

Do. Dr. Pelin KARAASLAN & Do. Dr. Reřit KARAASLAN

řİRKETLERDE SİBER DAYANIKLILIK

Uyum, Sözleşmeler ve Sorumluluk

7545 Sayılı Siber Güvenlik Kanunu, NIS2, CRA ve DORA



FİLİZ KİTABEVİ
İSTANBUL
2026



Filiz Kitabevi Basım Yayın Dağıtım
Petrol Ürünleri San. ve Tic. Ltd. Şti.
Genel Yayın No | General Publication Number: 1374
Sertifika no | Certificate Number: 77398

Filiz Kitabevi
Yayın No | Publication Number: 2026/124

Kitap Adı: Şirketlerde Siber Dayanıklılık Uyum, Sözleşmeler ve Sorumluluk
7545 Sayılı Siber Güvenlik Kanunu, NIS2, CRA ve DORA
Book Title: Cyber Resilience in Companies: Compliance, Contracts and Liability –
Cybersecurity Law No. 7545, NIS2, CRA and DORA
ISBN: 978-625-5007-00-1
DOI: doi.org/10.64161/filiz.9786255007001

Yazar(lar) | Author(s): Doç. Dr. Pelin KARAASLAN | orcid.org/0000-0001-5695-192X
Kurum | Institution: Eskişehir Osmangazi Üniversitesi Hukuk Fakültesi,
Fikri Mülkiyet Hukuku Anabilim Dalı
Doç. Dr. Reşit KARAASLAN | orcid.org/0000-0003-2931-4284
Kurum | Institution: Anadolu Üniversitesi Hukuk Fakültesi,
Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı

Konu Kategorisi | Subject Categories: Ticaret Hukuku, Bilişim ve Teknoloji Hukuku,
Siber Güvenlik Hukuku | Commercial Law,
Information Technology Law, Cybersecurity Law

Yayın Türü | Publication Type: Kitap | Book - Monograph
Yayın Dili | Language: Türkçe | Turkish
Ebat | Dimensions: 16 x 23 cm
Baskı Sayısı | Edition: 1
Sayfa Sayısı | Pages: 404

Yayın Tarihi | Publication Date: Eylül 2026 | September 2026
Yayın Yeri | Place of Publication: İstanbul, Türkiye
Mizanpaj | Layout: Vildan YAVUZ
Baskı ve Cilt | Printing and Binding: Filiz Kitabevi Basım Yayın Dağıtım
Petrol Ürünleri San. ve Tic. Ltd. Şti.
(Sertifika no: 77398)

© All rights reserved | Filiz Kitabevi Basım Yayın Dağıtım Petrol Ürünleri
San. ve Tic. Ltd. Şti.



Filiz Kitabevi Basım Yayın Dağıtım
Petrol Ürünleri San. ve Tic. Ltd. Şti.
Mollahüsrev Mah. Cemalyener Tosyalı Cad. No: 57A
Vefa-Fatih / İstanbul • Tel: +90 (212) 527 07 18
www.filizkitabevi.com • bilgi@filizkitabevi.com

YAZARLAR HAKKINDA

Doç. Dr. Pelin Karaaslan

Doç. Dr. Pelin Karaaslan, lisans eğitimini Ankara Üniversitesi Hukuk Fakültesinde, yüksek lisans ve doktora eğitimini ise devlet bursuyla Köln Üniversitesi Hukuk Fakültesinde tamamlamıştır. Karaaslan, fikrî ve sınai haklar alanında hazırladığı doktora tezini Almanca olarak kaleme almış; çalışma, Almanya'nın köklü hukuk yayınevlerinden Carl Heymanns Verlag tarafından *Verwechslungsschutz von Serienmarken nach dem deutschen Markengesetz* adıyla yayımlanmıştır.

Karaaslan, Türkiye'ye dönüşünün ardından devlet bursundan doğan hizmet yükümlülüğü kapsamında İstanbul Üniversitesi, Anadolu Üniversitesi ve Eskişehir Osmangazi Üniversitesinde görev yapmıştır. Karaaslan, hâlen Eskişehir Osmangazi Üniversitesi Hukuk Fakültesinde öğretim üyesi ve Fikrî Mülkiyet Hukuku Anabilim Dalı Başkanı'dır.

