımlar ile idari ve hukuki eksiklikler ile ilgili üst yönetimin belirleyeceği önlemler ivedilikle yerine getirilecektir.

6.8 Hukuki Düzenlemeler ile Verilerin Korunması

6.8.1 Hukuki ve idari güvenlik önlemleri

Madde 12-

1- Şirket bilgi güvenliği politikası komisyon tarafından hazırlanmalı, üst yönetim tarafından onaylanarak, şirket içinde duyurulmalıdır. Bilgi güvenliği politikası, uygulama ve ihtiyaca göre ve önemli değişiklikler olması halinde kontrol edilerek güncellenmelidir.

Şirket bilgi güvenliği politikasının, kapsamda belirtilen şirket ve tüm bağlı birimlerinde ve bilgi paylaşımında bulunulan üçüncü kişiler nezdinde uygulamaları denetlenmelidir.

2- Şirket verilerinin toplanması, kullanılması, saklanması, imhası, denetimiyle ilgili prosedürler oluşturmalıdır. Kişisel veriler için, kişisel verilerin korunması mevzuatı çerçevesinde uygun tedbirler alınmalıdır.

3- Şirket içindeki ve şirket ile diğer üçüncü taraflar arasındaki veri aktarımları için bilgi aktarım kuralları, prosedür ve anlaşmalar düzenlenerek hazır hale getirilmelidir. Veri güvenliğiyle ilgili hukuki, düzenleyici ve sözleşmeye tabi gerekliliklerin belirlenmesi, belgelendirilmesi ve güncel tutulması sağlanmalıdır. Şirketin bilgi güvenliği önlemleri,

insanlar, süreçler, hukuki düzenlemeler ve teknolojileri içerecek şekilde düzenli aralıklarla kontrol edilmelidir.

Kişisel veriler bakımından zorunlu olduğundan, veri işleyen konumundaki üçüncü kişilerin aldığı bilgi güvenliği tedbirleri belirli aralıklarla denetlenmelidir. Aynı denetim şirketin tüm diğer verilerine ilişkin olarak da yapılmalıdır.

4- Bilgi güvenliğinin sağlanmasına dair şirket içi rol ve sorumluluklar, şirketin gerekliliklerine göre tanımlanacaktır. Verilerin muhafaza edildiği fiziki ortamların güvenliğinden sorumlu kişiler ile sistem bilgisayarlarına erişebilecek sorumlu kişiler ve verilerin muhafaza edildiği fiziki ortamlara erişebilecek yetkili kişiler birim amirleri tarafından belirlenerek komisyon onayı ile atanacaktır. İlgili kişilere görevleri bildirilecektir.

5- Çalışanlar ile akdedilen sözleşmeler ile tedarikçi, iş ortakları gibi üçüncü taraflarla yapılan sözleşmelerde, gizlilik, bilgi güvenliği ve sır saklama yükümlülüklerine dair düzenlemelere yer verilmelidir.

Tedarikçi, iş ortakları gibi üçüncü kişiler ile imzalanan ticari sözleşmelerde, gizlilik yükümlülükleri geniş kapsamlı tutulmalı, ticari sır tanımı geniş kapsamlı yapılmalıdır. Gizlilik yükümlülüğünün, tarafların danışmanları, personeli gibi kişiler içinde uygulanacağı sözleşmede belirtilmelidir.

Tüm çalışanlar ve veri paylaşımında bulunulan üçüncü kişi ve kurumlar şirket bilgi güvenliği politikalarına uymak zorundadır.

6- Olası veri ihlallerinin önlenebilmesi, zamanında tespit edilebilmesine yönelik prosedürler hazırlanmalıdır. Veri ihlali yaşanması durumunda izlenecek süreçler, müdahale planları ve oluşacak kesinti durumunda, bilgi güvenliğinin sürdürülmesine ilişkin planlamalar yapılmalıdır. Oluşacak zarar ve bu halde uygulanacak eylem planları hazırlanmalıdır.

7- Çalışanlara, düzenli aralıklarla bilgi güvenliği eğitimi verilmeli ve yasal sorumlulukları anlatılmalıdır. Şirket bilgi güvenliği politikaları hakkında bilgi verilmelidir. Gerektiğinde güncellemeler yapılarak eğitimler tekrar edilmeli ve sonuçları değerlendirilmelidir.

8- Çalışanlar, amir yazılı izni olmadan, şirketin ticari ve ticari kapsamda bulunmayan işlemleri ile ilgili veriler dahil olmak üzere gizli bilgileri, şirket dışındaki kişisel e-posta hesaplarına veya diğer e-posta adreslerine ya da diğer bir yol ile şirket dışına çıkaramaz, iletemez, paylaşıp depolayamaz. Aynı kural veri paylaşılan, hizmet alınan üçüncü taraflar için de geçerlidir. Çalışanlar hiçbir sosyal mecrada şirkete ait kamuya açık olmayan bilgiler ve/veya ticari sırlara ilişkin paylaşımda bulunamaz. Bu hususlara, sözleşmelerde yer verilmelidir.

9- Çalışanlar, kişisel ve şirkete ait bilgiler içeren belge ve dökümanları, şifre, kullanıcı adı içeren yazılı dokümanları işlemleri bittiğinde açıkta bırakmamalıdır. Şirkete ait bilgileri içeren her türlü ekipman, belge ve materyalin kilitli alanlarda muhafazası sağlanmalıdır. Komisyon tarafından belirlenen temiz ortam kurallarına uyulmalıdır. Uygulamalar birim yetkilileri tarafından belirli aralıklarla denetlenmelidir.

10- Verilerin kayıt edilerek depolandığı dijital sistem ve fiziki ortamlara giriş yetkisi bulunan personel, şifre ve giriş ekipmanlarını korumalıdır. Çalışmaları sona erdiğinde, teknik birim tarafından bildirilen tüm güvenlik talimatlarına uyma ve uygun davranma yükümlüğündedir.

11- Verilere erişim yetkisi bulunan çalışanların, şirkette görev değişikliği olması ya da işten ayrılması halinde, verilere erişim yetkileri derhal sona erdirilmelidir. Verilere erişim yetkisi bulunan, tedarikçi, hizmet alınan veya iş ortakları gibi üçüncü taraf kişi/kurumlar ile sürdürülen iş ilişkisinin sona ermesi durumunda bu kişilerin/çalışanlarının vakit kaybetmeksizin hesaplarının silinmesi ve sisteme girişlerinin kapatılması ile şirket verilerine erişimlerine son verilmelidir.

Bu hallerde, şirket çalışanları ve üçüncü taraf kişilerin/çalışanlarının, ellerinde bulunan şirkete ait her türden belge ve bilgi ile verilerin kayıtlı olduğu tüm cihazların şirkete teslim edilmesi sağlanmalıdır.

12- Çalışanlardan kaynaklanan veri ihlalleri için komisyon tarafından personel disiplin süreçleri hazırlanmalıdır. Veri ihlalinde sorumluluğu bulunan çalışan, şirkete ait bilgi ve belge ile verilerin kayıtlı olduğu cihazları işverene teslim etmelidir. Verilere erişimi ivedilikle sonlandırılmalıdır.

Veri ihlalinde sorumluluğu olan, şirket bilgi güvenliği prosedürlerine uymayan tedarikçi, iş ortakları, destek hizmeti verenler gibi üçüncü kişi/kurumlarla ilişkilere derhal son verilmeli ve veri paylaşımı ivedilikle sona erdirilmelidir. Şirkete ait bilgi ve belge ile verilerin kayıtlı olduğu cihazların şirkete iadesi yapılmalıdır.

Veri ihlalinde sorumluluğu tespit edilen çalışan ve kişi ve/veya kurumlara karşı hukuki ve idari girişimler başlatılmalıdır.

13- Şirket dışından alınan hizmetlerde, hizmeti sunan veri işleyen kişi/kişiler/kurum ile şirket arasında bir sözleşme imzalanmalıdır. Veri işleyen, veri sorumlusu lojistik şirketin talimatlarına aykırı hareket edemez, sözleşmede tanımlanan verileri kaydetme amaç ve içeriğine uygun hareket etmek zorundadır. Kişisel veriler için, kişisel verilerin korunması mevzuatı ile uyumlu olacak şekilde hareket edilecektir. Kişisel veriyi koruma ve iptal etme politikasına uygun davranmalı, sır saklama yükümlülüğüne uymalıdır. Veri ihlallerini derhal veri sorumlusu lojistik şirketine iletmekle yükümlüdür.

14- Şirket veri kaynaklarının kullanılmasına dair delil özelliği taşıyan, veriye erişim bilgisi, tarih, zaman ve süre bilgisi, veriye ulaşılan Ip adresi bilgisi gibi bilgilerin korunması için güvenlik önlemleri alınmalıdır.

15- Yurt dışına kişisel verilerin aktarımı ile ilgili olarak, Kişisel Verilerin Korunması Kanununa uygun düzenlemeler yapılmalıdır.

16- Lojistik hizmetlerin sunulmasında veri ihlallerinin önlenebilmesi için, depo, antrepo ve/veya diğer birimlerde çalışanların yaptıkları işlere özgü bilgi güvenliği ihlallerini engellemek amacıyla, dikkat edilmesi gereken noktalar üzerine özel eğitimler sunulmalıdır. Aynı şekilde, lojistik faaliyetlerin icrasında karşılaşılabilecek spesifik veri ihlalleriyle ilgili olarak, şirketin bilgi güvenliği gereksinimlerine uygun eğitimler düzenlenmelidir.

17- Kişisel Verilerin Korunması Kanunu gereğince, kişisel veriler, kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilirler. Kişisel verilerin işlenme şartları yasada düzenlenmiştir. Kişisel verilerin kayıt edilmesinde bu

düzenlemelere uygun davranılmalıdır. Ayrıca, TCK madde 135'de, hukuka aykırı olarak kişisel verileri kaydedenlere ceza yaptırımı uygulanacağı düzenlenmiştir.

Kişisel verilerin korunması kanununda özel nitelikli kişisel veriler düzenlenmiştir. Bu nitelikteki verilerin işlenmesi yasaktır, ancak yasada belirtilen durumlarda işlenebilecektir. Özel nitelikli kişisel verilerin işlenmesinde yasal düzenlemelere uygun davranılmalıdır. Ayrıca, TCK madde 135/2'de hukuka aykırı olarak kaydedilen kişisel verinin bu nitelikte veri olması durumunda cezanın arttırılacağı belirtilmiştir.

18- Kişisel verileri hukuka aykırı şekilde yayan, başkasına veren veya ele geçiren kişiler içinde TCK 136 madde de ceza düzenlemesine yer verilmiştir. Tüm şirket çalışanları kişisel verilerin korunması kanunu düzenlemelerine uymak zorundadır.

19- Kişisel verilerin yok edilmesi, silinmesi veya anonim hale getirilmesi yasada açıkça düzenlenmiştir, bu düzenlemelere uymak zorunludur. TCK 138 madde de, kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmemeleri halinde ceza yaptırımı düzenlenmiştir.

20- Bir bilişim sistemine hukuka aykırı olarak giren, sistemi engelleyen, bozan, verileri yok edip değiştiren kişiler ile ilgili olarak TCK 243-244 maddelerinde ceza yaptırımı düzenlenmiştir. Şirket ve bağlı birimlerinde gerek kişisel veriler ile ilgili olarak gerekse diğer verilere karşı işlenen bilişim suçlarına ilişkin veri ihlalleri, yetkili birim amirine/komisyona/üst yönetime bildirilmeli ve gereken hukuki ve idari işlemler derhal başlatılmalıdır.

21- Kişisel verilerin korunması ile ilgili olarak, 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri ile kanunun uygulanmasına ilişkin olarak yayımlanan yönetmelik, rehberler, idari tedbirler rehberi ve diğer tüm düzenlemelere uygun davranılması zorunludur.

22- Bilgi güvenliğinin sağlanabilmesi için komisyonun belirlediği sürelerle genel iç denetimler yapılmalıdır. Uygulamaların yasal düzenlemelere, bilgi güvenliği standartlarına ve şirket bilgi güvenliği politikasına uygunluğu denetlenmelidir.

İç denetimler haricinde birim yetkilileri tarafından, kendi birimlerinin bilgi güvenliği uygulama denetimleri düzenli ve sık aralıklarla haftalık ve aylık olarak yapılmalı, aksıyan yönler komisyona rapor olarak sunulmalıdır. Habersiz denetimler ile bilgi güvenliği uygulamaları rutin işleyişi gözlemlenmelidir.

23- Şirketin veri paylaşımında bulunduğu, hizmet aldığı tedarikçi, paydaş gibi üçüncü kişilerin olması durumunda, dış denetimin de etkili bir şekilde ve düzenli aralıklarla yapılması sağlanmalıdır.

24- Bu politika ve ilgili süreçlere uymayan personel hakkında disiplin prosedürü uygulanmalıdır. Şirketin bilgi güvenliği politikasına uymayan üçüncü kişiler için idari prosedür uygulanmalı, gerekli hallerde iş ilişkisi sonlandırılmalıdır. Söz konusu prosedürler komisyon tarafından hazırlanacak, üst yönetimin onayı ile uygulanacaktır.

25- Bilgi güvenliği politikasında belirtilmeyen veya belirtildiği halde yetersiz kaldığı durumlarda meydana gelen veri ihlalleri, Komisyon tarafından incelenir, gerekli revizyonlar yapılarak tedbirler alınır.

6.9 Diğer Hususlar

Madde 13-

1- Lojistik şirket bilgi güvenliği politikası oluşturulurken, bilgi varlıklarının korunabilmesini sağlayacak temel ilkeler belirlenmiştir. Bu politika, şirketin ve bağlı birimlerinin uygulamaları ile sunduğu hizmete uygun olarak geliştirecekleri prosedür ve politikaların ana ilkelerini belirlemektedir.

Şirket ve bağlı birimleri, verdikleri lojistik hizmet ve ihtiyaca uygun olarak, bu politika ilkeleri çerçevesinde ve politikaya aykırı düzenlemelere yer vermeden kendi prosedür ve hizmet politikalarını hazırlayabilirler. Depo süreçlerine uygulanacak prosedür ve politikalar, gümrük işleri prosedürleri, taşımacılık politikası, veri ihlalinde müdahale ve eylem planı, personel disiplin politikası gibi.

2- Bu model münferit bilgi güvenliği politikasında yer verilen düzenlemeler, lojistik işletmelerin kendilerine özgü koşulları ve sundukları hizmetleri dikkate alarak

oluşturacakları bilgi güvenliği politikaları için bir tavsiye ve kaynak niteliğindedir. Tavsiye niteliğindeki bu tedbirlerin uygulanmasından kaynaklı oluşabilecek olumsuz durumlardan, bu tedbirleri uygulayan kişi/şirket/kurumlar sorumludur. Bu bilgi güvenliği politikasının tümü veya bir kısmı, kaynak belirtilmesi koşuluyla, şirketler veya kurumlar tarafından kullanılabilir.

7. SONUÇ VE ÖNERİLER

Çalışmanın bu bölümünde, araştırma problemi ile amaçlar, çalışmalar ve elde edilen bulguların özetlendiği sonuçlar alt bölümüne yer verilmiştir. Ayrıca, çalışmada ulaşılan sonuçlar ve araştırmanın literatüre sağlayabileceği katkılar üzerine değerlendirmeler ile araştırılan konuda yapılabilecek diğer çalışmaları içeren araştırmacının değerlendirmelerinin yer aldığı öneri bölümü yer almaktadır.

Sonuç:

Bilim ve teknolojinin hızlı gelişimi, iş ve sosyal yaşamdaki işleri daha verimli ve rahat yapılabilir hale getirmiştir. Elektronik cihazların yaygın kullanımıyla bilgiye erişim kolaylaşmış, verilerin depolanması, paylaşılması ve taşınması pratikleşmiştir.

2020 yılında dünyaya yayılan virüs nedeniyle pandemi ilan edilmesiyle birlikte, kalabalıklardan uzak yaşam şekilleri ortaya çıkmıştır. Dünya genelinde sınırlar kapatılmış, üretim, ticaret, çalışma şekillerine kadar her alanda önemli değişiklikler yaşanmıştır. Bu değişimlerden etkilenen sektörlerden birisi de lojistiktir. Bu dönem, lojistiğin kritik rolünüde ortaya koymuştur. Pandemi ile yaşam şekillerinde ortaya çıkan değişimler, teknolojiyi, interneti daha da önemli hale getirmiştir. Lojistik sektörü açısından dijital platformlar üzerinden taşıma yönetiminin önemi artmıştır. Teknolojinin sunduğu imkanlar yaşamları kolaylaştırmakla birlikte, bilginin yetkisiz kişilerin eline geçme riski arttığından verilerin korunması daha da önemli hale gelmiştir.

Gizlilik, erişilebilirlik ve bütünlük güvenlik üçgeninin bozulmadan ve süreçlerin aksamadan devamı için, bilgi akışının sürekliliğini sağlamak önemlidir. Teknolojinin yoğun kullanımı ile birlikte oluşan güvenlik riskleri o kadar büyüktür ki, ülke güvenliği ve rekabet gücü bakımından devletler için kritik bir mesele haline gelmiştir. Li (2021), günümüzde siber tehditlerin coğrafi boyutunun ortadan kalktığı, hükümetlerle de sınırlı olmadığı, bireyler ve şirketlerin bu tehditlerin zararlarından muaf olmayacakları belirtilmiştir. Hükümetlerin tek başına bunlara karşı koyamayacağı, o sebeple hükümetler ile özel sektör arasında etkili ikili iş birliğinin gerekli olduğu ifade edilmiştir.

Siber risklerin yayılmasında tedarik zincirleri verimli ortamlardır. İhtiyaç duyulan en temel maddelerin (gıda, su, ilaç gibi) tedariki, ulaştırılması, depolanması lojistik faaliyetler ile mümkündür. Bu nedenle sektörün siber saldırı riski altında olması, hizmetlerin kesintiye uğrama riski bakımından önemli ve endişe vericidir. Lojistik hizmetler, taşımacılık ve depolama faaliyetlerinden ibaret değildir. Taşınan ve depolanan ürünlerin zincir içindeki operasyon ve hareketlerini idare etmek işin asıl temelidir. Bu da ancak bilginin kesintisiz temini ve kullanılabilmesi ile mümkündür. Operasyon süreçlerinde, bilgi akışının korunması, doğru bilginin zamanında temin edilmesi önemlidir. Hizmetlerin sürdürülebilirliği, süreçlerin devamı, kayıt edilen ve paylaşılan bilgilerin korunması ile sağlanır. Lojistik sektörü için ciddi risk oluşturan siber saldırılarla başa çıkmak üzere önlem alınmalıdır.

Tehlikenin boyutu o kadar büyük ve ciddidir ki ülkeler nezdinde eylem planları ve yasal düzenlemeler yapılmıştır. Ulusal Siber Güvenlik Stratejisi 2016-2019 eylem planlarında (2016), tüm kuruluşların güvenlik risklerini bilmeleri, önlem almaları, farkındalık ve yetkinliğin sağlanması için eğitimler verilmesi, teknik boyutlar yanında hukuki, idari, ekonomik ve sosyal boyutlara da önem verilmesi gerektiği belirtilmiştir. Diğer taraftan yasa gereği, tacirlerin ticari işlerinde öngörü sahibi ve tedbirli bir iş insanı gibi hareket etme yükümlülüğü bulunmaktadır. Bu nedenle, veri sorumlularının kayıtlı verileri korumakta özenli davranmaları ve yeterli tedbirleri almaları gerekmektedir. Benzer şekilde Kişisel Verilerin Korunması Kanunu ile veri sorumlularına, işledikleri kişisel verileri koruma yükümlülüğü getirilmiştir.

Ulusal eylem planları ve literatürde, Safa, Maple ve Watson (2017), bilgi güvenliğinin tüm yönlerine dikkat edilmesi gerektiği, kanun ve yaptırımlar yönlerine de önem verilmesi gerektiği belirtilerek, yasal düzenlemelerin önemine vurgu yapılmaktadır. Ancak buna karşın, konuyu yasal açıdan inceleyen bir çalışmaya rastlanılmamıştır. Tezin temel amacı bu eksikliği vurgulayarak, bilgi güvenliğini hukuki boyutu ile incelemek ve verilerin korunmasına yönelik yasal düzenlemeler kapsamında değerlendirmektir. Yasalar ile uyumlu koruma tedbirleri alınmadan, bilgi güvenliğinin yeterli düzeyde sağlandığından söz edilemeyecektir.

Bu kapsamda, kişisel veriler ve tüzel kişi verilerinin korunmasına ilişkin yasal düzenlemeler ile Yargıtay ve Kişisel Verileri Koruma Kurulu kararları incelenerek, bilgi güvenliği çerçevesinde değerlendirilmesi yapılmıştır. Lojistik işletmelere uygulanan anket sonuçlarından, yasal düzenlemeler ve bilgi güvenliğine ilişkin ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardlarından yararlanılarak, lojistik işletmeler için öneri olarak, bir model münferit bilgi güvenliği politikası oluşturulması tezin ikinci amacıdır.

Ülkelerin ekonomik durumu, gelişmişlik ve kalkınmışlık düzeylerini anlamamızı sağlayan göstergelerdendir. Ekonomik göstergelerin değişiminde belirleyici bir rol oynayan araçlardan birisi lojistik faaliyetlerdir. Kalkınma Bakanlığı, (2019-2023) On Birinci Kalkınma Planında (2018), ekonomik faaliyetlerin sürekliliği için üretim ve ticaret sistemlerinin mutlaka lojistik sistemlerle desteklenmesi gerektiği belirtilmiştir. Türkiye'nin lojistik gücü ile birlikte bulunduğu bölgenin potansiyeli de dikkate alındığında, ülkemizin sahip olduğu lojistik avantajların boyutu belirgin bir şekilde görülmektedir. Lojistiğin ülkemiz için önemi ve sahip olduğu avantajlar karşısında, sektörün gelişiminin desteklenmesi ve her türlü riske karşı da korunması gerektiği ortadadır.

Araştırma kapsamında elde edilen bulguların değerlendirilmesi sonucunda, lojistik şirketlerinin, yasal düzenleme ve ulusal eylem planlarına karşın, bilgi güvenliğini sağlamaya yönelik tam ve yeterli önlem aldığına dair bir sonuca varılamamaktadır. Dolayısıyla, risklere karşı yeterli korumanın sağlandığı söylenemeyecektir. Yargıtay ve Kişisel Verileri Koruma Kurulu kararları da, alınan tedbirlerin yeterli olmadığı yönündedir.

Kişisel Verilerin Korunması Kanunu md. 12'ye göre, "Veri sorumluları, verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemek, muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." Aynı madde uyarınca, "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, bu veri ihlalinin veri sorumluları tarafından kişisel verileri koruma kuruluna iletilmesi gereklidir."

Kurul tarafından verilen kararlar kapsamına bakıldığında; Firmaların verilerine izinsiz erişimde bulunulduğu halde, ihlal durumunun uzun bir süre fark edilmediği, sistemlerin

uyarı vermediği ve personelin durumu fark etmediği görülmektedir. Firmalar, sisteme izinsiz giriş yapan kişi/kişiler tarafından gönderilen e-postalar vasıtasıyla durumdan haberdar olmuşlardır. Veri ihlalinin boyutunun oldukça büyük olduğu, birçok sunucuyu etkileyen saldırılar olduğu görülmektedir. Saldırıların boyutu, kimi zaman grup şirketleri ve değişik ülkelerde operasyonları bulunan fiziksel ve çevrimiçi mağazaları da kapsayacak büyüklükte yaşanmaktadır.

İncelenen bir kararda, bir kargo firmasının, çapraz barkodlama işlemi ile veri ihlaline yol açtığı olayda, yasal bir zorunluluk bulunmasına rağmen, ihlali kurula bildirilmediği ve yasaya aykırı davranıldığı tespit edilmiştir. Başka bir kararda, Gıda lojistiği alanında faaliyet gösteren bir firma, web uygulama sunucusundaki güvenlik açığı nedeniyle veri ihlaline sebep olmuş ve bu durumdan çok sayıda kullanıcı zarar görmüştür. İşletmelerin sistemlerine giren zararlı yazılımları tespit edememesi, firmalar açısından ciddi bir güvenlik sorunu oluşturmaktadır.

İncelenen kararlarda, veri sorumlusu konumundaki lojistik işletmelerinin, hizmet sağlayıcı üçüncü kişi firmalar üzerinde etkili bir kontrol mekanizması kuramadığı ve ayrıca güvenlik yazılımlarının izlenmesi ve güvenlik prosedürlerinin uygulanması konusunda eksikliklerinin bulunduğu belirlenmiştir.

Avrupa Birliği Siber Güvenlik Ajansı (ENISA) raporunda (2020), siber güvenlikte saldırı yüzeyinin genişlediği belirtilerek, siber güvenlik alanında yaşanan zorluklar arasında; Tedarik zinciri ve üçüncü taraflardan gelen saldırılar sayılmıştır. Kurumların kendi altyapı güvenliğini en üst düzeyde sağlıyor olsalar da, iş birliği yaptıkları tedarikçiler ya da üçüncü tarafların bilgi güvenliği uygulamalarının var olup olmadığının bilinmediği, çoğu zamanda olmadığı ifade edilmiştir.

İncelenen kararlarda, veri ihlallerinin sunucularda depolanan tüm kişisel verileri etkilediği görülmüştür. İhlalden etkilenen ilgili kişiler, veri sorumlularının yürüttüğü faaliyet çerçevesinde bilgileri sisteme kaydedilmiş olan personel, müşteriler/potansiyel müşteriler ve kullanıcılar olmak üzere tüm kişilerdir. İhlalin etkisi ile oluşan zarar da oldukça fazladır.

Genellikle verilerin dijital sistemlerde depolanması nedeniyle, veri güvenliği bakımından alınacak önlemlerin ilk sırasında teknik tedbirler gelmektedir. Ancak Kurul kararlarının incelenmesi sonucunda, firmaların bilgi güvenliği için rutin olarak yapılması gereken teknik testleri (sızma testleri) dahi gerçekleştirmedikleri ve ihlal sonrası yapılan testlerde ise, yüksek risk seviyeli zaafiyetler tespit edildiği belirlenmiştir. Diğer taraftan, firmaların, hizmet aldığı dış kaynak firması ile ticari ilişkilerini sonlandırmış olmalarına rağmen, veri imha prosedürlerini uygulanmadıkları, bu eksikliğin ise güvenlik açıklarına ve ihlale yol açtığı belirlenmiştir. Kararlarda, verilere izinsiz erişimin, her ölçekten firma için önemli bir tehdit oluşturduğu görülmektedir.

Verilere izinsiz erişim, kullanma, değiştirme, paylaşma gibi konularda Yargıtay Ceza ve Yargıtay Hukuk Daireleri tarafından verilmiş olan örnek kararlara, hukuk içtihatları sunan Lexpera, Legalbank, Yargıtay kararları, HukukTürk gibi hukuk siteleri taranarak ulaşılmıştır.

İncelenen yargı kararları kapsamında, firmaların bilgi güvenliği konusunda yeterli tedbir aldığını söylemek mümkün değildir. Bir kararda, şirket personeli olmayan şahısların, firmanın üretim sahasına girmesine izin verildiği belirtilmiştir. Üretim alanları, firmalar için ticari sır niteliğindeki bilgilerin (örneğin üretim formülleri, üretim teknikleri gibi) korunduğu ve sadece yetkilendirilmiş kişilerin erişim sağlayabildiği özel alanlardır. Bu bölgelere üst yönetimin izni olmadan girişin mümkün olması, firma açısından bir güvenlik açığı olarak değerlendirilebilir. İşletmenin gerekli önlemleri almadığı ve aynı zamanda denetimleri de gerçekleştirmediği söylenebilecektir.

Araştırma kapsamında lojistik işletmelere uygulanan anket sonuçları da yargı kararları ile benzerlik göstermektedir. Lojistik işletmelerinin, verilerin korunduğu fiziksel ve dijital alanlara erişim için gereken yetkilendirme ve denetim faaliyetlerini gerçekleştirmediği belirlenmiştir. Yargı kararları ile firma uygulamaları birbirini destekler niteliktedir. Yetkilendirme işlemi, mahkeme incelemesinde kritik bir rol oynamaktadır. Ticari sır niteliğindeki bilgileri açıklama suçunun işlendiği iddiası ile açılan davada, mahkeme, sanığın ilgili şirkette suç tarihindeki görevi ile, söz konusu belgelere erişim yetkisinin bulunup bulunmadığını araştırmıştır.

Yargı kararları veri ihlallerinin genel olarak firma içinden kaynaklı olduğunu göstermektedir. Özellikle işten çıkarılan personelin şirket ile tüm ilişkisinin kesilmesi, bilgisayar girişlerinin iptal edilmesi, yetkilerine son verilerek uhdesinde bulunan tüm bilgi ve belgelerin tesliminin sağlanması son derece önemlidir. Yargı kararları, firmaların bu önlemleri alamadığını, idari ve hukuki tedbirleri sağlamakta yetersiz kaldıklarını ortaya koymaktadır. Kişisel Verileri Koruma Kurulu kararları ile anket bulguları da benzer şekildedir.

Veri envanteri çıkarılması, risk ve önemine göre tasnif edilmesinin önemi yargı kararları ile de belirginleşmiştir. Mahkemeler özellikle ticari sır ihlaliyle ilgili ihtilaflarda, belgenin ticari sır niteliğine sahip olup olmadığını belirlemek üzere dosyayı bilirkişi incelemesine göndermektedir. İnceleme süreci, şirketin veri envanteri, verilerin sınıflandırılması ve derecelendirilmesi dikkate alınarak yapılacağından, firmanın bu işlemleri öncesinde tamamlamış olması davanın ispatı açısından büyük bir önem taşımaktadır. Yüksel (2018), çoğu zaman davalarda, ticari sır olduğu iddia edilen bilgilerin bu vasıfta olduğu ispatlanamadığından davalar red edilmektedir. Çünkü bu davalarda, mahkemece bilirkişi incelemesi yaptırılarak ticari sır olduğu ileri sürülen bilginin bu nitelikte olup olmadığı araştırılmaktadır.

Bilgi güvenliği teknik, idari, hukuki önlemlerin bir bütün olarak alınması ile sağlanabilir. Veriler genel olarak dijital sistemlerde muhafaza edildiğinden, öncelikli olarak teknik önlemlerin alınması gerekliliği ortaya çıkmaktadır. Ancak yargı kararları, firmaların, teknik önlemlerin alınmasında da yetersiz kaldıklarını göstermektedir.

Araştırma kapsamında, Adli suçlarla ilgili olarak Adalet Bakanlığı nezdinde kurulmuş olan Adli Sicil ve İstatistik Genel Müdürlüğü'nün, Bilişim alanındaki suçlar (TCK m.243-246) ve kişisel verilerin hukuka aykırı şekilde ele geçirilmesi, kaydedilmesi suçlarının da içinde bulunduğu, Özel hayata ve hayatın gizli alanına karşı suçlar (TCK m.132-140) ve Ekonomi, sanayi ve ticarete ilişkin suçlar (TCK m.239) bakımından savcılık ve dava aşamasında verilmiş olan karar istatistikleri incelenmiştir.

İstatistik sonuçlarından elde edilen bulgulara göre, bilişim alanındaki suçlar ve özel hayata ve hayatın gizli alanına karşı suçlar bakımından savcılığa başvurularda artış

yaşandığı görülmüştür. Aynı şekilde bu suçlar bakımından açılan davalar sonucunda verilmiş olan mahkumiyet kararlarında da artışlar olmuştur.

Ekonomi, sanayi ve ticarete ilişkin suçlar kapsamında bulunan ticari sırrın ifşasına ilişkin suç bakımından ise, kamu davası açılma oranlarının yıllar içinde artış gösterdiği diğer taraftan, verilen mahkumiyet karar sayılarının ise azaldığı belirlenmiştir. Bu durum, suçun ispatlanamamasından ya da mahkeme tarafından başkaca kararlar (görevsizlik gibi) verilmiş olmasından ileri gelebilir. Ticari sır olduğu iddia edilen bilgi ya da belgenin bu kapsamda olduğu ispatlanamamış olabilir.

Çalışma kapsamında, Türkiye genelinde faaliyette bulunan lojistik işletmelerine anket uygulanmıştır. Anket bulguları değerlendirildiğinde, ülkemizde lojistik sektöründe çeşitli ölçeklerde firmanın faaliyet gösterdiği ve küçük ve orta ölçekli işletmelerin sayıca fazla olduğu belirlenmiştir. Akademik çalışmalar, bu firmaların siber saldırılara karşı daha savunmasız ve risklerinin daha yüksek olduğunu ortaya koymaktadır. Veri İhlali Soruşturma Raporu Verizon (2022), küçük ve orta boyuttaki işletmeler, maliyet veya insan gücünün yeterli olmaması gibi sebeplerle bilgi güvenliğine önem vermemektedir. Bundan dolayı da güvenliğini yeterli seviyede sağlamış olan büyük firmalara kıyasla saldırılara daha açık vaziyettedirler.

Bu itibarla, sektörde veri güvenliğini sağlamamış olan firmaların risk altında olduğu söylenebilecektir. Ancak tedarik zinciri içerisinde çok sayıda lojistik faaliyet bulunduğundan risk, sadece bu işletmeler bakımından değil, aynı zamanda bunlarla bilgi paylaşımında bulunan diğer işletmeler/kişiler için de söz konusudur.

Türkiye Siber Risk Algı Araştırma Raporu (2020), günümüzde birlikte çalışan şirketlerin birbirine güven duymasının, zincirin etkin şekilde çalışması için gerekli olduğunu belirtmektedir. Şirketlerden, halkası oldukları değer zincirindeki rollerinin ve siber güvenlik konusundaki sorumluluklarının farkında olmaları beklenmektedir. Şirketler arasında üçüncü taraflardan kaynaklı siber riskler konusunda kendilerini tamamen güvende hissedenlerin oranı oldukça düşüktür. Yüksel (2018) göre, ticari sırların yetkisiz kişilerce ele geçirilmesinde yalnızca bilgisayarlar değil, akıllı araçlar, akıllı tıbbi cihazlar gibi bilgi işleme özelliğine sahip cihazlar da saldırıya uğrayabilmektedir. Firmaların bilgi

güvenlik tedbirleri, veri işlenen, depolanan tüm ortamları korumayı sağlayacak, risk seviyesini düşürecektir.

Anket bulguları, şirketlerin veri envanteri çıkarılmasında iyi bir durumda olduklarını ortaya koymaktadır. Ancak, verilerin risk ve önemine göre gruplandırılması ile risklerin gerçekleşmesi halinde ortaya çıkabilecek zararlar konusunda yeterli çalışmanın yapılmadığı görülmektedir. Yargı kararları, özellikle ticari sırların ihlali ile ilgili davalarda, veri envanterinin çıkarılması, risk ve önemine göre gruplandırılması ve derecelendirilmesi gibi çalışmaların, davanın ispatı açısından çok önemli olduğunu göstermektedir.

Yargı kararları, veri ihlallerinin genel olarak şirket içinden kaynaklı olduğunu gösterirken, anket bulguları da benzer bir sonuç sunmaktadır. Diğer yandan anket sonuçları, çok az sayıda firmanın çalışanlarına bilgi güvenliği konusunda eğitim verdiğini göstermektedir. Personel kaynaklı ihlaller, kasıtlı eylemler ile gerçekleşebildiği gibi çoğu zaman bilgi eksikliğinden kaynaklanmaktadır. Bu durumda, firmaların ihlal sebeplerinin farkında olmalarına karşın, çözüm bulmak üzere yeterli eğitim imkanı sağlamamış olmaları, idari ve hukuki eksiklik olarak değerlendirilebilecektir.

Anket bulguları, lojistik işletmelerinin, iş akdi feshedilen ya da görevi değiştirilen personelin, verilere erişim yetkilerinin zamanında sonlandırılması için yeterli özeni göstermediklerini ortaya koymaktadır. Kişisel Verileri Koruma Kurulu ve Yargıtay'ın, yetkinin zamanında sonlandırılmamasının sonuçlarına ilişkin veri ihlal kararları bulunmaktadır.

Günümüzde veriler genel olarak dijital ortamlarda depolanmaktadır. Anket bulguları da bu yöndedir. Bazen de yasalar gereği fiziki ortamlarda saklanması gereken veriler ile firma ticari sırlarının elektronik olmayan ortamlarda saklanması gereklidir. Bu durumda fiziki ortam güvenliğinin sağlanmış olması önemli olacaktır. Anket sonuçları, fiziki ortam güvenliği ve yetkilendirme işlemlerinin yeterince yapılmadığını göstermektedir. Yargıtay 9HD.(2016) kararı, üretim sahasında şirket personeli olmayan şahısların bulunduğu, bu alanda olmaları sebebi ile şirketin gizli bilgi ve ticari sırlarını öğrendiklerine ilişkin kararı, yetkilendirme prosedürlerinin yerine getirilmemesinin şirket için hangi risk ve zararlara yol açtığını göstermesi bakımından önemlidir. Türk Ticaret Kanunu gereği, "Her tacir,

ticari faaliyetlerinde basiretli bir iş adamı gibi davranmak zorundadır.” Kayıt altına aldığı verileri koruma görev ve sorumluluğu bulunan şirket yönetiminin, verilerin korunmasında özenli davranması ve her türlü koruyucu tedbiri alması kanun gereğidir.

Bilgilerin korunması, saklanması, işlenmesi ve imhasına ilişkin politikaların oluşturulması konusunda anket sonuçları genel itibarı ile olumsuzdur. Bazı yargı kararlarında, politikalarla ilgili düzenlemelere yer verildiği görülmektedir. Bilgi güvenliği politikaları, şirket iş süreçlerini düzenlerken, kurumsallaşmaya da katkı sağlayacaktır.

Anket bulguları, şirketin mali durumu ile bilgi güvenliğine ayrılan bütçe arasında önemli bir ilişki olduğunu belirlemiştir. Ancak dijitalleşmenin getirdiği bilgi güvenliği risklerine karşı önlem alınması gerekli olduğu gibi yasal olarak da bir zorunluluktur. ISO 27001:2022 BGYS (madde 5.1), bilgi güvenliğinin sağlanması konusunda şirket üst yönetimine sorumluluklar yüklemiştir. Şirket üst yönetimi, bilgi güvenliği yönetim sistemi için gereksinim duyulan kaynakların mevcut olmasını sağlamakla yükümlüdür. Bu nedenle, firmaların veri envanterlerini çıkararak risk ve önemine göre sınıflandırması, önceliklerini belirlemesi ve riskin gerçekleşmesi durumunda oluşacak zararlara yönelik araştırma yapması önemlidir. Yapılacak çalışma, şirket bütçesi belirlenirken bilgi güvenliğine ayrılacak pay konusunda da firmaya yol gösterici olacaktır. Şirket büyüklüğü, işlenenen verilerin türü ile risk seviyesi, ayrılacak bütçe de etkili olmaktadır. Arroyabe (2023), siber güvenlik yatırımı kuruluşlarda stratejik bir karardır. Şirket ölçüleri siber güvenlik yatırımında önemli bir değişkendir.