Akademik çalışmalarını avukatlık ile patent ve marka vekilliği faaliyetleriyle birlikte sürdüren Karaaslan'ın *Dolaylı Patent İhlali* ve *Tasarım Hukukunda Sınırlamalar* başlıklı kitaplarının yanı sıra marka, patent, tasarım, telif, reklam, teknoloji ve sözleşmeler hukuku alanlarında yayımlanmış çok sayıda çalışması bulunmaktadır.

Doç. Dr. Reşit Karaaslan

Doç. Dr. Reşit Karaaslan, lisans eğitimini Marmara Üniversitesi Hukuk Fakültesinde, yüksek lisans ve doktora eğitimini ise Köln Üniversitesi Hukuk Fakültesinde tamamlamıştır. Karaaslan, akademik çalışmalarını ceza ve ceza muhakemesi hukuku, ekonomi ceza hukuku, şirket yöneticilerinin ceza sorumluluğu ve bilişim suçları alanlarında yoğunlaştırmıştır.

Karaaslan, Türkiye'ye dönüşünün ardından devlet bursundan doğan hizmet yükümlülüğü kapsamında Atatürk Üniversitesi Hukuk Fakültesinde görev yapmış; daha sonra Anadolu Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalına geçmiştir. Karaaslan, şirket yöneticilerinin suç genel teorisi çerçevesindeki ceza sorumluluğunu konu alan çalışmasıyla doçentlik unvanını almış ve akademik çalışmalarını Eskişehir'de sürdürmüştür.

Özellikle şirketlerde uyum programları, iç soruşturmalar, yöneticilerin ceza sorumluluğu ve kurumsal ceza hukuku riskleri üzerinde çalışan ve aynı zamanda avukat/arabulucu olarak görev yapan Karaaslan'ın *Şirket Yöneticilerinin Suç Genel Teorisi Çerçevesinde Ceza Sorumlulukları* ile *Ceza Hukuku Boyutuyla Şirketlerde Uyum (Compliance)* ve *İç Soruşturma* başlıklı kitapları bulunmaktadır.

ÖNSÖZ

Şirket faaliyetlerinin giderek dijital sistemlere bağımlı hâle gelmesi, siber güvenliği yalnız bilgi işlem biriminin işi olmaktan çıkarmıştır. Bir saldırı veya yazılım hatası üretimi durdurabilir, hizmetleri aksatabilir, ticari sırların ya da kişisel verilerin açığa çıkmasına yol açabilir. Böyle bir olay bildirim yükümlülüklerini, sözleşmesel sorumluluğu, sigorta kapsamını ve yönetim organlarının gözetim görevini de gündeme getirir. Siber dayanıklılık bu nedenle şirketin bütünüyle ilgili bir hukuk ve yönetim meselesidir.

Türkiye’de 7545 sayılı Siber Güvenlik Kanunu’nun yürürlüğe girmesi, Avrupa Birliği’nde ise NIS2, Cyber Resilience Act ve DORA’nın kabul edilmesiyle şirketler bakımından yeni bir uyum alanı oluşmuştur. Bu düzenlemeler şirketlerden yalnızca güvenlik tedbiri almalarını değil, olayları ve zafiyetleri bildirmelerini, tedarikçilerini denetlemelerini, görev dağılımını belirlemelerini ve aldıkları kararları belgelendirmelerini de istemektedir.

Bu kitabı, siber dayanıklılığın şirketler bakımından ne anlama geldiğini ve yürürlükteki düzenlemelerin şirketlerden ne beklediğini açıklamak amacıyla hazırladık. Konuyu ilk kez ele alan şirket yöneticilerinin, yazılımcıların ve ürün geliştiricilerinin hukuki meseleleri anlayabilmesini; hukukçuların da teknik bir olayın hangi kurallarla bağlantılı olduğunu görebilmesini istedik. Türk hukuku ile Birlik pazarı ile bağlantısı olan şirketler bakımından Avrupa Birliği hukukundan doğabilecek yükümlülükleri şirket yönetimi, sözleşmeler, sorumluluk, sigorta ve ispat sorunlarıyla birlikte ele aldık.