Anket bulguları genel itibari ile, şirketlerin ISO 27001 bilgi güvenliği yönetim sistemi sertifikasına sahip olmadığını göstermektedir. Bu sonucun bütçe ile ilgisi olduğu gibi, başka sebepleri de olabilir. Literatürde, Mirtsch, Kinne ve Blind (2021), firmaların yalnızca kendilerinin bilgi güvenliği sertifikası aramadığını, aynı zamanda web sitelerinde bilgi güvenliği sertifikası olan ortaklara başvurduğu belirtilmektedir. Yapılan araştırmalar, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin, Genel Veri Koruma Tüzüğü (GDPR) veya ulusal siber güvenlik yasaları ile ilgili düzenlemelere uyumu kolaylaştırdığı etkili olduğu, ifade edilmiştir. Benzer şekilde ISO 27001 standardı KVKK’ya uyum sağlanmasında da kolaylaştırıcıdır.

Firmalarda bilgi güvenliğinin sağlanması için çalışacak ve sorumlu olan bir kurul/komisyon/birim kurulması önemlidir. Anket bulguları, firmaların genel olarak böyle bir kurul/komisyon/birime sahip olmadığını göstermektedir. Hipotez sonuçlarına göre, bilgi güvenliğinden sorumlu komisyonun varlığı, verilere ilişkin prosedür ve politikaların oluşturulmasında etkili olmaktadır. Kurulacak komisyonun, teknik, idari, hukuk, insan kaynakları ve üst yönetim temsilcilerinden oluşması faydalı olacaktır. Türkiye Siber Risk Algı Araştırması Raporunda (2020), her şirkette siber risklerin gelişimi ve stratejilerine yönelik çalışacak ayrı bir Siber Güvenlik Komitesi kurulmasını, komitenin insan kaynakları, operasyon, hukuk ve diğer iş birimlerinden yetkilileri barındırması belirtilmektedir.

Araştırma kapsamında elde edilen anket sonuçları, veri sorumlusu lojistik işletmelerinin, bilgi güvenliğini sağlamak için gerekli hukuki ve idari tedbirler bakımından eksikliklerinin olduğunu ortaya koymaktadır. Firmaların, bilgi güvenliğini tam ve etkili şekilde sağlayamadıklarını söylemek mümkündür. Bu durumda, firmalar risklere açık bir konumda bulunmaktadır.

Araştırma kapsamında elde edilen anket bulguları ile literatür, yargı kararları ve kurul kararları arasında bir uyum olduğu gözlemlenmektedir. Literatürde belirtilen hususlar, anket sonucu elde edilen lojistik işletme uygulamaları ile genel olarak ortaya konulmuştur. Firmaların bilgi güvenliği uygulama sonuçları, yargı ve kurul kararlarında da benzer şekilde görülmektedir. Çalışma kapsamında yer alan hipotezler de, elde edilen bulguları destekler niteliktedir. Tüm bu hususlar birlikte değerlendirildiğinde, mevcut durum ve gelecekte siber saldırı tehditi ile karşı karşıya olan lojistik sektöründe, bilgi güvenliğinin tam ve yeterli düzeyde sağlanabilmesi için çalışmalar yapılması son derece önemlidir. Firma düzeyinde gerçekleştirilecek bilgi güvenliği çalışmalarının, tüm tedarik zincirini de etkileyeceği göz ardı edilmemelidir. Lojistik, tedarik zinciri sürecinin bir bileşenidir. Lojistik işletmeleri, tedarik zinciri içerisinde bilgi, ürün ve hizmet akışını yöneterek tedarikçi ve müşteri arasında bağlantı sağlar. Üstlendikleri görev ağır ve oldukça önemlidir. Şirket verilerini elde etmeye yönelik saldırılar, dışarıdan veya şirket içinden yapılmış olsun, her yönüyle yeterli koruma tedbiri alınmaz ise, bilgi güvenliğinin tam ve yeterince sağlanmış olduğundan bahsedilemeyecektir.

Tezin üçüncü amacı, araştırma kapsamında, Ulaştırma ve Altyapı Bakanlığı'nca hazırlanan 2020 tarihli, Türkiye Ulaştırma Politika Belgesinin "Veri (Bilgi)" başlıklı bölümünde yer alan siber güvenliğin sağlanmasına yönelik düzenlemelerin Lojistik Sektörü için uygun ve yeterli olup olmadığı hususunun değerlendirilmesidir.

Belgede siber güvenlik konularına yer verilerek:

"Ulusal siber güvenliğimizin sağlanması için ulusal stratejiler geliştirileceği ve güncelleneceği; Ulusal stratejiler temel alınarak siber güvenliğin sağlanması için eylem planları oluşturulacağı; Kritik altyapıların kullanıldığı haberleşme,ulaştırma gibi alanlarda bilişim sistemlerinin güvenliğini sağlamak için risk analizleri, sektörel düzenlemeler yapılmasının gerekli olduğu; Ulaştırma verilerine KVKK'ya uygun ve güvenilir şekilde erişime sahip olunması, paylaşımı için veri yönetişimi mekanizmaları geliştirileceği; Ülkemizde üretilen ulaştırma ve haberleşme verilerinin,uluslararası arenada kabul görmüş güvenlik standartları ve gereksinimlerini karşılayacak şekilde üretimi, iletimi, saklanması, ve paylaşımının yapılacağı; Siber Güvenliğe ilişkin ulusal mevzuatın geliştirilmesinde uluslararası düzenlemeler ve standartların dikkate alınacağı; Ulusal siber güvenliğin sağlanması amacıyla kamu kurum ve kuruluşları, sivil toplum kuruluşları, yerel yönetimler, üniversiteler ve özel sektörün iş birliği içinde çalışacağı; Siber güvenliğin sağlanması konusunda bireylerin, kurum ve kuruluşların ve tüm paydaşların üzerine düşen sorumlulukları anlayarak bu sorumlulukları yerine getirecek şekilde hareket etmeleri gerektiği; Siber güvenlik alanında uzman insan kaynağının geliştirilmesine yönelik faaliyetlerin sürdürüleceği; Bilgi teknolojileri ile ilgili sağlanan her türlü hizmet, işlemde ve sunumunda kullanılan sistemlerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanmasına yönelik çalışmalar yürütüleceği; Siber güvenliğin sağlanması ve riskler ile mücadele için farkındalığın artırılarak konuya ilişkin eğitimler düzenlenerek bu eğitimlerin teknik bilgiler ile birlikte olayı bir bütün olarak görülmesini sağlayan hukuki, idari, ekonomik, politik ve sosyal kısımları da içerek şekilde oluşturulmasının sağlanacağı" ifade edilmiştir.

Bu politikaların ele alındığı 12. Ulaştırma ve Haberleşme Şurası, 6-7-8 Ekim 2021 tarihinde İstanbul'da yapılmıştır. Şura Sonuç Bildirgesi (2021) Aralık 2021'de yayınlanmıştır. Bildirgede, sektörler bazında yürütülen çalışmaların "Lojistik, Mobilite

ve Dijitalleşme" temaları altında ve Türkiye Ulaştırma Politika Belgesi doğrultusunda sentezlendiği ifade edilmiştir.

"Sonuç Bildirisi özetle;

- Siber güvenliğe ilişkin ulusal mevzuatın geliştirilmesinde uluslararası düzenlemeler ve standartların dikkate alınması,
- Siber güvenliğin sağlanması konusunda bireylerin, kurumların, kuruluşların ve tüm paydaşların üzerine düşen sorumlulukları anlayarak bu sorumlulukları yerine getirecek şekilde hareket etmelerinin sağlanması,
- Bilgi teknolojileri ile ilgili verilen tüm hizmetler, bilgiler ve işlemler ile bunların işlenmesi, depolanması ve sunumunda kullanılan sistemlerin; gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanmasına yönelik çalışmalar yürütülmesi, gerekli önlemlerin alınması,
- İnsan, yük ve veri hareketliliğinin etkin yönetilebilmesini sağlayacak araştırma ve geliştirme çalışmalarını teşvik etmek amacıyla kamu, özel sektör ve üniversite iş birliğinin gelişiminin desteklenmesi,
- Veri merkezi sektöründe nitelikli insan kaynağının artırılmasına yönelik politikalar uygulanması,
- Ulusal siber güvenliğin sağlanması doğrultusunda yerel yönetimler, üniversiteler, kamu kurum ve kuruluşları, özel sektör ve sivil toplum kuruluşlarıyla iş birliği içinde çalışılması,
- Ulaştırma ve Haberleşme Şûrası'nın çatısını oluşturan "Lojistik, Mobilite ve Dijitalleşme" yaklaşımlarımız, Türkiye Ulaştırma Politika Belgesi'nde yer alan ve 'Temel Politika Alanları' diye adlandırılan başlıklar çerçevesinde tam 50 yıl sonrasını düşünerek vizyoner adımlara dönüştürülmüş, "ve konulan hedeflerle somutlaştırılmıştır" şeklindedir.

Sonuç bildirgesine göre: Konuya ilişkin olarak sektörler bazında yapılmış olan çalışmalar, "Lojistik, Mobilite ve Dijitalleşme" temaları altında ve Türkiye Ulaştırma Politika Belgesi doğrultusunda sentezlenerek farklı hedefler oluşturulmuştur. Ana başlıklardan anlaşılacağı üzere,

- Siber güvenlik mevzuat çalışmalarında, uluslararası standardlardan faydalanılacaktır.

- Bilgi güvenliği konusunda sektörlerin üzerine düşen güvenlik önlemlerini alması gerekmektedir.
- Bilginin gizlilik, bütünlük, erişilebilirlik ögelerinin sağlanmasına yönelik çalışmalar yapılması gerekmektedir.
- Siber güvenliğin sağlanması konusunda özel sektör, üniversiteler iş birliği içinde çalışacaktır.
- Veri konusunda nitelikli insan kaynağının arttırılması önemlidir.

Sonuç bildirgesi ana başlıklarına göre, Türkiye Ulaştırma Politika Belgesi güncelliğini korumakta olup, çalışmalar bu belge doğrultusunda ve geliştirilerek devam etmektedir. Politika belgesi ve bildirgede bahsedilen siber güvenliğin sağlanması için konulan hedeflerin gerçekleştirilebilmesi için yapılacak çalışmaların lojistik sektörüne uygun olup fayda sağlayacağı değerlendirilmektedir.

Ulaştırma ve Altyapı Bakanlığı'nın 2053 Ulaştırma ve Lojistik Ana Planı'nda (2022), Şura bildirisinde belirtilen birçok nokta tekrar edilmiştir. ''İnsan, yük ve veri hareketliliğinin etkin yönetilebilmesini sağlayacak araştırma ve geliştirme çalışmalarını teşvik etmek amacıyla kamu-özel sektör ve üniversite iş birliğinin gelişimi desteklenmelidir. Ulusal siber güvenliğin sağlanması amacıyla üniversiteler, yerel yönetimler, kamu kurum ve kuruluşları, özel sektör ve sivil toplum kuruluşları iş birliği içinde çalışmalıdır. Ulusal siber güvenliğin, ulaştırma ve haberleşme sistemlerinin güvenliğinin sağlanmasına. Siber güvenliğin sağlanması konusunda bireylerin kurumların, kuruluşların ve tüm paydaşların üzerine düşen sorumlulukları anlayarak bu sorumlulukları yerine getirecek şekilde hareket etmeleri beklenmektedir. Siber güvenliğe ilişkin ulusal mevzuatın geliştirilmesinde uluslararası düzenlemeler ve standartlar dikkate alınmalıdır. Bilgi teknolojileri ile ilgili verilen tüm hizmetler, bilgiler ve işlemler ile bunların işlenmesi, depolanması ve sunumunda kullanılan sistemlerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanmasına yönelik çalışmalar yürütülmeli, gerekli önlemlerin alınması gerektiği'' belirtilmiştir.

Öneriler

Teknolojinin gelişmesi ile birlikte iş süreçlerinin hızlanmış olması, müşteri memnuniyetini de arttırmıştır. Süreçlerin aksamadan sürdürülebilmesi, müşteri

taleplerine zamanında cevap verilebilmesi için, mal, bilgi ve nakit akışının da sürekli olarak devam etmesi gerekmektedir.

Ülkelerin ekonomik faaliyetlerinin sürdürülebilmesi için etkin lojistik sistemlerle desteklenmesi gerekir. Ülkemiz coğrafi konumu itibariyle, büyük bir lojistik avantaja sahiptir. Ayrıca lojistiğin önemi 2020 yılında yaşanan pandemi ile bir kez daha anlaşılmıştır. Lojistik sektörünün ülkemiz için önemi, sahip olduğu lojistik avantajlar karşısında, gelişiminin desteklenmesi ve risklere karşı da korunması gerekmektedir.

Günümüzde, izinsiz erişim, izinsiz kullanım ve verinin değiştirilmesi gibi bilgiye yönelik saldırılar daha kolay gerçekleştirilir hale gelmiştir. Siber saldırı ve izinsiz fiziksel erişim risklerine karşı korunmada en büyük zorluklardan biri, veri güvenliğinin yeterince sağlanmamış olmasıdır. Lojistik işletmelerinin bilgi güvenliği ve riskleri konusunda bilinçlendirilmeleri ve desteklenmeleri, iş birliği yapmaya istekli olmaları için önemlidir. Bu amaçla, zaman ve bütçe ayırarak çaba göstermeleri için teşvik edilmelidirler. Şirket üst yönetiminin bilgi güvenliği konusunda bilinçlendirilmesi ve şirkete sağlayacağı faydaların aktarılması amacıyla, seminer ve toplantılar düzenlenmesi mümkündür.

Araştırma bulguları, veri ihlal sebepleri arasında personel davranışlarının önemli olduğunu göstermektedir. Bu nedenle çalışanlara, bilgi güvenliğinin sağlanmasında hak ve sorumlulukları ile ilgili eğitim verilmesi ve farkındalık yaratılması önemlidir. Bilgi güvenliği, geniş kapsamlı ve çok yönlü bir alan olduğundan, her yönüyle ele alındığı eğitimlerle bilinçlendirme ve farkındalık yaratılması sağlanabilecektir.

Lojistik işletmeler açısından, personel ile yapılacak sözleşmelerde, bilgi güvenliği, gizlilik ve sır saklamaya ilişkin düzenlemelere ve bunların ihlal edilmesi halinde sonuçlarına ilişkin düzenlemelere yer verilebilir.

Siber risk, her ölçekten firma için söz konusudur. Tedarik zinciri içerisinde birçok lojistik işlem bulunduğundan, zincirde yer alan tüm firmaların bilgi güvenliği önlemini alması gerekir. Araştırma sonuçları, küçük ve orta ölçekli lojistik işletmelerin sayısının fazla olduğunu ortaya koymuştur ve bu ölçekteki firmaların siber risklere maruz kalma olasılığı daha yüksektir. Bu ölçekteki firmalar için, çalışma kapsamında elde edilen bulgular temel alınarak, farklı araştırmalar yapılabilir.

Araştırma bulguları, şirketlerin mali durumu ile bilgi güvenliği için bütçe ayırmaları arasında önemli bir ilişki olduğunu göstermiştir. Diğer taraftan, artan riskler ve mevzuat gereğince veri güvenliğinin sağlanması zorunluluğu bulunmaktadır.

Çalışma kapsamında, yasal düzenlemeler detaylı olarak incelenmiş ve konu hukuki boyutu ile ele alınmıştır. Ayrıca bilgi güvenliğinin sağlanması için yapılması gerekenler konusunda bilgilere de yer verilmiştir. Bilgi güvenliği için çalışma yapacak ve bunun için bütçe ayıracak lojistik işletmelerinin, öncelikle veri envanterlerini oluşturması ve ardından verileri risk ve önem derecelerine göre sınıflandırması gerekmektedir. Bu çalışma, şirket bütçesinin belirlenmesi sürecinde, bilgi güvenliğine ayrılacak payın belirlenmesinde firmalara rehberlik edecektir. Firma, veri türleri ile riskleri belirleyeceği için, tedbirlerini de bu bilgilere göre alacaktır. Şirketin büyüklüğü, işlenen veri türü ve risk seviyesi, ayrılacak bütçeyi belirlemede bir kriter olacaktır. Bu çabalara rağmen, bütçe ayırmakta zorlanan küçük ve orta ölçekli işletmeler bakımından, ticaret ve sanayi odaları, çeşitli meslek kuruluşları, organize sanayi bölgeleri gibi kuruluşların sağlayacağı destek imkanları değerlendirilebilecektir.

Çalışmanın araştırma kapsamı, Türkiye'de faaliyet gösteren TIO belgeli lojistik işletmeleridir. Farklı ülkelerdeki şirketler kapsamda değildir. Gelecek çalışmalarda, farklı ülkelerde araştırma tekrar edilip sonuçlar karşılaştırılabilir.

Araştırma verilerinde değişiklik yapılmak suretiyle ve çalışma kapsamı dışında olan veri üzerinde hak sahibi diğer unsurlar dahil edilerek yeni araştırmalar yapılması mümkündür.

Bilgi güvenliği ile ilgili olarak ceza ve hukuk olmak üzere ihtisas mahkemeleri kurulması hususu değerlendirilebilir.

Bulgular, günümüzde ve gelecekte siber saldırı tehdidinin artarak devam edeceğini ortaya koymaktadır. Yapılan çalışmanın, farklı sektörler için yapılacak araştırmalarda yol göstereci olacağı düşünülmektedir.

Bu çalışmanın mevcut literatüre yaptığı katkı, bilgi güvenliğini hukuki açıdan inceleyen bir çalışmanın eksikliğini vurgulamaktır. Dolayısıyla, lojistik sektöründe bilgi güvenliği ile ilgili araştırmalarda, konunun hukuki boyutu ile ele alındığı bir çalışmaya rastlanılmadığından, bu çalışmada, bilgi güvenliğini hukuki açıdan inceleyen bir

araştırma yapılarak, literatürdeki bu boşluğun doldurulması ve gelecekte yapılacak araştırmalar için örnek teşkil etmesi amaçlanmıştır.

Tez çalışmasının, bilgi güvenliğinin hukuki yönünün anlaşılması, önemi ve dikkate alınması açısından literatüre fayda sağlayacağı düşünülmektedir. Bilgi güvenliği alanında hukuki farkındalık ve yeterlilik oluşturulması bakımından araştırmanın önemli olduğu değerlendirilmektedir.

KAYNAKÇA

Adıgüzel B. (2005). Bilişim Sistemlerinin Lojistik Yönetiminde Etkin Kullanımı ve Buna İlişkin Bir Uygulama. (Yayın No: 215588), [İstanbul Üniversitesi, Yüksek Lisans Tezi].https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Adli Sicil ve İstatistik Genel Müdürlüğü, (2023). Bilişim Alanındaki Suçlar Savcılık Kararları, Adalet İstatistikleri Dökümanı. 2017-2023, 51,58,69,72, Erişim Tarihi: 18 Nisan 2024 tarihinde https://adlisicil.adalet.gov.tr/Home/SayfaDetay/adalet-istatistikleri-yayin-arsivi adresinden alındı.