Siber dayanıklılık hukuku hızla gelişen bir alandır. Türkiye’de çıkarılacak ikincil düzenlemeler ve Avrupa Birliği’ndeki uygulamalar bu alanı önümüzdeki dönemde daha da şekillendirecektir. Bu nedenle çalışmada yalnız mevcut düzenlemeleri aktarmakla yetinmeyip, uygulamada yol gösterebilecek temel ilkeleri de ortaya koymaya çalıştık. Kitabın uygulayıcılara yararlı olmasını diliyoruz.

Eskişehir, Ağustos 2026

İÇİNDEKİLER

YAZARLAR HAKKINDA.....	III
ÖNSÖZ	V
İÇİNDEKİLER.....	VII
KISALTMALAR	XIX
ÖZET.....	XXIX
ABSTRACT	XXIX
GİRİŞ	1

BİRİNCİ KISIM

SİBER DAYANIKLILIK KAVRAMI VE ETKİ ALANI

I. Kavram ve Kapsam.....	7
A. Siber Güvenlik, Bilgi Güvenliği ve Siber Dayanıklılık Ayrımı	7
B. Koruma, Sürdürme, Tespit, Müdahale ve Toparlanma Döngüsü.....	9
C. Gizlilik, Bütünlük ve Erişilebilirlik.....	10
D. İş Sürekliliği ve Operasyonel Dayanıklılık	13
E. Kurumsal Dayanıklılık, Ürün Dayanıklılığı ve Tedarik Zinciri Dayanıklılığı.....	14
F. Siber Olay, Siber Tehdit, Zafiyet ve Saldırı Kavramları	16
G. Siber Dayanıklılıkta Risk ve Ölçülülük Esası	17
H. Teknik, Kurumsal ve Hukuki Tedbirler	18
II. Siber Dayanıklılığın Etkilediği Hukuk Alanları	19
A. Siber Dayanıklılığın Kamu Hukuku Boyutu	19
B. Siber Dayanıklılığın Özel Hukuk Boyutu	20

VIII

C. Siber Dayanıklılık ve Sözleşme Hukuku.....	21
D. Siber Dayanıklılık, Şirket Yönetimi ve Yönetim Organının Sorumluluğu	22
E. Siber Dayanıklılık, Ürün Güvenliği ve Ürün Sorumluluğu	23
F. Siber Dayanıklılık ve Tedarik Zinciri Yönetimi	25
G. Siber Dayanıklılıkta Özen Borcu ve Öngörülebilir Risk.....	27
H. Basiretli Tacir Ölçütü ve Dijital Risk Yönetimi.....	29
III. Teknik Normlar ve Hukuki Etkileri.....	33
A. Teknik Standardın Hukuk Düzenindeki Yeri.....	33
B. ISO/IEC 27001 ve Bilgi Güvenliği Yönetim Sistemi	34
C. ISO/IEC 27002, 27005 ve 22301 Standartları.....	35
D. NIST Cybersecurity Framework	36
E. ENISA Rehberleri ve Bilgi ve İletişim Güvenliği Rehberi	37
F. Sertifikasyon ve Uygunluk Değerlendirmesi.....	38
G. Standartlara Uyum Taahhüdünün Sözleşmesel Etkisi.....	39
H. Teknik Standartların Denetim, İspat ve Sorumluluktaki Yeri.....	40
I. Bağlayıcı Olmayan Düzenleyici Belgelerin Özel Hukuk İlişkilerine Etkisi.....	40