Adli Sicil ve İstatistik Genel Müdürlüğü, (2023). Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar Savcılık Kararları, Adalet İstatistikleri Dökümanı, 017-2023, 51,54,69,72, Erişim Tarihi: 18 Nisan 2024 tarihinde https://adlisicil.adalet.gov.tr/Home/SayfaDetay/adalet-istatistikleri-yayin-arsivi adresinden alındı.

Adli Sicil ve İstatistik Genel Müdürlüğü, (2021). Ekonomi, Sanayi ve Ticarete İlişkin Suçlar (Ticari Sır) Savcılık Kararları, Adalet İstatistikleri Dökümanı, 2017-2021, 58, Erişim Tarihi: 18 Nisan 2024 tarihinde https://adlisicil.adalet.gov.tr/Home/SayfaDetay/adalet-istatistikleri-yayin-arsivi adresinden alındı.

Adli Sicil ve İstatistik Genel Müdürlüğü, (2021), Bilişim Alanındaki Suçlar Mahkeme Kararları, Adli İstatistik Dökümanı, 2017-2021, 40, 43,44, Erişim Tarihi: 18 Nisan 2024 tarihinde https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/31052022141642 2021HİZMETE ÖZELKİTAP.pdf sitesinden erişildi.

Adli Sicil ve İstatistik Genel Müdürlüğü, (2021), Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar Mahkeme Kararları, Adli İstatistik Dökümanı, 2017-2021, s.40,43,44, Erişim Tarihi: 18 Nisan 2024 tarihinde

https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/31052022141642021HİZMETEÖZELKİTAP.pdf adresinden alındı.

Adli Sicil ve İstatistik Genel Müdürlüğü, (2021), Ekonomi, Sanayi ve Ticarete İlişkin Suçlar Mahkeme Kararları, Adalet İstatistikleri Dökümanı, 2017-2021, 110,164, 182, Erişim Tarihi: 18 Nisan 2024 tarihinde https://adlisicil.adalet.gov.tr/Home/SayfaDetay/adalet-istatistikleri-yayin-arsivi adresinden alındı.

A1 Certification ve Inspection, (t.y.). ISO 27701:2019 KVYS Kişisel Veri Yönetim Sistemi. Erişim Tarihi: 11 Nisan 2023 tarihinde https://www.a1cert.com/hizmetler/iso-277012019-kvys-kisisel-veri-yonetim-sistemi sitesinden alındı.

Airway Post İnternet Sitesi, (2023, 16 Şubat), Almanya havalimanlarına siber saldırı yapılıyor. Erişim Tarihi: 18 Haziran 2024 tarihinde https://www.airwaypost.com/almanya-havalimanlarina-siber-saldiri-yapiliyor/ adresinden alındı.

Aktaş K., (2020). ISO 27001 Bilgi Güvenliği Yönetim Sistemi: Erişim Kontrol Politikasi Üzerine Bir İnceleme, (Yayın No: 632526), [Doğuş Üniversitesi, Yüksek Lisans Tezi], https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Alemdaroğlu A., (2020). Çalışanların Bilgi Güvenliği Farkındalığına İlişkin Algıları: Bankacılık Sektöründe Bir Araştırma, (Yayın No: 650063), [İstinye Üniversitesi, Yüksek Lisans Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Aliusta C. ve Benzer R., (2018).Avrupa Siber Suçlar Sözleşmesi Ve Türkiye'nin Dahil Olma Süreci. Türkiye, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, Cilt:4, No:2, S:35-42, 2018. Gazi Üniversitesi, Bilişim Enstitüsü, Ankara.

Anayasa Mahkemesi Kararı, (2019). 2017/16 Esas 2019/64 Karar Numaralı, 24.07.2019 Tarihli Kararı. Resmi Gazete:13.11.2019 Tarih ve 30947 Sayı. 17 Nisan 2024 tarihinde https://normkararlarbilgibankasi.anayasa.gov.tr adresinden alındı.

AND Akademi İnternet Sitesi, (t.y.). ISO 27002:2022 Revizyonu İle Neler Değişti?. Erişim Tarihi: 11 Nisan 2023 tarihinde https://andbelgelendirme.com/iso-27002-2022-revizyonu-ile-neler-degisti sitesinden alındı.

Antunes, M., Maximiano, M., Gomes, R. ve Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, 1 (2), 219–238. https://doi.org/10.3390/jcp1020012.

Araalan, C. (2020). Teknik Ve Hukuki Boyutlarıyla Elektronik Ödeme Sistemlerinde Siber Güvenlik. Yayın No: 653998 [İstanbul Bilgi Üniversitesi İ, Yüksek Lisans Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Arroyabe I.F., Arranz C., Arroyabe M.F. ve Arroyabe D.C.F., (2023), Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Volume 124, 102954, https://doi.org/10.1016/j.cose.2022.102954 Elsevier, Science Direct

Arslan S., (2018). Sosyal Medya Platformları Üzerinden Kişilik Hakları İhlali, Korunmasına Yönelik Düzenlemeler, Ülke Uygulamaları, Sorunlar Ve Çözüm Önerileri, Bilişim Uzmanlığı Tezi. Bilgi Teknolojileri ve İletişim Kurumu BTK Yayın No: 0256, BTK ISBN 978-605-345-145-7

Aselsan, (2022, Ağustos). Tedarik Zinciri Saldırıları. Aselsan A.Ş. Aylık İletişim Bülteni, Bilgi Yönetimi Direktörlüğü, Ağustos 2022, Sayı:50, s.24-25. Erişim Tarihi: 18 Nisan 2023 tarihinde https://wwwcdn.aselsan.com/api/file/ASELSANabulten50.pdf sitesinden alındı.

Aslay F., (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. International Journal of Multidisciplinary Studies and Innovative Technologies, 1(1): 24 – 28.

Atakan M., (2021). Siber Güvenlik Risklerinin ve Covid-19 Salgınının Uzaktan Denetim Üzerindeki Etkileri, *Hakemli Denetişim Ortak Aklın Harmanı* Yıl: 11, Sayı: 22, s.27.

Atiker Yazılım İnternet Sitesi, (2019, 3 Mayıs). Stok ve Depo Modülü. Erişim Tarihi: 6 Mayıs 2024 tarihinde https://forum.atikeryazilim.com.tr/stok-revizyon-uygulamasi_topic471.html ve https://forum.atikeryazilim.com.tr/depolar-arasi-transfer-dat_topic245.html adresinden alındı.

Avci S.B. ve Karataş A., (2017), Lojistik Bilgi Sistemi Güvenliği Kültürü Üzerine Bilgi Sistem Güvenliği Farkındalığı ve Bağlılığının Etkisi: Kargo Lojistik Firmalarından Bulgular, *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi,* Cilt: 31 2017 Sayı: 3

Aver H., (2020). Endüstriyel Siber Güvenlik Anketi 2020, Kaspersky Daily, Kaspersky Endüstriyel Siber Güvenlik, Erişim Tarihi: 3 Mayıs 2021 tarihinde https://www.kaspersky.com.tr/blog/industrial-cybersecurity-2020/8840/, https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2020/ sitelerinden alındı.

Azimli M., (2013). Tedarik Zinciri Yönetiminde Kullanılan Bilişim Teknolojileri, Tedarik Zinciri ve Lojistikte BT Uygulamaları Dersi (Slayt belgesi). Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Erişim Tarihi: 27 Mart 2021 tarihinde https://www.slideshare.net/MuratAzimli/murat-azimli-tedarik-zinciri-yonetiminde-bilisim-teknolojileri sitesinden alındı.

Babaeinesami A., Tohidi H. ve Seyedaliakbar S.M., (2020). A Closed Loop Stackelberg Game İn Multi-Product Supply Chain Considering İnformation Security: A Case Study. Advances in Production Engineering & Management Volume 15, Number 2, June 2020, s. 233–246, ISSN 1854-6250, https://www.researchgate.net/publication/343452849, https://doi.org/10.14743/apem2020.2.361

Bağrıaçık, S. N.,(2017). ‘’Türk Ticaret Kanunu’nda m.55/b-3’e Göre Üretim ve İş Sırrının Korunması’’. Üretim ve İş Sırlarının Korunması, s.110. İstanbul: On İki Levha Yayıncılık, Aralık 2017, ISBN: 978-605-152-644-7

Baltacı Hukuk İnternet Sitesi, (2016, 3 Mayıs). Türk Ceza Kanunu Madde Gerekçeleri. Erişim Tarihi: 9 Mart 2021 tarihinde http://www.baltaci.av.tr/turk-ceza-kanunu-madde-gerekceleri/ sitesinden alındı.

Bargshady G., Zahraee S.M., Parto A. ve Ahmadi M., (2016). The Effect Of Information Technology On The Agility Of The Supply Chain in The Iranian Power Plant Industry. *Journal of Manufacturing Technology Management*, 27 (3), s. 427- 442. DOI:10.1108/JMTM-11-2015-0093.

Başar C., (2020). *Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması.* İstanbul, On İki Levha Yayıncılık, ISBN: 978-625-7899-40-6.

Batı Akdeniz İhracatçılar Birliği, (2017). ISO/27001 EK-A Maddeleri. Batı Akdeniz İhracatçılar Birliği, 2017/093 Sirküler (12.05.2017), Batı Akdeniz İhracatçılar Birliği Üyelerine Sirküler 2017-093. Erişim Tarihi: 16 Mart 2021 tarihinde https://baib.gov.tr/tr/aktuel-sirkuler-2017-yili-sirkulerleri-2017093-sirkuler-12052017.html adresinden alındı.

Baylan H.C., (2020, Aralık). Ticari Sırların Korunması, 30 Ocak 2021 tarihinde https://www.erdem-erdem.av.tr/bilgi-bankasi/ticari-sirlarin-korunmasi sitesinden alındı.

Bhargava B., Ranchal R. ve Othmane L.B., (2013). Secure Information Sharing in Digital Supply Chains, 2013 3rd IEEE International Advance Computing Conference (IACC), https://doi.org/10.1109/IAdCC.2013.6514473

BG Hukuk İnternet Sitesi, (2021, 3 Mayıs). Kişisel Verilerin Korunmasına Neden İhtiyaç Duyulmuştur? Erişim Tarihi: 8 Haziran 2021 tarihinde https://www.bghukukburosu.com/kisisel-verilerin-korunmasina-neden-ihtiyac-duyulmustur/ sitesinden alındı.

Big Danışmanlık İnternet Sitesi, (2023, 8 Mayıs). ISO 27001 ve Cumhurbaşkanlığı Bilgi ve İletişim Rehberi Arasındaki Farkı Anlamak. Erişim Tarihi: 11 Temmuz 2023 tarihinde https://www.bigdanismanlik.com.tr/iso-27001-2/ sitesinden alındı.

Bilgi Teknolojileri ve İletişim Kurumu, (2023, Mart). Uluslararası Elektronik Haberleşme Sektöründe Gelişmeler Bülteni Sayı:190. Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı. Ankara.

Bilgiç E. Türkmenoğlu, M.A. ve Koçak, A., (2020). Dijitalleşmenin Lojistik Yönetimi Bağlamında İncelenmesi, *BEÜ İİBF AİD*., 5(1), 56-69.).

Boiko A., Shendryk V. ve Boiko O., (2019). Information systems for supply chain management: uncertainties, risks and cyber security, https://doi.org/10.1016/j.procs.2019.01.108, *Science Direct Procedia Computer Science Volume,* 149, 65-70

Bolhari A., (2009). Electronic-Supply Chain Information Security: A Framework for Information Security in e-SCM (e- SCIS), 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd, https://doi.org/10.4225/75/57b404e730ded, https://ro.ecu.edu.au/ism/10

Boyar-Sozonovitch A.S., Pitelinskiy K.V. ve Ermolatiy D.A., (2019). Innovation Economy: Aspects Of Economic And Information Security İn Logistics İnnovation. Web of Science Accession Number: WOS:000479315400001, *Publisher Amazonia Investiga,* 8(21), 6-13.

BT Haber İnternet Sitesi. (2021, 18 Şubat). ‘’Covid-19 İle Kritik Sektörlerin Siber Güvenliğini Hatırladık’’. Erişim Tarihi: 25 Mart 2021 tarihinde https://www.bthaber.com/covid-19-ile-kritik-sektorlerin-siber-guvenligini-hatirladik/ sitesinden alındı.

BTK İnternet Sitesi, (2020), Bilgi Güvenliği Standartları Tanımı. Bilgi Teknolojileri ve İletişim Kurumu. Erişim Tarihi: 11 Şubat 2020 tarihinde https://www.btk.gov.tr/ilgili-standartlar adresinden alındı

Burrell D.N., Bhargava N., Swanson O.B., Harmon M., Wright J., Springs D., vd., (2020). Supply Chain And Logistics Management And An Open Door Policy Concerning Cyber Security Introduction, *International Journal of Management and*

Sustainability 2020 Vol. 9, No. 1, pp. 1-10. ISSN(e): 2306-0662 ISSN(p): 2306-9856, DOI: 10.18488/journal.11.2020.91.1.10

Can M., (2012, 1 Ocak). ISO ve Standartlara Genel Bakış, ISO 27001'ye göre Bilgi ve Bilgi Güvenliği-Bölüm 1, Erişim Tarihi: 27 Şubat 2021 tarihinde https://www.cozumpark.com/iso-ve-standartlara-genel-bakis-iso-27001-ye-gore-bilgi-ve-bilgi-guvenligi-bolum-1 adresinden alındı.

Cheung K.F ve Bell M.G.H., (2019). Attacker–Defender Model Against Quantal Response Adversaries For Cyber Security In Logistics Management: An İntroductory Study. ScienceDirect, *European Journal of Operational Research,* Volume 291, Issue 2, s.471-481, https://doi.org/10.1016/j.ejor.2019.10.019

Cheung K-F, Bell M.G.H. ve Bhattacharjya J., (2021), Cyber Security In Logistics And Supply Chain Management: An Overview And Future Research Directions. *ScienceDirect Transportation Research Part E: Logistics and Transportation Review*, 146, 102217. https://doi.org/10.1016/j.tre.2020.102217

Colicchia C., Creazza A. ve Menachof D.A., (2019). Managing Cyber and Information Risks in Supply Chains: insights from an Exploratory Analysis. *Supply Chain Management An International Journal* 24(2), Emerald Group Publishing Ltd. ISSN:1359-8546, DOI:10.1108/SCM-09-2017-0289

Çağlayan R., (2018). *İdare Hukuku Dersleri Temel Bilgiler,* Ankara, Adalet Yayınevi,

5 bs., s. 71.

Çek E., (2017). Kurumsal Bilgi Güvenliği Yönetişimi Ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi. (Yayın No: 496021), [İstanbul Bilgi Üniversitesi, Yüksek Lisans Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

CottGroup İnternet Sitesi, (2022, 9 Şubat). Kişisel Verilerin Korunması Kanunu ve ISO 27001:2013 Karşılaştırması. Erişim Tarihi: 11 Ocak 2023 tarihinde https://www.cottgroup.com/tr/blog/kvkk-gdpr/item/iso-27001-kvkk-iliskisi sitesinden alındı.

Çubukçu F. (2018). Bilgi Güvenliği Yönetim Sistemi ISO 27001:2013 Uygulama Kılavuzu. İstanbul: Pusula Yayınevi. ISBN NO: 978-605-2359-59-4, s.93

Davis A., (2015). Building Cyber-Resilience into Supply Chains. *Technology Innovation Management Review April 2015*, 5(4):19- 27, https://doi.org/10.22215/timreview/887

Deloitte İnternet Sitesi, (t.y.). Avrupa Birliği Siber Güvenlik Kanunu. Erişim Tarihi: 10 Haziran 2022 tarihinde https://www2.deloitte.com/tr/tr/pages/risk/topics/cyber-risk/articles/avrupa-birligi-siber-guvenlik-kanunu.html sitesinden alındı.

Deniz Ş.Ü., (2017). Tedarik Zincirinde Dış Kaynak Kullanımı Olarak Taşıma Sözleşmelerinde Yaşanan Sorunlar Ve Çözüm Önerileri. (Yayın No:486396) [Maltepe Üniversitesi, Doktora Tezi]. s.9,11,12. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Denolf J.M., Trienekens J., Vorst J.V.d. ve Omta O., (2015). The Role Of Governance Structures İn Supply Chain Information Sharing. *Article in Journal on Chain and Network Science January; 15*(1): 83-99, Wageningen Academic Publishers, DOI:10.3920/JCNS2014.0004

Diamantopoulou V.,Tsohou A. ve Karyda M., (2020), From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance. Computer Security, 238-257. DOI:10.1007/978-3-030-42048-2_16https://www.researchgate.net/publication/339402861.

Di G. ve Libin G., (2010). The Study of Security of Network Management Information System Based on Logistics Information Platform. 2010 Second International Conference on Multimedia and Information Technology https://doi.org/10.1109/MMIT.2010.87 24-25 April 2010

Digital Report İnternet Sitesi, (2022, 15 Haziran). ‘’KOBİ’ler siber saldırılara yüzde 350 daha fazla maruz kalıyor’’. Erişim Tarihi: 22 Haziran 2022 tarihinde https://digitalreport.com.tr/2022-veri-ihlali-sorusturma-raporu-aciklandi-91214/ sitesinden alındı.

Duran G. ve Türkoğlu M., (2019). Lojistik Sektörünün Önemi ve Bölgesel Kalkınmaya Katkıları. Isparta Uygulamalı Bilimler Üniversitesi, *Uygulamalı Sosyal Bilimler ve Güzel Sanatlar Dergisi (SOSGÜZ)*, Cilt : 1, Sayı: 2 s.:86-97

Durowoju O.A. ve Chan H.K., (2012). The Role of Integration in Information Security Breach Incidents. 17th International Working Seminar on Production Economics, Austria, s. 129-140, https://www.researchgate.net/publication/268367033_The_Role_of_Integration_in_Information_Security_Breach_Incidents

Durowoju O.A., Chan H.K. ve Wang X., (2022). Investigation of the Effect of e-Platform Information Security Breaches: A Small and Medium Enterprise Supply Chain Perspective. *IEEE Transactions on Engineering Management,* Volume: 69, Issue: 6, s.3694 – 3709, https://doi.org/10.1109/TEM.2020.3008827, https://researchonline.ljmu.ac.uk/id/eprint/13301,

Durowoju O.A., Chan H.K., Wang X. ve Akenroye T., (2020). Supply Chain Redesign Implications To Information Disruption Impact. *International Journal Of Production Economics*, V.232, 107939, https://doi.org/10.1016/j.ijpe.2020.107939

Dülger M.V., (2019). Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması. *Yaşar Hukuk Dergisi* 1(2)., 71-174.

Dwivedi S.K., Amin R. ve Vollala S., (2020). Blockchain Based Secured Information Sharing Protocol In Supply Chain Management System With Key Distribution Mechanism. *Journal of Information Security and Applications*, https://doi.org/10.1016/j.jisa.2020.102554

Elektronik Haberleşme Kanunu, (10 Kasım 208) (2008Md. 60/11. 5809 Sayılı Elektronik Haberleşme Kanunu,). T.C. Resmi Gazete. 27050. 10 Kasım 2008. Ankara: Türkiye Büyük Millet Meclisi.

Ekiz, D. (2003). Eğitimde Araştırma Yöntem ve Metotlarına Giriş- Nitel, Nicel ve Eleştirel Kuram Metodolojileri. s.20. Ankara: Anı Yayıncılık.

Elhabashy A.E., Wells L.J. ve Camelio J.A., (2019), Cyber-Physical Security Research Efforts in Manufacturing – A Literature Review, *Procedia Manufacturing Volume 34*, s.921-931, www.sciencedirect.com, https://doi.org/10.1016/j.promfg.2019.06.115

ENISA Siber Tehdit Ortam Raporu. (2020). Araştırma Raporları, Siber Güvenlik. Retrieved from https://penceremden.com/enisa-siber-tehdit-ortam-raporu-1/), Nisan 2022 de erişildi. 16.11.2020

Epiphaniou G., Pillai P., Bottarelli M., Maple C., Al-Khateeb H. ve Hammoudesh M., (2020). Electronic Regulation of Data Sharing and Processing Using Smart Ledger Technologies for Supply-Chain Security. *IEEE Transactions on Engineering Management* Vol. 67, No. 4, November 2020, s:1059 – 1073, DOI: 10.1109/TEM.2020.2965991

EPN Haber Merkezi, (2023, 10 Ocak). Türkiye 2022'de 1 Milyon Siber Saldırıya Tanık Oldu. Erişim Tarihi: 20 Şubat 2023 tarihinde https://epnext.com/turkiye-2022de-1-milyon-siber-saldiriya-tanik-oldu/ sitesinden alındı.

Erden C., (2021, 8 Mart). Lojistik İş Süreçleri ve Tedarik Zinciri Aşamaları. Sakarya Uygulamaları Bilimler Üniversitesi. [Video] Erişim Tarihi: 22 Nisan 2022 tarihinde https://www.youtube.com/watch?v=9LCop0R4MHg sitesinden alındı.

Ernst ve Young, (2024, 17 Ocak). EY Küresel Siber Güvenlik Liderliği İçgörüleri araştırması yayımlandı. EY Basın Bülteni. Erişim Tarihi: 18 Mart 2024 tarihinde https://www.ey.com/tr_tr/news/2024/1/ey-kuresel-siber-guvenlik-liderligi-icgoruleri-arastirmasi-yayimlandi sitesinden alındı.

Estay D.A.S.,(2017). Managing Cyber-Risk And Security in The Global Supply Chain: A Systems Analysis Approach To Risk, Structure And Behaviour. DTU Management Engineering, Department of Management Engineering Technical University of Denmark, PhD Thesis. 01.01.2023 tarihinde https://orbit.dtu.dk/en/publications/managing-cyber-risk-and-security-in-the-global-supply-chain-a-sys adresinden alındı.

E-Şirket İnternet Sitesi, (t.y.). Mars Lojistik Ulus.Taş.Dep.Dağ.ve Tic. AŞ. Bilgi Toplumu Hizmetleri. Erişim Tarihi: 5 Mayıs 2024 tarihinde https://e-sirket.mkk.com.tr/?page=company&company=10950# sitesinden alındı.

Evrin V. ve Demirer M., (2011). Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği. IV. Ağ Ve Bilgi Güvenliği Sempozyumu 2011, s.30-31, Ankara.

Farah, M., Ukwandu, E., Hindy , H., Brosset, D., Bures, M., Andonovic, I.,ve Bellekens, X. (2022). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. MDPI, Information 2022, 13, 22, https://www.mdpi.com/2078-2489/13/1/22/htm, DOI: 10.3390/info13010022

Fernando Y., Chidambaram R.R.M. ve Wahyuni I.S., (2018). The Impact of Big Data Analytic and Data Security Practices on Service Supply Chain Performance. *Emerald Group Publishing*, 25 (9) s. 4009-4034 ISSN 14635771, www.emeraldinsight.com/1463-5771.htm, DOI 10.1108/BIJ-07-2017-0194

Filho N.G., Rego N. ve Claro J., (2021), Supply Chain Flows And Stocks As Entry Points For Cyber-Risks. *Procedia Computer Science Volume* 181, s.261-268, Elsevier, https://doi.org/10.1016/j.procs.2021.01.145

Fu Y. ve Zhu J., (2017). Operation Mechanisms for Intelligent Logistics System: A Blockchain, Perspective. *IEEE Access Volume XX*, 2017, https://doi.org/10.1109/ACCESS.2019.2945078

Ghadge A., Weiß M., Caldwell N. ve Wilding R., (2019). Managing Cyber Risk In Supply Chains: A Review And Research Agenda. Supply Chain Management: An International Journal, *Emerald*, 25/2 s.223-240, http://dx.doi.org/10.2139/ssrn.3426030

Girgin G., (2020). Salgın Dönemi Lojistikte Dijital Altyapının Önemini Ortaya Çıkardı. 19 Ocak 2021 tarihinde https://www.kargohaber.com/salgin-donemi-lojistikte-dijital-altyapinin-onemini-ortaya-cikardi-5820h.htm adresinden alındı.

Gov.uk., (2021, 3 24). Cyber Security Breaches Survey 2021 Rapor Analizi, Erişim Tarihi: 3 Mayıs 2021 tarihinde http://bit.ly/NS202104-Report adresinden alındı.

Gov.uk (2022, 3 30), Cyber Security Breaches Survey 2022 Rapor Analizi, Erişim Tarihi: 8 Mayıs 2022 tarihinde https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022 adresinden alındı.

Gov.uk (2023, 4 19), Cyber Security Breaches Survey 2023 Rapor Analizi, Erişim Tarihi: 10 Aralık 2023 tarihinde https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023 adresinden alındı.

Göktaş, B.,(2022, 25 Temmuz). Şimdiye Kadarki En Büyük 20 GDPR Cezası. Nesil Teknoloji. Erişim Tarihi: 14 Eylül 2022 tarihinde https://www.nesilteknoloji.com/simdiye-kadarki-en-buyuk-20-gdpr-cezasi/ sitesinden alındı.

Güden A. ve Girinti D., (t.y.). Kişisel Verilerin Korunması Kanunu "KVKK" ve Genel Veri Koruma Yönetmeliği "GDPR" Üzerine Karşılaştırma. Guden Avukatlık Bürosu. Erişim Tarihi: 17 Şubat 2024 tarihinde https://www.guden.av.tr/kvkk-gdpr-uzerine-karsilastirma sitesinden alındı.

Gülenç İ.F. ve Karagöz B.. (2008). E-Lojistik Ve Türkiye'de E-Lojistik Uygulamaları. *Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* (15) 2008 / 1 : 73-91

Gürel B., (t.y.). BG Hukuk Bürosu. Erişim Tarihi: 12 Mart 2022 tarihinde https://www.bghukukburosu.com.tr/8910/ sitesinden alındı.

Güler Ş., (2022). Egzersiz Liderlerinin Özliderlik Algıları İle Egzersiz Katılımcılarının Temel Psikolojik İhtiyaçları Arasındaki İlişkinin İncelenmesi. (Yayın No: 715112), [Marmara Üniversitesi, Yüksek Lisans Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Hashem A.E.A., Hossam A. ve Hanafy H., (2017). Impact of Information Security Initiatives on Supply Chain Performance. *Supply Chain Management Journal,* 2017, Volume 8, Number1, https://www.researchgate.net/publication/322477689

Hatemi H., (1979). Medeni Hukuk Tüzel Kişileri, İstanbul Üniversitesi Yayınları No: 2280, İstanbul, Sulhi Garan Matbaası Koll Şti., s. 2

Hatipoğlu C. ve Tunacan T., (2021). Türkiye'de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması. *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi* 8(1), 430-445, e-ISSN:2458-7575. https://doi.org/10.35193/bseufbd.838732

Henkoğlu, T., (2015), Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi, (Yayın No: 380076), [Hacettepe Üniversitesi, Doktora Tezi], https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp, Ankara

Henkoğlu T., Yılmaz B., (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları, *Türk Kütüphaneciliği* 27, 3 (2013), 451-471, Ankara

Hürriyet Gazetesi İnternet Sitesi, (2020, 28 Mayıs), Avrupa Genel Veri Koruma Yönetmeliği (GDPR) ikinci yaşını kutluyor, Teknoloji Haberleri, Erişim Tarihi: 10 Temmuz 2023 tarihinde https://www.hurriyet.com.tr/teknoloji/avrupa-genel-veri-koruma-yonetmeligi-gdpr-ikinci-yasini-kutluyor-41526878 adresinden alındı.

ICT Media, (2019, 16 Temmuz). Veri ihlaline uğrayan British Airways ve Marriott'a ceza yağdı. Erişim Tarihi: 15 Eylül 2022 tarihinde https://ictmedia.com.tr/haber/veri-ihlaline-ugrayan-british-airways-ve-marriotta-ceza-yagdi adresinden alındı.

ISO/IEC, (2022). TS ISO/IEC 27001:2022, ISO/IEC 27001:2022, Türk Standardları Enstitüsü. Ankara. 03.02.2024 tarihinde https://intweb.tse.org.tr/Standard/Standard/StandardAra.aspx adresinden alındı.

İSO Yeşil Blog, (2024, 11 Ocak). Küresel Riskler Raporu 2024 yayımlandı. İstanbul Sanayi Odası Sürdürülebilirlik Vizyonu. Erişim Tarihi: 20 Nisan 2024 tarihinde https://www.isoyesilblog.com/kuresel-riskler-raporu-2024-yayimlandi/ adresinden alındı.

İstanbul Ticaret Gazetesi İnternet Sitesi, (2024, 12 Şubat). Avrupa'da 4, ABD'de 2 yurtdışı lojistik dağıtım ağına onay verildi. Erişim Tarihi: 20 Haziran 2024 tarihinde https://istanbulticaretgazetesi.com/tr/avrupada-4-abdde-2-yurtdisi-lojistik-dagitim-agina-onay-verildi sitesinden alındı.

Jalali M., Siegel M. ve Madnick S., (2019), Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*,28 (1), 66-82 https://doi.org/10.1016/j.jsis.2018.09.003

Jbair, M., Ahmad, B., Maple, C. ve Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. ScienceDirect, Computers in Industry www.elsevier.com/locate/compind, DOI: 10.1016/j.compind.2022.103611

Jianqiang G. , Shue M. ve Weijun Z., (2015). Analyzing Information Security Investment in Networked Supply Chains. IEEE 2015 International Conference on Logistics, *Informatics and Service Sciences*. DOI: 10.1109/LISS.2015.7369701

Kalitest İnternet Sitesi, (t.y.). ISO/IEC 27001:2022 Revizyonu Geçiş Kılavuzu. Erişim Tarihi: 11 Nisan 2023 tarihinde https://www.kalitest.com.tr/Haber/13/ISO-270012022-standardi-revize-olduDetayli-bilgi-ve-gecis-kilavuzunu-indirmek-icin-tiklayiniz sitesinden alındı.

Karaca M., (2019). Kritik Altyapılara Yönelik Bilişim Suçları; Türkiye ve AB Uygulamaları. (Yayın No: 604541), [İstanbul Şehir Üniversitesi, Yüksek Lisans Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Karasar, N. (1999). Bilimsel Araştırma Yöntemi-Kavramlar, İlkeler, Teknikler (9. baskı). Ankara: Nobel Yayın Dağıtım. s.79

Karasar, N., (2005), *Bilimsel Araştırma Yöntemi,* Ankara: Nobel Yayım Dağıtım, a.97

Karasar, N. (2010). *Bilimsel Araştırma Yöntemi,* 22. Baskı. Nobel Yayın Dağıtım. Ankara

Kattan I.A., Nunu A.A. ve Saleh K., (2009). A Stochastic Model For Improving Information Security in Supply Chain Systems. Supply Chain Optimization, Management and Integration, *36 Int'l Journal of Information Systems and Supply Chain Management, 2*(3), 35-50, DOI: 10.4018/978-1-60960-135-5.ch014

Kechagias, E., Chatzistelios, G., Papadopoulos, G. ve Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, 37, 100526, ScienceDirect,www.elsevier.com/locate/ijcip,https://doi.org/10.1016/j.ijcip.2022.100526.

Khan O. ve Estay D.S., (2015). Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. *Technology Innovation Management Review* 5(4), s:6-12, April 2015,DOI:10.22215/timreview/885,,https://www.researchgate.net/publication/326309680

Kılıç B., (2019). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Açısından Türkiye' de Hukuk Bürolarında Bilgi Güvenliği Yönetimi. (Yayın No: 607327), [Gazi Üniversitesi, Yüksek Lisans Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Kişisel Verilerin Korunması Kanunu, (2016). Md. 18. 6698 Sayılı Kişisel Verilerin Korunması Kanunu, T.C. Resmi Gazete. 29677. 7 Nisan 2016 Ankara: Türkiye Büyük Millet Meclisi.

Kişisel Verileri Koruma Kurumu, (t.y.). Kişisel Verilerin Korunması Kanunu ve Uygulaması. 10 Mart 2021 tarihinde https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf sitesinden alındı.

Kişisel Verileri Koruma Kurumu, (t.y.). Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Yasal Düzenlemeler. Erişim Tarihi:7 Mart 2021 tarihinde https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler sitesinden alındı.

Kişisel Verileri Koruma Kurumu, (t.y.). Kişisel Verilerin İşlenme Şartları. 14 Mart 2021 tarihinde https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari adresinden alındı.

Kişisel Verileri Koruma Kurumu, (t.y.). VERBİS-Veri Sorumluları Sicil Bilgi Sistemi. 21 Nisan 2024 tarihinde https://verbis.kvkk.gov.tr/ sitesinden alındı. Ankara

Kişisel Verileri Koruma Kurumu, (t.y.). Veri Sorumlusu ve Veri İşleyen. Erişim Tarihi:15 Mart 2021 tarihinde https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen sitesinden alındı.

Kişisel Verileri Koruma Kurumu, (t.y.).Kişisel Verileri Koruma Kurumu 2024-2028 Stratejik Plan. Erişim Tarihi:15 Mart 2024 tarihinde https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bdee3837-8560-4a02-be75-e5c312c28768.pdf sitesinden alındı.

Kişisel Verileri Koruma Kurumu, (2017, 28 Ekim). Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik. 28.10.2017 tarih ve 30224 sayılı Resmi Gazete. Erişim Tarihi:25 Ekim 2021 tarihinde https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm sitesinden alındı.

Kişisel Verileri Koruma Kurumu, (2018, Ocak). Kişisel Veri Güvenliği Rehberi (Teknik Ve İdari Tedbirler). Erişim Tarihi:10 Nisan 2023 tarihinde https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf sitesinden alındı.

Kişisel Verileri Koruma Kurumu, (2019a, Aralık). 100 Soruda Kişisel Verilerin Korunması Kanunu. KVKK Yayınları No: 03, ISBN : 978-975-19-6883-8. 11 Mart 2021 tarihinde https://kvkk.gov.tr/Icerik/2030/Rehberler sitesinden alındı.

Kişisel Verileri Koruma Kurumu, (2019b, Mart). Madde Ve Gerekçesi İle Kişisel Verilerin Korunması Kanunu (Bilgi Notu) Ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü. Erişim Tarihi: Erişim Tarihi:15 Mart 2021 tarihinde https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-

Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu sitesinden alındı.

Kişisel Verileri Koruma Kurumu, (2019c, Aralık). Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular. Erişim Tarihi:14 Mart 2021 tarihinde https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular sitesinden alındı.

Kişisel Verileri Koruma Kurumu, (2019d, Haziran). Örneklerle Kişisel Verilerin Korunması. KVKK Yayınları No.29. Erişim Tarihi:9 Mart 2021 tarihinde https://kvkk.gov.tr/Icerik/5383/Diger-Dokumanlar?&page=2 sitesinden alındı.

Kişisel Verileri Koruma Kurumu, (2019e, Aralık). Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi. Erişim Tarihi: 25 Mart 2022 tarihinde https://kvkk.gov.tr/Icerik/2030/Rehberler?&page=2 sitesinden alındı.

Kişisel Verileri Koruma Kurumu, (2024a, 5 Ocak). 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İdari Para Cezası Tutarları 2024 Yılı. 6 Şubat 2024 tarihinde https://kvkk.gov.tr/Icerik/7790/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Idari-Para-Cezasi-Tutarlari adresinden alındı.

Kişisel Verileri Koruma Kurumu, (2024b, 10 Temmuz). Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkındaki Yönetmelik. 10 Temmuz 2024 tarih ve 32598 sayılı Resmi Gazete. Erişim Tarihi:21 Temmuz 2024 tarihinde https://www.resmigazete.gov.tr/eskiler/2024/07/20240710-2.htm adresinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2018). 19.11.2018 tarih ve 2018/131 sayılı karar, Erişim Tarihi:17 Ağustos 2021 tarihinde https://www.kvkk.gov.tr/Icerik/5423/2018-131 sitesinden erişildi.

Kişisel Verileri Koruma Kurulu Kararı, (2019). 17/07/2019 tarih ve 2019/222 sayılı karar. Erişim Tarihi:15 Mart 2022 tarihinde https://www.kvkk.gov.tr/Icerik/5523/-Dubsmash-Inc-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-17-07-2019-Tarihli-ve-2019-222-Sayili-Karari-Ozeti adresinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2020). 20/01/2020 tarih ve 2020/50 sayılı Kararı, Erişim Tarihi:14 Mart 2022 tarihinde https://www.kvkk.gov.tr/Icerik/7026/2020-50 sitesinden erişildi.

Kişisel Verileri Koruma Kurulu Kararı, (2021). 29.03.2021 tarih ve 2021/321 sayılı karar. Erişim Tarihi:18 Haziran 2021 tarihinde https://kvkk.gov.tr/Icerik/6936/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Yemek-Sepeti-Elektronik-Iletisim-Perakende-Gida-Lojistik-AS sitesinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2021). 11.11.2021 tarih ve 2021/1175 sayılı karar. Erişim Tarihi:12 Mart 2022 tarihinde https://www.kvkk.gov.tr/Icerik/7079/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Media-Markt-Turkey-Ticaret-Limited-Sirketi- sitesinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2021). 23/12/2021 tarih ve 2021/1324 sayılı Karar. Erişim Tarihi:12 Mart 2022 tarihinde https://kvkk.gov.tr/Icerik/7168/2021-1324 sitesinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2021). 07/10/2021 tarih ve 2021/1021 sayılı karar. Erişim Tarihi:15 Mart 2022 tarihinde https://www.kvkk.gov.tr/Icerik/7081/2021-1021 sitesinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2021). 11.11.2021 tarih ve 2021/1168, 1169, 1170, 1171, 1172, 1173, ve 1174 sayılı Kararları. Erişim Tarihi:11 Ocak 2022 tarihinde https://www.kvkk.gov.tr/Icerik/7080/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-May-Sirketler-Grubu sitesinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2022). 04.03.2022 tarih ve 2022/209 sayılı Kararı. Erişim Tarihi:20 Haziran 2022 tarihinde https://www.kvkk.gov.tr/Icerik/7190/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Marti-Ileri-Teknoloji-A-S-?s=09?utm_source sitesinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2023). 05/01/2023 tarihli ve 2023/4 sayılı Karar. Erişim Tarihi:25 Şubat 2023 tarihinde https://www.kvkk.gov.tr/Icerik/7598/2023-4 sitesinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2023). 01.06.2023 tarih ve 2023/978 sayılı karar. Erişim Tarihi:11 Mart 2024 tarihinde https://www.kvkk.gov.tr/Icerik/7618/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Arcelik-A-S- sitesinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2023). 10.08.2023 tarih ve 2023/1387 sayılı Kararı. Erişim Tarihi: 18 Temmuz 2024 tarihinde https://www.kvkk.gov.tr/Icerik/7684/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-UPS-Hizli-Kargo-Tasimaciligi-AS sitesinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2024). 24.04.2024 tarih ve 2024/657 sayılı kararı. Erişim Tarihi:5 Mayıs 2024 tarihinde https://www.kvkk.gov.tr/Icerik/7886/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Titiz-Plastik-Dis-Ticaret-ve-Sanayi-Limited-Sirketi sitesinden alındı.