İKİNCİ KISIM

AVRUPA BİRLİĞİ HUKUKUNDA SİBER DAYANIKLILIK

I. AB Siber Dayanıklılık Hukukunun Kaynakları ve Kapsamı	43
A. AB'nin Dijital Alandaki Hukuk Politikası	43
B. İç Pazar, Siber Güvenlik ve Dijital Ürün Güvenliği İlişkisi	45
C. ENISA'nın Rolü.....	46
D. Cybersecurity Act ve Sertifikasyon Çerçevesi	47
E. NIS2, CRA ve DORA'nın Düzenleme Alanları	48
F. Siber Dayanıklılığın Veri Koruma, Yapay Zekâ, Ürün Güvenliği ve Finansal Düzenleme ile Kesişimi	49
G. AB Hukukunun Türkiye'de Yerleşik Şirketlere Sözleşmesel ve Ticari Etkisi.....	51
H. AB Müşterileriyle Çalışan Şirketlerin Sözleşmesel Uyum Talepleri.....	51
II. NIS2 Direktifi: Kurumsal Siber Risk Yönetimi ve Olay Bildirimi.....	52

A. Direktifin Amacı ve NIS1'den NIS2'ye Geçiş	52
B. Direktifin Kapsamı.....	54
1. Sektör ve Büyüklük Ölçütleri.....	54
2. Temel ve Önemli Kuruluş Sıfatının Kazanılması.....	55
C. Siber Güvenlik Risk Yönetimi Tedbirleri	56
1. Tedbirlerin Ölçüsü ve Asgari İçeriği.....	56
2. Tedarik Zinciri Güvenliği.....	57
3. Dijital Sektör için Uygulama Tüzüğü.....	59
D. Yönetim Organlarının Gözetim ve Eğitim Yükümlülüğü	59
E. Olay Bildirimi Yükümlülükleri	60
F. Kayıt Yükümlülüğü, Yetkili Üye Devlet ve AB Dışı Kuruluşlar	61
G. Denetim ve Yaptırımlar	61
H. NIS2'nin Türkiye'de Yerleşik Şirketlere Etkisi ve Sözleşmelere Yansımaları.....	62
III. Cyber Resilience Act: Dijital Unsur İçeren Ürünlerde Siber Dayanıklılık	63
A. Tüzüğün Amacı ve Sistematığı	64
B. Dijital Unsur İçeren Ürün Kavramı.....	64
C. Ürün Kategorileri ve Uygunluk Değerlendirmesine Etkisi	65
D. Üreticinin Yükümlülükleri	67
1. Tasarımdan Piyasaya Arza Kadar Olan Yükümlülükler	67
2. Yaşam Döngüsü Boyunca Güvenlik, Zafiyet Yönetimi ve Destek Süresi	68
3. Teknik Dokümantasyon, Uygunluk Beyanı ve CE İşareti.....	69
E. Bildirim Yükümlülükleri	70
F. İthalatçı ve Dağıtıcıların Yükümlülükleri	72
G. Açık Kaynak Yazılımlar	73
H. Piyasa Gözetimi ve Yaptırımlar	74
I. CRA'nın Satış, Lisans ve Teknoloji Transferi Sözleşmelerine Etkisi	75
J. Türkiye'de Yerleşik Üretici, İhracatçı ve Yazılım Şirketlerinin CRA'ya Uyumu	76
IV. DORA: Finans Sektöründe Dijital Operasyonel Dayanıklılık.....	77
A. Tüzüğün Amacı ve Kapsamı	77
B. BİT Risk Yönetimi Çerçevesi ve Yönetim Organının Sorumluluğu	80