Kişisel Verileri Koruma Kurulu Kararı, (2024). 02.05.2024 tarih ve 2024/693 sayılı Kararı. Erişim Tarihi:10 Mayıs 2024 tarihinde https://www.kvkk.gov.tr/Icerik/7892/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Akil-Plastik-Sanayi-ve-Ticaret-Limited-Sirketi sitesinden alındı.

Koca G. ve Tözer A., (2012). Elektronik Haberleşme Sektöründe Veri Gizliliği Düzenlemeleri. İnet-tr'12 17. Türkiye'de İnternet Konferansı Bildiriler Kitabı, 7-9 Kasım 2012, 19-25. Erişim Tarihi:8 Mart 2021 tarihinde https://inet-tr.org.tr/inetconf17/kitap/inetconf17.pdf sitesinden alındı.

Koç F., (2022, 2 Haziran). Patentli Ürünün İthali Ve Satışından Doğabilecek Hukuki Ve Cezai Sorumluluk. Erişim Tarihi:10 Eylül 2023 tarihinde https://sen.av.tr/tr/makale/patentli-urunun-ithali-ve-satisindan-dogabilecek-hukuki-ve-cezai-sorumluluk sitesinden alındı.

Köprülü B., (1967). *Medeni Hukukta Tüzel Kişiler,* İstanbul, Fakülteler Matbaası, s. 291

Kron Teknoloji, (2023, 25 Haziran). Verizon 2023 DBIR: Siber Tehditlere İlişkin Güncel İçgörüler. Erişim Tarihi:20 Ocak 2024 tarihinde https://kron.com.tr/verizon-2023-dbir-siber-tehditlere-iliskin-guncel-icgoruler sitesinden alındı.

Kunnathur A.S. ve Vaithianathan S., (2008). Information Security Issues In Global Supply Chain. IMR Conference 2008 paper, Erişim Tarihi:8 Şubat 2020 tarihinde https://www.utoledo.edu/business/ISCMIA/documents/IS_Issues_In_Global_SCM_Draft_.pdf adresinden alındı.

Kurt S., (2019). Ticari Sır, Bankacılık Sırrı Veya Müşteri Sırrı Niteliğindeki Bilgi Veya Belgelerin Açıklanması Suçu. (Yayın No: 554640), [Galatasaray Üniversitesi, Yüksek Lisans Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp.

Küçükoğlu M., (2020). Tedarik Zincirinde Risk Değerlendirme: Risklerin Tanımlanması, Gruplandırılması ve Önceliklendirilmesi Üzerine Bir Çalışma, *İşletme Araştırmaları Dergisi* 12-(2),2126-2141, s.2130,2132.

Küpeli C., (2019). Tüzel Kişi Verilerinin Korunmasında İdarenin Sorumluluğu. (Yayın No: 589429), [İstanbul Üniversitesi, Yüksek Lisans Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Latif M.N.A., Aziz N.A.A., Hüseyin N.S.N. ve Aziz Z.A., (2021), Cyber Security In Supply Chain Management: A Systematic Review, *LogForum* 17 (1), 49-57, DOI: 10.17270/J.LOG.2021555, https://www.researchgate.net/publication/350496787, p-ISSN 1895-2038

Li Y. ve Liu Q., (2021), A Comprehensive Review Study Of Cyber-Attacks And Cyber Security; Emerging Trends And Recent Developments. *Energy Reports Volume* 8176-8186, https://doi.org/10.1016/j.egyr.2021.08.126

Li W., Lai Y. ve Zhong Y., (2024), The Closer The Better: Supplier Geographic Proximity and Corporate Information Disclosure Violation. ScienceDirect, *North American Journal of Economics and Finance*, Volume 69, Part A, 102024, s.15-16. https://doi.org/10.1016/j.najef.2023.102024

Liu H., Jiang W., Feng G., Chin K.S., (2020). Information Leakage And Supply Chain Contracts. Sciencedirect, Omega Vol.90, https://doi.org/10.1016/j.omega.2018.11.003

Liu H., Sun R. ve Zhao G., (2018). A Method Of Logistics Information Security Based On Blockchain Technology. Proceedings of the 2018 3rd Joint International Information Technology, Mechanical and Electronic Engineering Conference (JIMEC 2018), Volume 3, https://www.researchgate.net/publication/330493256 https://doi.org/10.2991/jimec-18.2018.43

Lojiport Teknoloji İnternet Sitesi, (2017, 28 Haziran). Siber saldırı lojistik sektörünü de vurdu. Erişim Tarihi:22 Aralık 2021 tarihinde https://www.lojiport.com/siber-saldiri-lojistik-sektorunu-de-vurdu-98539h.htm sitesinden alındı.

Lojistik Programı, (t.y.). Nakliye Yönetim Modülü Sevkiyatlar. Erişim Tarihi: 6 Mayıs 2024 tarihinde http://www.lojistikprogrami.net/tr/project.aspx?tip=m&kod=11 sitesinden alındı.

Lojistik Programı, (t.y.). Sipariş Modülü. 6 Mayıs 2024 tarihinde http://www.lojistikprogrami.net/tr/project.aspx?tip=m&kod=11 sitesinden alındı.

Long D., (2016). Uluslararası Lojistik Küresel Tedarik Zinciri Yönetimi. Ankara: Nobel Akademik Yayıncılık.

Małkus T. ve Wawak S., (2015), Information Security In Logistics Cooperation. *Acta Logistica - International Scientific Journal about Logistics,* 2(1), s.9-14 ISSN 1339-5629, www.actalogistica.eu, DOI:10.22306/al.v2i1.32. https://www.researchgate.net/publication/285153432,

Marsh ve TÜSİAD, (2020), Türkiye Siber Risk Algı Araştırması Raporu, TZ' de Siber Risk Yönetimi. 1-31. İstanbul: Marsh&Mclennan Companies. 01. 02.2024 tarihinde https://tusiad.org/tr/yayinlar/raporlar/item/10602-2020-turkiye-siber-risk-algi-arastirmasi adresinden alındı.

Michelberger P. ve Labodi C., (2009), Development Of Information Security Management System At The Members Of Supply Chain, Annals of the University of Petrosani, *Economics,* vol.9(4), 69-78, https://www.researchgate.net/publication/46524118.

Mirtsch M., Kinne J. ve Blind K., (2021), Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions On Engineering Management*, 68 (1). DOI: 10.1109/TEM.2020.2977815.

Mirtsch M., Blind K., Koch C. ve Dudek G., (2021), Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. Elsevier, ScienceDirect, computers & security 109 (2021) 102383, https://doi.org/10.1016/j.cose.2021.102383.

Mungan, S.S., (2022). Dağıtım Lojistiğinde Paketlemenin Rekabet Avantajı Sağlanmasındaki Rolü: Balıkesir İli Uygulaması, (Yayın No: 718943), [Maltepe Üniversitesi, Doktora Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Nitelikli Veri İnternet Sitesi (t.y.). 6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar. Nitelikli Veri Kişisel Verileri Koruma Platformu. Erişim Tarihi:10 Mart 2021 tarihinde https://nitelikliveri.com/wp-content/uploads/2020/01/6698_sayili_kisisel_verilerin_korunmasi_kanununun_uygulanmasina_yonelik_soru_ve_cevaplar.pdf sitesinden alındı.

Nitelikli Veri İnternet Sitesi, (t.y.). Kişisel Verilerin Korunması Hukuku Gelişim Süreci. 8 Mart 2021 tarihinde https://nitelikliveri.com/kvkk-mevzuat/kisisel-verilerin-korunmasi-hukuku-gelisim-sureci/ sitesinden alındı.

Özsunay E., (t.y.). *Medeni Hukukumuzda Tüzel Kişiler,* İstanbul: İstanbul: Üniversitesi Yayınları s.69

Para Dergi İnternet Sitesi, (2024, 14 Mart). En çok siber saldırıya maruz kalan ülke: Türkiye. https://www.paradergi.com.tr/teknoloji/2024/03/15/en-cok-siber-saldiriya-maruz-kalan-ulke-turkiye sitesinden alındı.

Palamutçuoğlu B.T, (2012). Lojistik Yönetimi Ders Notu (Pdf Belgesi). Celal Bayar Üniversitesi Kula Meslek Yüksekokulu İşletme Yönetimi Programı. Erişim

Tarihi:8 Mart 2022 tarihinde https://www.mku.edu.tr/files/1054-29cc9f87-bbcf-4d24-b6a6-65fff6d11bc9.pdf sitesinden alındı.

Pawar S. ve Palivela H., (2022), LCCI: A Framework For Least Cybersecurity Controls to be Implemented For Small and Medium Enterprises (SMEs). *International Journal of Information Management Data Insights*.2(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080

Pham H.C., Nguyen T.T., Mcdonald S. ve Tran-Kieu N.Q., (2019). Information Sharing in Logistics Firms: An Exploratory Study of theVietnamese Logistics Sector, Science Direct Elsevier, *The Asian Journal of Shipping and Logistics*, 35(2), June 2019, Pages 87-95, https://doi.org/10.1016/j.ajsl.2019.06.001

Ried L., Carter C., Eckerd S. ve Kaufmann L., (2020). Spillover Effects Of İnformation Leakages İn Buyer-Supplier-Supplier Triads. Journal of Operations Management 67 (1), https://doi.org/10.1002/joom.1116, https://www.researchgate.net/publication/344416377

Roy A., Gupta A.D. ve Deshmukh S.G., (2012). Information Security in Supply Chains – A Process Framework. *IEEE International Conference on Industrial Engineering and Engineering Management*. https://doi.org/10.1109/IEEM.2012.6837986

Roy A. ve Kundu A., (2012). Management of Information Security In Supply Chains – A Process Framework. Computers and Industrial Engineering 42 Proceedings, CIE42 Proceedings, 16-18 July 2012 Cape Town, South Africa https://www.researchgate.net/publication/262003358

Roy A., Gupta A.D. ve Deshmukh S.G., (2013). Information Security Risk Assessment in SCM. 2013 IEEE International Conference on Industrial Engineering and Engineering Management. Electronic ISBN:978-1-4799-0986-5, DOI: 10.1109/IEEM.2013.6962561

Saatçıoğlu Y.Ö., Görçün F.Ö., Görçün Ö., Aydınocak U.E. ve Saatçıoğlu D., (2019). Bilişim Sistemleri Ve Lojistik. Eskişehir. Anadolu Üniversitesi, Açıköğretim Fakültesi Yayını. s.7,11,12,13

Safa N.S., Maple C. ve Watson T., (2017), The Information Security Landscape in Supply Chain, Science Direct, *Computer Fraud & Security*, 6, s.16-20, https://doi.org/10.1016/S1361-3723(17)30053-2

Savaş S. ve Karataş S., (2022), Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. International Cybersecurity Law Review volume 3, 7–34, Google Akademik, https://doi.org/10.1365/s43439-021-00045-4

Sayın A.A., (2017). Lojistik Risk Yönetiminde Yönetim Bilişim Sistemleri Ve Uygulaması. (Yayın No: 492168), [Selçuk Üniversitesi, Doktora Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Selvan E., (2023), Veri Diplomasisi Ve Uluslararası Veri Güvenliği Politikaları. (Yayın No: 782426). [Millî Savunma Üniversitesi, Yüksek Lisans Tezi]. Millî Savunma Üniversitesi, Atatürk Stratejik Araştırmalar Ve Lisansüstü Eğitim Enstitüsü, Stratejik İletişim Anabilim Dalı, Stratejik İletişim Programı. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Selvi B., (2020). Hızlı Tüketim Ürünlerinin Lojistiğinde Kullanılan Elektronik Sistemler Ve Endüstri 4.0: Balıkesir İli Örneği. (Yayın No:627079), [Çanakkale Onsekiz Mart Üniversitesi, Çanakkale Onsekiz Mart Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi], https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Senarak C., (2021), Port Cybersecurity And Threat: A Structural Model For Prevention And Policy Development, *The Asian Journal of Shipping and Logistics*, 37(1), March 2021, Pages 20-36, Elsevier, www.elsevier.com/locate/ajsl, https://doi.org/10.1016/j.ajsl.2020.05.001

Sindhuja P.N.,(2014). Impact Of Information Security Initiatives On Supply Chain Performance. Information Science & Technology Abstracts Information

Management Computer Security. *Emerald*, 22 (5), s.450-473, ISSN : 0968-5227, DOI: 10.1108/IMCS-05-2013-0035

Sindhuja P.N, (2021), The Impact Of Information Security Initiatives On Supply Chain Robustness And Performance: An Empirical Study. *Information and Computer Security*, 29 (2), 365-391. Emerald, https://doi.org/10.1108/ICS-07-2020-0128

Sindhuja P.N. ve Kunnathur A.S., (2015). Information Security in Supply Chains: A Management Control Perspective. *Information and Computer Security*,.23(5), s:476-496 https://www.researchgate.net/publication/ 283560388 DOI:10.1108/ICS-07-2014-0050

Smith G.E., Watson K.J. ve Baker W.H., (2008). Perception And Reality: An Introspective Study On Supply Chain Information Security Risk. IACIS, *Issues in Information Systems*, 9(2), https://doi.org/10.48009/2_iis_2008_272-278

Smith G.E., Watson K.J., Baker W.H. ve Pokorski J.A.,(2007). A Critical Balance: Collaboration And Security In The IT- Enabled Supply Chain. *International Journal of Production Research* s:2595–2613 Scopus 10, https://doi.org/10.1080/00207540601020544

Sözcü Gazetesi İnternet Sitesi, (2021, 19 Mart), Pegasustan Siber Saldırı Açıklaması. Erişim Tarihi:15 Haziran 2021 tarihinde https://www.sozcu.com.tr/2021/gundem/pegasustan-siber-saldiri-aciklamasi-6324126/ sitesinden alındı.

Speier C., Whipple J.M., Closs D.J. ve Voss M.D., (2011). Global supply chain design considerations: Mitigating product safety and security risks. *ScienceDirect, Journal of Operations Management* 29 (2011) s.721–736, doi:10.1016/j.jom.2011.06.003

Spiliotopoulou E., Donohue K. ve Gürbüz M.Ç., (2016). Information Reliability in Supply Chains: The Case of Multiple Retailers. Scopus, *Production and Operations Management.* 25(3), s:548-567. ISSN 1059-1478, DOI 10.1111/poms.12418

STM Mühendislik Teknoloji Danışmanlık, (2022), Siber Tehdit Durum Raporu Ekim-2022, s.5,10,23. Thinktech STM Teknolojik Düşünce Merkezi, 5 Aralık 2022 tarihinde https://thinktech.stm.com.tr/uploads//docs/2023-yili-pdf-leri/1675175420_stmsibertehditdurumraporuekimaralik2022.pdf? adresinden alındı.

STM Mühendislik Teknoloji Danışmanlık, (2023), Siber Tehdit Durum Raporu Ekim-Aralık 2023 s.5,6. Thinktech STM Teknolojik Düşünce Merkezi, Erişim Tarihi:14 Ocak 2024 tarihinde https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ekim-aralik-2023 adresinden alındı.

Sulu M., (2020). *Ticari Sırların Korunması.* İstanbul, On İki Levha Yayıncılık.

Suluk C., (t.y.). Ticaretle Bağlantılı Fikri Mülkiyet Hakları. Erişim Tarihi:30 Ekim 2023 tarihinde https://fikrimulkiyet.com/mevzuat/ticaretle-baglantili-fikri-mulkiyet-haklari/ sitesinden alındı.

Syed N.F., Shah S.W., Rasua R.T., Doss R., (2021), Traceability In Supply Chains: A Cyber Security Analysis, *Computers & Security* 112, 102536, Elsevier, https://doi.org/10.1016/j.cose.2021.102536

Şahinaslan E., Kantürk A., Şahinaslan Ö. ve Borandağ E., (2009), Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri, Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri 11-13 Şubat 2009 Harran Üniversitesi, 597-598, Şanlıurfa

Tan K.H., Wong W.P. ve Chung L., (2015). Information and Knowledge Leakage in Supply Chain., *Published:* 18, s. 621–638, (JUN 2016), https://doi.org/10.1007/s10796- 015-9553-6, https://www.researchgate.net/publication/276076856

Tankard C., (2015), Data Classification – The Foundation Of İnformation Security, Network Security, 8 https://doi.org/10.1016/S1353-4858(15)30038-6

Tanyaş M., (t.y.). *Lojistik Yönetimine Giriş,* Atatürk Üniversitesi, Açıköğretim Fakültesi,s.6

Tanyaş M., (2013). Lojistik ve Tedarik Zinciri Yönetimi (Slayt belgesi). Erişim Tarihi:25 Ocak 2021 tarihinde https://slideplayer.biz.tr/slide/2927432/ adresinden alındı.

Tanyaş M., (2020). Koronavirüs Salgını Tedarik Zincirlerini Kırdı. LODER Bülteni 2020-1, 15-17. Erişim Tarihi:19 Ocak 2021 tarihinde https://www.loder.org.tr/loder-bulten adresinden alındı.

T.C. Anayasası, (1982). T.C. Resmi Gazete. 17863. 9 Kasım 1982, 1982 Tarihli Türkiye Cumhuriyeti Anayasası, Ankara, Türkiye Büyük Millet Meclisi

T.C. Cumhurbaşkanlığı, (2019, 18 Temmuz).T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı 100. Yıl Türkiye Planı, 11. Kalkınma Planı (2019-2023). Erişim Tarihi:24 Ocak 2024 tarihinde https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Plani-2019-2023.pdf sitesinden alındı.

T.C. Dışişleri Bakanlığı, (2023, 5 Aralık). 95/46/AT Sayılı Direktif'i Yürürlükten Kaldıran, Gerçek Kişilerin Kişisel Verilerin İşlenmesi Bakımından Korunması ve Bu Tür Verilerin Serbest Dolaşımı Hakkında Avrupa Parlamentosu ve Konsey Tüzüğü (Genel Veri Koruma Tüzüğü). T.C. Dışişleri Bakanlığı Avrupa Birliği Başkanlığı. Erişim Tarihi:12 Ocak 2024 tarihinde https://www.ab.gov.tr/ab-genel-veri-koruma-tuzugu-gdpr-turkceye-cevrildi_53650.html adresinden alındı.

T.C. Kalkınma Bakanlığı, (2018). 11. Kalkınma Planı Lojistik Hizmetlerinin Geliştirilmesi Özel İhtisas Komisyonu Raporu (2019-2023). Yönetim Hizmetleri Genel Müdürlüğü, Bilgi Ve Belge Yönetimi Dairesi Başkanlığı Yayın NO: KB: 3036- ÖİK: 818. Ankara

T.C.Kültür ve Turizm Bakanlığı, (t.y.). Ticaretle Bağlantılı Fikri Mülkiyet Anlaşması (TRIPS). Erişim Tarihi: 30 Eylül 2023 tarihinde https://telifhaklari.ktb.gov.tr/TR-332365/ticaretle-baglantili-fikri-mulkiyet-anlasmasi-trips.html sitesinden alındı.

T.C. Kültür ve Turizm Bakanlığı, (t.y.). Fikir Mülkiyeti Haklarının Ticari Niteliklerine İlişkin Anlaşma (TRIPS Agreement 1994). Erişim Tarihi:30 Eylül 2023 tarihinde https://telifhaklari.ktb.gov.tr/Eklenti/106881,trps20120318183846pdf.pdf?0 ve

https://telifhaklari.ktb.gov.tr/TR-332441/uluslararasi-sozlesmeler.html.sitelerinden alındı.

T.C. Milli Eğitim Bakanlığı, (2011). *Lojistik Yönetimi,* Ankara: Ulaştırma Hizmetleri, s.6-7

T.C. Resmi Gazete, (2005). Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri Ve Sınıflandırılması Hakkında Yönetmelik. Resmi Gazete no 25997, 18 Kasım 2005 Erişim Tarihi:17 Şubat 2021 tarihinde https://www.resmigazete.gov.tr/ sitesinden alındı.

T.C. Resmi Gazete, (2023). Küçük Ve Orta Büyüklükteki İşletmeler Yönetmeliği. Resmi Gazete no 32201 Tarih: 25 Mayıs 2023. Erişim Tarihi:15 Ağustos 2023 tarihinde https://www.resmigazete.gov.tr/ adresinden alındı.

T.C. Resmi Gazete. (2013). Sermaye Şirketlerinin Açacakları İnternet Sitelerine Dair Yönetmelik. Resmi Gazete no 28663 Tarih: 31 Mayıs 2013. Erişim Tarihi:20 Eylül 2022 tarihinde https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=18419&MevzuatTur=7&MevzuatTertip=5 sitesinden alındı.

T.C. Resmi Gazete. (2014). Gümrük İşlemlerinin Kolaylaştırılması Yönetmeliği. Resmi Gazete No:29006 Tarih: 21.05.2014. Erişim Tarihi:28 Mart 2021 tarihinde https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19689&MevzuatTur=7&MevzuatTertip=5 sitesinden alındı.

T.C. Resmi Gazete. (2022). Bağımsız Denetime Tabi Şirketlerin Belirlenmesine Dair Karar. Resmi Gazete No: 32029, Tarih: 30 Kasım 2022. Erişim Tarihi:5 Mart 2023 tarihinde https://www.resmigazete.gov.tr/eskiler/2022/11/20221130-14.pdf sitesinden alındı.

T.C. Resmi Gazete, (2022). Yurt Dışı Lojistik Dağıtım Ağlarının Desteklenmesi Hakkında Karar. Resmi Gazete No: 31815. 20 Nisan 2022. Erişim Tarihi:1 Ağustos 2023 tarihinde https://www.mevzuat.gov.tr/MevzuatMetin/20.5.5449.pdf sitesinden alındı.

T.C. Resmi Gazete. (2023). Vergi Usul Kanunu Genel Tebliği. Resmi Gazete No: 32380. 25 Kasım 2023. Erişim Tarihi:26 Ocak 2024 tarihinde https://www.resmigazete.gov.tr/eskiler/2023/11/20231125-27.htm ve https://www.resmigazete.gov.tr/eskiler/2023/12/20231229M2-22.pdf adreslerinden alındı.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, s.38 11 Aralık 2023 tarihinde https://afyonluoglu.org/PublicWebFiles/Reports-TR/2013-2014%20Ulusal%20Siber%20Güvenlik%20Stratejisi%20ve%20Eylem%20Planı.pdf adresimden alındı.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2014).Sektörel SOME Kurulum ve Yönetim Rehberi. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Haberleşme Genel Müdürlüğü, Sürüm 1 Ankara. 11 Aralık 2023 tarihinde https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/sektorel-some-reh.pdf sitesinden alındı.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2016), 2016-2019 Ulusal Siber Güvenlik Stratejisi, s. 9,10,11,Ankara 11 Aralık 2023 tarihinde https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf adresinden alındı.

T.C. Ulaştırma ve Altyapı Bakanlığı, (2020a), Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023, s. 12,18-19,21,23-24, Ankara. 11 Aralık 2023 tarihinde https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf adresinden alındı.

T.C. Ulaştırma ve Altyapı Bakanlığı, (2020b). Türkiye Ulaştırma Politika Belgesi. S.10-11. Ankara11 Aralık 2023 tarihinde https://www.uab.gov.tr/uploads/pages/stratejik-yonetim/turkiye-ulastirma-politikasi-141220.pdf adresinden alındı.

T.C. Ulaştırma ve Altyapı Bakanlığı, (2021). 12. Ulaştırma ve Haberleşme Şurası Sonuç Bildirgesi. 12. Ulaştırma ve Haberleşme Şurası 6-7-8 Ekim 2021, İstanbul.

T.C. Ulaştırma ve Altyapı Bakanlığı, (2022, 1 Mart). Ulaştırma ve Altyapı Bakanlığı Lojistik ve Kombine Taşımacılık Daire Başkanlığı Taşıma İşleri Organizatörlüğü Firma Listesi. Erişim Tarihi: 20 Haziran 2022 tarihinde https://uhdgm.uab.gov.tr/uploads/pages/tasima-isleri-organizatorlugu-tio/tio-liste-xhtml.pdf sitesinden alındı.

T.C. Ulaştırma ve Altyapı Bakanlığı, (2022), 2053 Ulaştırma ve Lojistik Ana Planı, Ulaştırma ve Altyapı Bakanlığı Strateji Geliştirme Başkanlığı, s.24-27, Ankara. 11 Aralık 2023 tarihinde https://www.uab.gov.tr/uploads/pages/bakanlik-yayinlari/20221025-2053-ulastirma-ve-lojistik-ana-plani-tr.pdf adresinden alındı.

Timofeyev Y. ve Dremova O., (2022). Insurers' responses to Cyber Crime: Evidence From Russia. Science Direct, *International Journal of Law, Crime and Justice* 68. https://doi.org/10.1016/j.ijlcj.2021.100520

Topping C., Dwyer A., Michaleca O., Craggsa B. ve Rashida A., (2021), Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks, www.elsevier.com/locate/cose, https://doi.org/10.1016/j.cose.2021.102324

Tosunoğlu A., (t.y.). ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi Sertifikalı Başdenetçi Eğitim Notları (Slayt belgesi). PROKS Belgelendirme ISO 27001:2022 Geçiş Eğitimi. İstanbul.

Tosunoğlu A., (t.y.). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin KVKK'ya Etkisi. Erişim Tarihi:5 Haziran 2023 tarihinde https://proks.co/haberler/iso-iec-27001-bilgi-guvenligi-yonetim-sistemi-nin-kvkk-ya-etkisi adresinden alındı.

Tran T.T.H., Childerhouse P. ve Deakins E., (2016). Supply Chain Information Sharing: Challenges and Risk Mitigation Strategies. Emerald Insight, *Journal of Manufacturing Technology Management,* 27(8), s.1102-1126 Emerald Group Publishing, DOI 10.1108/JMTM-03-2016-0033

Tuptuk N. ve Hailes S., (2018). Security Of Smart Manufacturing Systems. *ScienceDirect Journal of Manufacturing Systems*,47 s:93-106, April 2018, https://doi.org/10.1016/j.jmsy.2018.04.007

Turan M., (2021, 1 Mart). "Kron, en sık karşılaşılan 10 siber saldırı yöntemini duyurdu." Erişim Tarihi:20 Mart 2021 tarihinde https://www.aa.com.tr/tr/sirkethaberleri/bilisim/kron-en-sik-karsilasilan-10-siber-saldiri-yontemini-duyurdu/663052 sitesinden alındı.

Türk Borçlar Kanunu, (2011). T.C. Resmi Gazete. 27836. 4 Şubat 2011. 6098 Sayılı Türk Borçlar Kanunu, Türkiye Büyük Millet Meclisi, Ankara.

Türk Ceza Kanunu, (2004). T.C. Resmi Gazete. 25611. 12 Ekim 2004. 5237 Sayılı Türk Ceza Kanunu, s.9023, Türkiye Büyük Millet Meclisi, Ankara.

Türk Medeni Kanunu, (2001). T.C. Resmi Gazete. 24607. 8 Aralık 2001 Md. 8, 4721 Sayılı Türk Medeni Kanunu, Türkiye Büyük Millet Meclisi. Ankara

Türk Ticaret Kanunu, (2011). T.C. Resmi Gazete. 27846. 14 Şubat 2011. 6102 Sayılı Kanun. Türkiye Büyük Millet Meclisi. Ankara

Türkiye Büyük Millet Meclisi,(2011, 23 Kasım). Sanayi, Ticaret, Enerji, Tabii Kaynaklar, Bilgi ve Teknoloji Komisyonu Tutanak Dergisi. Yasama dönemi 24 Yasama yılı 2 15 Haziran 2024 tarihinde https://www5.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.goruntule?pTutanakId=706 sitesinden alındı.

Türkiye Büyük Millet Meclisi, (2016). Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, Sıra sayısı: 117, Yasama Dönemi 26, Yasama Yılı 1, Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, Ankara.

Ulhag I., Kuruvilla K.T., Nkhoma M.Z., Vu H.H. ve Truong N.T., (2016). Information Security Risks In Supply Chain Management: A Review Of Literature For The Developing Country Context. *International Journal of Information System and Engineering,* 4 (2), 58-68 https://www.researchgate.net/publication/317134711, DOI: 10.24924/ijise/2016.11/v4.iss2/58.68

Uslan Y.U. ve Değirmenci S. (2023). Avrupa Birliği Genel Veri Koruma Tüzüğü Işığında Türkiye'de Kişisel Verileri Koruma Kurumu. *Optimum Ekonomi ve Yönetim Bilimleri Dergisi,* 10 (1), 23-38.

USOM, (t.y.). Ulusal Siber Olaylara Müdahale Merkezi USOM. 01.03 2021 tarihinde https://www.usom.gov.tr/hakkimizda.html, sitesinden alındı.

Varma T.N. ve Khan D.A., (2015). Information Technology And E-Risk Of Supply Chain Management. *African Journal of Business Management Academic Journal Vol.* 9(6), s. 243-258, Article Number: 60A7A0351964 ISSN 1993-8233, DOI: 10.5897/AJBM2013.7308

Velasco J., Ullauri R., Pilicita L., Jacome B., Saa P. ve Moscoso-Zea O., (2018), Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry. 2018 International Conference on Information Systems and Computer Science (INCISCOS), Date of Conference: 13-15 Nov. 2018, IEEE, DOI: 10.1109/INCISCOS.2018.00049

Vikipedi, (t.y.). Ticari Sırların Korunmasına İlişkin Yönerge. 8 Kasım 2023 tarihinde https://en.wikipedia.org/wiki/Directive_on_the_Protection_of_Trade_Secrets adresinden alındı.

Vikipedi, (2020a). Ticari Sır Tanımı. Erişim Tarihi:10 Şubat 2020 tarihinde https://tr.wikipedia.org/wiki/Ticari_sır adresinden alındı.

Vikipedi, (2020b). Genel Veri Koruma Tüzüğü (GDPR) Tanımı. 8 Şubat 2020 tarihinde https://tr.wikipedia.org/wiki/Genel_Veri_Koruma_Yönetmeliği adresinden alındı.

Vikipedi, (2020c). Siber Saldırı Tanımı. Erişim Tarihi:8 Şubat 2020 tarihinde https://en.wikipedia.org/wiki/Cyberattack adresinden alındı.

Wadhwa S., Prakash A., Deshmukh S.G. ve Wadhwa B., (2009). Information Security in Flexible Supply Chain Network: A Decision Information Security (DIS) Model. *Global Journal of Enterprise Information System* 2(1),

Wang X., (2012). Research on the Construction of Supply Chain Collaboration System Based on Information Sharing. IEEE 2012 International Conference on Information Management, *Innovation Management and Industrial Engineering,* https://doi.org/10.1109/ICIII.2012.6339704

Weaver G.A., Feddersen B., Marla L., Wei D., Rose A. ve Moer M.V., (2022), Estimating Economic Losses from Cyber-Attacks on Shipping Ports: An Optimization-Based Approach, ScienceDirect, *Transportation Research Part C: Emerging Technologies* 137, 103423, https://doi.org/10.1016/j.trc.2021.103423

Werthmuller S. ve Angajman U., (2023). Küresel Riskler 2023: Acil Yaşam Maliyeti Krizi ile Sürdürülebilir İklim Aksiyonu Arasındaki Gerilimler Doruk Noktasında. World Economic Forum News Release, Dünya Ekonomik Forumu. İsviçre.

Wolden M., Valverde R. ve Talla M.,(2015). The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System. *ScienceDirect IFAC-Conference Papers OnLine* 48-3 (2015) s:1846-1852 https://doi.org/10.1016/j.ifacol.2015.06.355

Yargıtay 4 Hukuk Dairesi, (2013). 2013/7417 Esas 2013/10004 Karar Numaralı 27.05.2013 Tarihli Kararı. Erişim Tarihi:25 Şubat 2023 tarihinde www.legal.com.tr adresinden alındı.

Yargıtay 12 Ceza Dairesi, (2014). 2013/17414 E. 2014/9013 Karar Sayılı 14.4.2014 Tarihli Kararı. Erişim Tarihi:26 Şubat 2023 tarihinde www.lexpera.com.tr sitesinden alındı.

Yargıtay 5 Ceza Dairesi, (2015). 2013/11125 Esas 2015/14700 Karar Sayılı 1.10.2015 Tarihli Kararı, Erişim Tarihi:26 Şubat 2023 tarihinde https://www.eyavuz.av.tr/ticari-sir-bankacilik-sirri-veya-musteri-sirri-niteligindeki-bilgi-veya-belgelerin-aciklanmasi-sucu/ sitesinden alındı.

Yargıtay 9 Hukuk Dairesi, (2016). 2015/5771 Esas 2016/21271 Karar Numaralı, 29.11.2016 Tarihli Kararı. Erişim Tarihi:11 Kasım 2023 tarihinde https://legalbank.net sitesinden alındı.

Yargıtay 5 Ceza Dairesi, (2017). 2014/7809 Esas 2017/118 Karar Sayılı 12.01.2017 Tarihli Kararı. Erişim Tarihi: 9 Kasım 2023 tarihinde https://barandogan.av.tr/blog/mevzuat/tck-madde-239-ticari-sir-bankacilik-sirri-veya-musteri-sirri-niteligindeki-bilgi-veya-belgelerin-aciklanmasi-sucu.html sitesinden alındı.

Yargıtay 12 Ceza Dairesi, (2018). 2017/3302 Esas 2018/1900 Karar Sayılı 21.2.2018 Tarihli Kararı. Erişim Tarihi:26 Şubat 2023 tarihinde www.lexpera.com.tr sitesinden alındı.

Yargıtay 5 Ceza Dairesi, (2019). 2016/1992 Esas ve 2019/3829 Karar Sayılı 03.04.2019 Tarihli Kararı, Erişim Tarihi:25 Şubat 2023 tarihinde www.lexpera.com.tr sitesinden alındı.

Yargıtay 23. Hukuk Dairesi, (2019), 21.10.2019 tarihli ve 2016/6958 E., 2019/4349 K. Sayılı kararı. Erişim Tarihi:29 Ocak 2021 tarihinde https://karararama.yargitay.gov.tr/ adresinden alındı.

Yargıtay 15 Ceza Dairesi, (2019). 2017/28124 Esas 2019/10556 Karar Numaralı 24.10.2019 Tarihli Kararı. Erişim Tarihi: 11 Kasım 2023 tarihinde https://legalbank.net sitesinden alındı.

Yargıtay 15 Ceza Dairesi, (2020). 2020/1582 Esas 2020/11159 Karar Sayılı 05.11.2020 Tarihli Kararı. Erişim Tarihi:25 Şubat 2023 tarihinde www.lexpera.com.tr sitesinden alındı.

Yargıtay 9 Hukuk Dairesi, (2021). 2019/2639 Esas 2021/2697 Karar Sayılı 28.01.2021 Tarihli Kararı, Erişim Tarihi:25 Şubat 2023 tarihinde www.lexpera.com.tr sitesinden alındı.

Yargıtay 5 Ceza Dairesi, (2023). 2020/6015 Esas 2023/7213 Karar Sayılı 07.06.2023 Tarihli Kararı. Erişim Tarihi:22 Şubat 2023 tarihinde www.legal.com.tr adresinden alındı.

Yıldırım, E. Y., (2018). Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması. 2. Uluslararası Mesleki Bilimler Sempozyumu, IVSS 2018, *Mesleki Bilimler Dergisi (MBD) Ankara Üniversitesi,* s. 4.

Yıldıztekin A., (2009, 1 Aralık). Lojistiğin 7 Doğrusu Yaşamımızın Doğruları Olsun. İstanbul Üniversitesi Lojistik Kulübü, Sayı 7. Erişim Tarihi:17 Ocak 2021 tarihinde https://www.lojistikkulubu.ist/lojistigin-7-dogrusu-yasamimizin-dogrulari-olsun/ adresinden alındı.

Yıldıztekin A., (2012, 27 Eylül). Lojistikte Bilgi Güvenliği ve İletişim. Erişim Tarihi:21 Aralık 2021 tarihinde http://www.lojistikdunyasi.net/lojistikte-bilgi-guvenligi-ve-iletisim.html sitesinden alındı.

Yılmaz H., (2014). TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi, Kidder Kamu İç Denetçi Derneği, *Denetişim* / 2014-15

Yılmaz M., (2018). İşletmelerde Bilgi Güvenliği Uygulama Sorunları Ve Çözüm Önerileri; Konya Örneği. (Yayın No: 529299), [KTO Karatay Üniversitesi, Yüksek Lisans Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp.S.14-15.

Yılmaz G., (2022). Kaspersky. 2023 Yılında Siber Saldırılarda Nelere Dikkat Etmeli?: 20 Mart 2023 tarihinde https://akillifabrikalar.com.tr/2023-yilinda-siber-saldirilarda-nelere-dikkat-etmeli/ adresinden alındı.

Yüksel, B.A.E., (2018), Ticari Sırların Dijital Ortamda Korunması, *TAAD*, Yıl:9, Sayı:33, s.143

Zadeh A.V., Ramayah T., Hanifah H., Kurnia S. ve Mahmud I., (2020), Supply Chain Information Integration and Its Impact on The Operational Performance of Manufacturing Firms in Malaysia, Science Direct, *Information & Management* 57(8), https://doi.org/10.1016/j.im.2020.103386

Zaralı M., (2022), Dijital Dönüşüm Çağında Siber Güvenlik Ve Mahremiyet. (Yayın No: 725152), [Bahçeşehir Üniversitesi, Yüksek Lisans Tezi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Zhang C. ve Li S., (2006). Secure Information Sharing in Internet-Based Supply Chain Management Systems. Journal of Computer Information Systems Article in *Journal of Computer Information Systems* · https://www.researchgate.net/publication/37160675

Zhang C., Duan J., Gong Y., Brown S. ve Li Z., (2020), A Content-Analysis Based Literature Review in Blockchain Adoption within Food Supply Chain, *International Journal of Environmental. Research and Public Health,* 6, 1784; doi:10.3390/ijerph17051784, www.mdpi.com/journal/ijerph

Zhang D.Y., Zeng Y., Wang L., Li H. ve Geng Y., (2011). Modeling And Evaluating Information Leakage Caused By Inferences In Supply Chains. *ScienceDirect Computers in Industry*, 62, s: 351-363, doi:10.1016/j.compind.2010.10.002

Zhang D.Y., Cao X., Wang L. ve Zeng Y., (2012). Mitigating The Risk Of İnformation Leakage In A Two-Level Supply Chain Through Optimal Supplier Selection. Scopus, *Journal of Intelligent Manufacturing* 23(4) s:1351-1364, DOI 10.1007/s10845-011-0527-3

Zhong S. ve Deng Z., (2010). Model Design of Information Security Monitoring System of Nanchang Bonded Logistics Park. IEEE, *Third International Symposium on Information Science and Engineering,* https://doi.org/10.1109/ISISE.2010.124

Zümbül Hukuk İnternet Sitesi, (2019, 7 Haziran). Avrupa Birliği Siber Güvenlik Yasası Yayımlandı. Erişim Tarihi:10 Haziran 2022 tarihinde https://www.zumbul.av.tr/tr/kisisel-verilerin-korunmas-ve-gizlilik/cybersecurity adresinden alındı.