C. Olay Yönetimi, Sınıflandırma ve Bildirim	81
D. Dijital Operasyonel Dayanıklılık Testleri	84
E. BİT Üçüncü Taraf Riski ve Zorunlu Sözleşme Hükümleri	85
1. Genel Esaslar.....	85
2. DORA m. 30 Kapsamında Sözleşmenin Zorunlu İçeriği	86
F. Kritik BİT Üçüncü Taraf Hizmet Sağlayıcılarının Gözetimi.....	87
G. Yaptırımlar.....	89
H. DORA'nın Türkiye'de Yerleşik Teknoloji Şirketlerine Etkisi ve Sözleşme Müzakereleri	89
V. AB Siber Dayanıklılık Hukukunun Diğer Düzenlemelerle İlişkisi	90
A. Genel Veri Koruma Tüzüğü ve Veri Güvenliği	90
B. Yapay Zekâ Tüzüğü ve Yüksek Riskli Yapay Zekâ Sistemlerinde Siber Güvenlik.....	91
C. Veri Tüzüğü ve Güvenli Veri Paylaşımı	94
D. Ürün Sorumluluğu Direktifi ve Siber Zafiyet Kaynaklı Sorumluluk	95
E. Dijital Hizmetler Tüzüğü ve Platform Güvenliği	97
F. Bağlantılı Fiziksel Ürünlerde Makine Tüzüğü ve Telsiz Ekipmanları Direktifi.....	97
G. Siber Dayanışma Tüzüğü ve Birlik Düzeyinde Olaya Müdahale	99
H. Birden Çok Düzenlemeye Uyum ve Eşgüdüm İhtiyacı	99

ÜÇÜNCÜ KISIM

TÜRK HUKUKUNDA SİBER DAYANIKLILIK

I. 7545 Sayılı Siber Güvenlik Kanunu.....	101
A. Kanunun Amacı, Kapsamı ve Sistematiği	101
B. Temel Kavramlar: Kritik Altyapı ve Kritik Kamu Hizmeti	103
C. Kanunun Dayandığı İlkeler	104
D. Siber Güvenlik Başkanlığı	105
1. Kurumsal Yapı	105
2. Görevler ve Yetkiler.....	106
E. Siber Güvenlik Kurulu	108
F. Şirketlerin Yükümlülükleri.....	108

G. Denetim Yetkisi ve Usulü	110
H. Siber Güvenlik Şirketlerine İlişkin Hükümler	111
I. Yaptırım Hükümleri	112
J. İkincil Mevzuat Süreci ve Şirketlerin Hukuka Uyum Çalışmalarına Etkisi	114
K. 7590 Sayılı Kanunla Yapılan Değişiklikler ve Devralınan Yetkiler	116
L. İdari İşlemlere Karşı Başvuru Yolları ve Temel Hak Güvenceleri.....	121
II. Ulusal Siber Güvenlik Stratejisi ve Kritik Altyapılar	124
A. Strateji Belgelerinin Gelişimi ve 2024-2028 Stratejisi.....	125
B. Strateji Belgelerinin Hukuki Niteliği	126
C. USOM ve SOME Yapısı	127
D. Kritik Altyapıların Korunması ve Kamu-Özel İş Birliği.....	128
III. Türk Hukukunda Sektörel Siber Dayanıklılık Düzenlemeleri	129
A. Genel Siber Güvenlik Mevzuatı ile Sektörel Düzenlemelerin İlişkisi	130
B. Finans Sektörü.....	130
1. Bankacılık	130
2. Ödeme Kuruluşları ve Sermaye Piyasası	131
a. Ödeme ve Elektronik Para Kuruluşları	131
b. Sermaye Piyasası Kuruluşları ve Halka Açık Ortaklıklar	132
C. Elektronik Haberleşme ve Enerji	137
D. Sağlık, Sigortacılık ve Nükleer Enerji	138
E. Kamu İhaleleri, Savunma ve Ar-Ge Faaliyetleri	140
IV. Kişisel Veri Güvenliği ile Siber Dayanıklılık Arasındaki İlişki ve Sınırlar	140
A. Siber Dayanıklılığın Kişisel Veri Güvenliğini Aşan Kapsamı	141
B. Veri Güvenliği Yükümlülüğü (KVKK m. 12)	142
C. Veri İhlali Bildirimi ile Siber Olay Bildirimi Arasındaki Ayrım	143
D. Veri İşleyenle Yapılan Sözleşmeler, Bulut Hizmetleri ve Yurt Dışı Veri Aktarımı	145
E. KVKK Uyum Çalışmalarının Siber Dayanıklılığa Katkısı ve Sınırları	146