EKLER

Ek:1: Anket Formu

I. BÖLÜM: DEMOGRAFİK SORULAR

3. 1-Şirket Adı Veya Ticaret Ünvanı

4. 2-Şirket Toplam Çalışan Sayısı

Yalnızca bir şıkkı işaretleyin.

- ◯ Çalışan Sayısı 10'dan Az
- ◯ Çalışan Sayısı 10-50 Arası
- ◯ Çalışan Sayısı 50-250 Arası
- ◯ Çalışan Sayısı 250'den Fazla

5. 3-Şirketin Sermaye Yapısı

Yalnızca bir şıkkı işaretleyin.

- ◯ Yabancı
- ◯ Yerli
- ◯ Yabancı Ortaklı

6. 4-Son Mali Yıla Ait Yıllık Geliriniz (Şirket Cirosu)

Yalnızca bir şıkkı işaretleyin.

- ◯ 5 Milyon TL altında
- ◯ 5 Milyon TL - 50 Milyon TL arasında
- ◯ 50 Milyon TL - 250 Milyon TL arasında
- ◯ 250 Milyon TL ve üzerinde

7. 5-Şirketiniz Hangi Lojistik Hizmetleri Vermektedir? (Hizmet Durumunuza Göre Birden Fazla Seçeneği İşaretleyebilirsiniz)

Uygun olanların tümünü işaretleyin.

	Taşımacılık	Gümrük	Sigorta	Depolama	Talep ve Stok Yönetimi	Muayene, Gözetim vb. Terminal Hizmetleri	Paketleme, Etiketleme vb. Katma Değerli Hizmetler
1. Satır	☐	☐	☐	☐	☐	☐	☐

8. 6- Şirketiniz Hangi Coğrafi Alanda Hizmet Vermektedir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Sadece Yurtiçi
- ◯ Sadece Yurtdışı
- ◯ Her İkisi Birlikte

9. soruya gidin

II.BÖLÜM: VERİLERE İLİŞKİN SORULAR

9. 1-Şirketinizde Hangi Türden Verilerin Kayıt Altına Alındığını Biliyor Musunuz?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim yok

10. 2-Kişisel Veriler İle Tüzel Kişi Verileri Hakkında Bilginiz Var Mı?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim yok

11. 3-Şirketinizin Veri Envanteri Bulunmakta Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim yok

12. 4-Şirketinizde Kayıt Altına Alınan Veriler Risk Ve Önemine Göre Gruplandırılmış Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

13. 5-Şirketinizde Kayıt Altına Alınan Verilere Yönelik Risklerin Gerçekleşmesi Halinde Ortaya Çıkabilecek Zararlar Konusunda Çalışma Yapılmış Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim yok

14. 6-Veriler Elektronik (Dijital) Ortamlarda Mı, Yoksa Elektronik Olmayan (Fiziki) Ortamlarda Mı Kayıt Altına Alınmaktadır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Elektronik ortamlarda
- ◯ Elektronik olmayan ortamlarda
- ◯ Her İki Ortamda

15. 7-Kişisel Veriler İle Tüzel Kişi Verilerinin Genellikle Hangi Ortamlarda (Dijital veya Fiziki) Kayıt Altına Alındığı Bilinmekte Midir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim yok

16. 8-Şirketinizde Hangi Türden Veriler Kayıt Edilmektedir? (Birden Fazla Seçeneği İşaretleyebilirsiniz.)

Uygun olanların tümünü işaretleyin.

	Personel Verileri	Operasyonel Veriler	Stratejik (Planlar) Veriler	Finansal Veriler	Tedarikçi Verileri	Depo Envanter Verileri	Müşteri Verileri	Üretim Verileri	Ziyaretçi Verileri
Seçenekler	☐	☐	☐	☐	☐	☐	☐	☐	☐

17. 9-Şirketiniz Mobil Ağına Bağlı Olan Cihaz ve Sistemlerin Veri Envanteri Çıkarılmış Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok
- ◯ Mobil Ağa Bağlı Cihaz ve Sistemimiz Bulunmamaktadır

III.BÖLÜM: BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

18. 1-ISO 27001 Bilgi Güvenliği Yönetim Sistemi Hakkında Bilginiz Var Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

19. 2-Şirketinizin ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi Bulunmakta Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

20. 3-ISO 27001 BGYS Belgesine Sahip Olmanın Firmanıza Hangi Açılardan Olumlu Etkileri Olduğunu Düşünüyorsunuz? (Birden Fazla Seçeneği İşaretleyebilirsiniz)

Uygun olanların tümünü işaretleyin.

	Veriler Koruma Altına Alındığından Müşteri Güveni Artar	Ticari Rekabete Olumlu Etkisi Olur	ISO 27001 BGYS Belgesi, Firmanın Tercih Edilmesinde Etkilidir	Hukuki Yükümlülüklere Uyumu Sağlar	Veri İhlallerine Karşı Koruma Sağlar	Veri İhlalinden Doğabilecek Maddi Zararların Oluşması Engellenir	Ticari İtibara Olumlu Etkisi Olur	Veri İhlalinde Doğabilec Cezai Yaptırımla Oluşmas Engellen
1. Satır	☐	☐	☐	☐	☐	☐	☐	☐

21. 4-ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi veya Diğer Bilgi Güvenliğine Yönelik Yıllık Giderleriniz Aşağıdaki Aralıklardan Hangisine Uymaktadır?

Yalnızca bir şıkkı işaretleyin.

- ◯ 1 TL. - 50.000 TL.
- ◯ 50.001 TL. - 100.000 TL.
- ◯ 100.001 TL. - 500.000 TL.
- ◯ 500.001 TL. - 1.000.000 TL.
- ◯ 1.000.000 TL'den Fazla
- ◯ Bilgi Güvenliğine İlişkin Bir Giderimiz Bulunmamaktadır.

22. 5-Şirketinizin Bilgi Güvenliğine Yatırım Yapmasının Temel Nedenleri Nelerdir? (Birden Fazla Seçeneği İşaretleyebilirsiniz)

Uygun olanların tümünü işaretleyin.

	Sistemlerimizi Korumak	Çalışan,Tedarikçi, Müşteri Ve Paydaşların Verilerini Korumak	Kanun Ve Yönetmeliklere Uymak	Dolandırıcılık Ve Hırsızlığı Önlemek	Ticari Sırları, Fikri Mülkiyeti Ve Diğer Varlıkları (nakit gibi) Korumak	Kesintilerin Önlenmesi Ve İş Sürekliliğinin Devamını Sağlamak	Şirket İtibarını Ve Markayı Korumak
1. Satır	☐	☐	☐	☐	☐	☐	☐

23. 6-Şirketinizde Bilgi Güvenliğinden Sorumlu Bir Kurul/Komisyon/Birim Bulunmakta Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

24. 7- Bilgi Güvenliği Kurul/Komisyon/Birimi Aşağıda Ki Seçeneklerin Hangilerinden Oluşmaktadır? (Birden Fazla Seçeneği İşaretleyebilirsiniz)

Uygun olanların tümünü işaretleyin.

	Teknoloji Birimi	Üst Yönetim	Hukuk Birimi	Bölüm Müdürleri	İnsan Kaynakları Birimi	Operasyon Sorumluları	Fikrim Yok
1. Satır	☐	☐	☐	☐	☐	☐	☐

25. 8-Şirketinizdeki Verilerin İşlenmesi, Saklanması, Korunması Ve İmhası Konusunda Prosedür ve Politikalar Belirlenmiş Midir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

26. 9-Şirketinizdeki Verilerin İşlenmesi, Saklanması ve Korunması Konusunda Denetimler Yapılmakta Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

27. 10-Şirketinizin Çalışanlarına Veriler Ve Bilgi Güvenliğine İlişkin Teknik, İdari ve Yasal Hak ve Yükümlülükler Konusunda Eğitim Verildi Mi?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

IV.BÖLÜM: VERİ İHLALİ

28. 1-Veri İhlali Hakkında Bilginiz Var Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

29. 2-Şirketinizde Veri İhlali Yaşandı Mı?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

30. 3-Sizce Veri İhlalleri Aşağıdakilerden Hangileri Kaynaklı Olabilir? (Birden Fazla Seçeneği İşaretleyebilirsiniz)

Uygun olanların tümünü işaretleyin.

	Personelden Kaynaklanan İhlal	Teknik Güvenlik Açıklarından Kaynaklanan İhlal	Zararlı Yazılımdan Kaynaklanan İhlal	Fiziki Ortamda Saklanan Bilgilerin Çalınması	Tedarikçi, Müşteri Bilgi Güvenliği Tedbirlerinin Eksik Olmasından Kaynaklanan İhlal	Verileri Korumaya Yönelik Politikaların Bulunmaması
1. Satır	☐	☐	☐	☐	☐	☐

31. 4-Şirketinizde Veri İhlali Durumunda İzlenecek Süreçler ve Olaya Müdahale Yazılı Eylem Planı Oluşturulmuş Mudur?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

32. 5-Şirketinizde Bilgi Güvenliği (Veri) İhlali Yaşanır İse Bu Olayın Şirketinize Etkisi Aşağıdakilerden Hangisi Olabilir? (Birden Fazla Seçeneği İşaretleyebilirsiniz)

Uygun olanların tümünü işaretleyin.

	Şirketin itibarını olumsuz etkilemez, fakat bilgi güvenliği organizasyon yapısını etkiler yada personel değişikliği yapılır	Şirketin itibarı olumsuz etkilenir	Şirkete bir etkisi olmaz, şirket mevcut organizasyonunu ve itibarını devam ettirir	Şirkete idari para cezası, hukuki tazminat ve ceza yükümlülüğü getirebilir	Fikrim yok
1. Satır	☐	☐	☐	☐	☐

33. 6-Personel Kaynaklı Veri İhlalleri İçin Uygulanacak Disiplin Süreci Belirlenmiş Midir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim yok

34. 7-Olası Veri İhlallerinin Zamanında Tespit Edilebilmesine Yönelik Prosedürler Hazırlanmış Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

35. 8-Veri Sızıntısında (İhlalinde) Sorumluluğu Olan, Şirket Bilgi Güvenliği Prosedürlerine Uymayan Tedarikçi, İş Ortakları, Destek Hizmeti Veren vb. lere Uygulanacak Yazılı Politikalar Bulunmakta Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

V.BÖLÜM: BİLGİ GÜVENLİĞİNE İLİŞKİN TEDBİR VE YÜKÜMLÜLÜKLER

36. 1-Şirket Verilerinin Korunmasından Yasal Olarak Sorumlu Olduğunuzu Düşünüyor Musunuz?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim yok

37. 2-Şirket Verilerinin Korunması İçin Aşağıdaki Önlemlerden Hangileri Alınmaktadır? (Birden Fazla Seçeneği İşaretleyebilirsiniz)

Uygun olanların tümünü işaretleyin.

	Teknik Önlemler	Hukuki Önlemler	Bilgi Güvenliği Konusunda Personele Eğitim Verilmesi	İdari Önlemler	Bu Önlemler İle Bilgi Güvenliği Sağlanamaz	Önlem Alınmasına Gerek Yoktur	Fikrim Yok
1. Satır	☐	☐	☐	☐	☐	☐	☐

38. 3-Şirketiniz, Verilerin Korunması İçin Gerekli ve Yeterli Teknik Donanıma Sahip Midir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

39. 4-Cevabınız Evet İse, Teknik Donanımın Yedekleme, Bakım, Güncellemeleri ve Gerekli Güvenlik Testleri Düzenli Olarak Yapılmakta Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

40. 5-Verilerin Muhafaza Edildiği "Fiziki Ortamların" (Kasa, Kilitli Dolap, Sunucu, Sistem Odaları vb) Güvenliğinden Sorumlu Kişiler Belirlenmiş Midir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

41. 6-Kişisel ve Tüzel Kişi Verilerinin Kaydedildiği "Bilgisayarlara" Erişebilecek Sorumlu Kişiler Belirlenerek, Yetkilendirme Prosedürleri Hazırlanmış Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

42. 7-Verilerin Muhafaza Edildiği "Fiziki Ortamların" Hırsızlık, Sel, Yangın, Deprem vb. Olaylarına Karşı Korunma Önlemleri Alınmış Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

43. 8-Şirketinizde Kayıtlı "Tüzel Kişi Verileri" İle İlgili Hangi Yasal Düzenlemeler Gereğince Sorumlu Olduğunuzu Düşünüyorsunuz? (Birden Fazla Seçeneği İşaretleyebilirsiniz)

Uygun olanların tümünü işaretleyin.

	Kişisel Verileri Koruma Kanunu	Türk Ceza Kanunu	Sorumlu Olduğumu Düşünmüyorum	Avrupa Genel Veri Koruma Tüzüğü (GDPR)	Türk Ticaret Kanunu	Fikrim Yok
1. Satır	☐	☐	☐	☐	☐	☐

44. 9-Kişisel ve Tüzel Kişi Verilerinin Muhafaza Edildiği "Fiziki Ortamlara" Erişebilecek Sorumlu Kişiler Belirlenmiş Midir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim yok

45. 10-Bilgi Güvenliğinin Sağlanması Konusunda Şirket Üst Yönetimi Destek Olmakta Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

46. 11-Şirketinizde Yurt Dışı İle İşlem Yapılıyor İse, Yurt Dışına Kişisel Veri Aktarımı Konusunda Yazılı Düzenlemeler Yapılmış Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

47. 12-Veri Paylaşımında Bulunduğunuz Tedarikçi, İş Ortakları, Hizmet Alınan Firmalar vb.lerinin, ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesine Sahip Olması Şirketiniz İçin Önemli Midir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

48. 13-"Kişisel Verilerin İhlal Edilmesi" Halinde Aşağıda Sayılanlardan Hangileri Yapılmalıdır? (Birden Fazla Seçeneği İşaretleyebilirsiniz)

Uygun olanların tümünü işaretleyin.

	Kişisel Verileri Koruma Kurumuna Bildirimde Bulunma	Bildirim Yapılmasına Gerek Yoktur	Şirket Üst Yönetimine Haber Verme	Gazetelere Bildirme	Fikrim Yok
1. Satır	☐	☐	☐	☐	☐

49. 14-"Şirket Çalışanlarınız İle" Aranızdaki Sözleşmelerde, Bilgi Güvenliği, Gizlilik Ve Sır Saklama Yükümlülüğüne İlişkin Hükümlere Yer Verilmiş Midir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim yok

50. 15-"Tedarikçi ve İş Ortaklarınız İle" Aranızda ki Sözleşmelerde Bilgi Güvenliği, Gizlilik ve Sır Saklama Yükümlülüğüne İlişkin Hükümlere Yer Verilmiş Midir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim yok

51. 16-Verilere Erişim Yetkisi Bulunan Personelin Görev Değişikliği Yada İşten Ayrılması Halinde, Verilere Erişim Yetkileri İvedi Olarak Sonlandırılmakta Mıdır?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim yok

52. 17-Bilgi Güvenliği Konusunda Dışarıdan Teknik Destek Hizmeti (Bakım, Proje vs) Alıyor Musunuz?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

53. 18-Şirketiniz, Verilerin Korunması Konusunda İdari Ve Hukuki Düzenlemelere Sahip Midir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

54. 19-Bilgi Güvenliğini Sağlamaya İlişkin Politika Ve Prosedürlerin Şirket İçinde Tam Olarak Uygulandığı Denetlenmekte Midir?

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

Ek:2: Etik Kurul Kararı

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" ile bildirilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

ÖZGEÇMİŞ

Ayşe İLAGA ÇAKIR

Eğitim

Doktora	2024	Maltepe Üniversitesi, Lisansüstü Eğitim Enstitüsü, Uluslararası Ticaret ve Lojistik Anabilim Dalı, Lojistik ve Tedarik Zinciri Yönetimi
Yüksek Lisans	2005	Ahmet Yesevi Uluslararası Türk-Kazak Üniversitesi, Ekonomi Fakültesi, İşletme Bölümü, İşletme Yüksek Lisans
Lisans	1993	İstanbul Üniversitesi, Hukuk Fakültesi

İş/İstihdam (Varsa)

2006-	İlaga Hukuk Bürosu – Avukat
2010-2011	İstanbul Üniversitesi, Mühendislik Fakültesi, Deniz Ulaştırma İşletme Mühendisliği - Öğretim Görevlisi (Ek Dersli)
2001-2005	Akbank Hukuk Müşavirliği - Avukat, Hukuk dersi eğitmeni
1995-2001	Alara Hukuk Bürosu - Avukat
1993-1994	Gezmişoğlu Hukuk Bürosu - Stajyer Avukat

Mesleki Birlik/Dernek Üyelikleri (Varsa)

2023-	Exemplar Global - ISO/IEC 27001 Başdenetçi
2018-	LODER Lojistik Derneği - Üye-Disiplin Kurulu Üyesi
2022-	İstanbul Barosu Taşıma Hukuku ve Lojistik Komisyonu - Üye
2022-	İstanbul Barosu Bilişim Hukuku Komisyonu - Üye

Yayınlar ve Diğer Bilimsel/Sanatsal Faaliyetler

Uluslararası bilimsel toplantılarda sunulan ve bildiri/özet bildiri kitabında (Proceedings) basılan bildiriler

İlaga Çakır, A., 'The Effects Of The Personal Data Protection Law On Human Resources Applications Of Logistics Companies' 17th International Logistics and Supply Chain Congress,

Beykoz University, Loder and Jacobs University, İstanbul, October 17-18 2019, Beykoz Akademi Dergisi, 2019; Özel Sayı 172-187.

Ulusal bilimsel toplantılarda sunulan ve bildiri/özet bildiri kitabında basılan bildiriler

İlaga Çakır, A., 'Karayolu Yük Taşımacılığında Güveni Kötüye Kullanma ve Hırsızlık' Niğde Ömer Halisdemir Üniversitesi 8. Ulusal Lojistik ve Tedarik Zinciri Kongresi Bildiriler Kitabı, 25-27 Nisan 2019, 220-232

İlaga Çakır, A., 'Covid-19 Pandemi Sürecinde Tedarik Zincirlerinde Siber Güvenlik Sorunları' Kahramanmaraş Sütçü İmam Üniversitesi Türkoğlu Meslek Yüksekokulu 10.Ulusal Lojistik ve Tedarik Zinciri Kongresi Bildiriler Kitabı, 24-25 Haziran 2021, 42

Diğer Faaliyetler

Lojistikte Dijitalleşme ve Siber Güvenlik Semineri, ''Lojistik İşletmelerde Bilgi Güvenliği'' sunumu, İstanbul Barosu Lojistik ve Taşıma Hukuku Komisyonu- LODER ve Galatasaray Üniversitesi İşbirliği, 15 Aralık 2021, İstanbul