DÖRDÜNCÜ KISIM

ŞİRKETLERDE SİBER DAYANIKLILIĞIN YÖNETİMİ VE HUKUKA UYUM

I. Yönetim Organlarının Siber Dayanıklılık Sorumluluğu	147
A. Yönetim Kurulunun Gözetim Yükümlülüğünün Hukuki Temeli	148
B. Sorumluluğun Şartları ve İleri Sürülmesi	150
C. Görev Dağılımı, Üç Hat Modeli ve COSO İç Kontrol Çerçevesi	152
D. Siber Olay Sonrası Sorumluluk ve Özenin Belgelenmesi	155
II. Siber Dayanıklılık Alanında Hukuka Uyum Sisteminin Kurulması	156
A. Hukuka Uyumun Amacı, Uyum Yükümlülüğü ve Uyum Yönetim Sistemi	156
B. Kapsamın Belirlenmesi: Faaliyet Yapısı ve Mevzuatla Bağlantılar	159
C. Varlık, Süreç, Tedarikçi ve Sözleşme Envanterleri	160
D. Risk Değerlendirmesi ve Eksikliklerin Belirlenmesi	161
E. Politikaların Uygulanması, İzlenmesi ve Denetimi	162
III. Şirket İç Politikalar ve Uygulama Usulleri	164
A. Politikaların Amacı ve Hazırlanması	164
B. Temel Politikalar: Bilgi Güvenliği ve Siber Dayanıklılık Politikaları	165
C. Erişim, Yetkilendirme ve Kimlik Doğrulama	166
D. Uygulama Usulleri: Zafiyet, Güncelleme, Yedekleme, Kayıt ve Olay Yönetimi	168
E. Güvenli Yazılım Geliştirme, Tedarikçiler, Eğitim ve İç Denetim	169
F. Kurum İç Bildirim, Değerlendirme Süreci ve Bildirenin Korunması	170
IV. Siber Olay ve Kriz Yönetimi	172
A. Tespit, Sınıflandırma ve İlk Müdahale	172
B. Delil Koruma, Hukuk Biriminin Rolü ve Şirket İç Soruşturma	173
C. Yetkili Makamlara, Sözleşme Taraflarına ve Diğer İlgililere Bildirim	178
D. Müşterilerin Bilgilendirilmesi, Kamuoyu Açıklamaları ve İtibar Yönetimi	179
E. Kök Nedenin Belirlenmesi, İyileştirme ve Olay Dosyası	180
V. Tedarikçilerden ve Diğer Üçüncü Kişilerden Kaynaklanan Siber Riskler	181
A. Tedarikçilerin Sınıflandırılması ve Seçim Öncesi İnceleme	181
B. Riskli Hizmet Türleri: Uzaktan Erişim, Bakım, Bulut ve Yazılım	183

C. Denetim, Sözleşmesel Yaptırımlar ve Sözleşmenin Sona Ermesi.....	183
D. Tedarikçi Kaynaklı Olaylar ve Rücu.....	184

BEŞİNCİ KISIM

SÖZLEŞMELERDE SİBER DAYANIKLILIK

I. Siber Dayanıklılığın Sözleşmelere Yansıması	185
A. Güvenlik Hükümlerinin Sözleşmedeki Yeri ve Temel Kavramlar	185
B. Taahhütlerin Yapısı: Standartlar, Tedbirler ve Hizmet Seviyeleri	187
C. Sözleşme Süresince Devam Eden Yükümlülükler: Zafiyet, Güncelleme ve Olay Bildirimi.....	188
D. Denetim, Alt Yükleniciler ve Sözleşmenin Güvenli Biçimde Sona Ermesi	189
E. Risk Dağıtımı: Sorumluluk Sınırları, Mücbir Sebep ve Tazminat	189
1. Sözleşmesel Sorumluluk Sınırlamalarının Kapsamı ve Geçerliliği.....	190
2. Mücbir Sebep ve Siber Saldırı.....	191
3. Tazminat, Rücu ve Zararın Azaltılması.....	192
II. Yazılım Lisans Sözleşmelerinde Siber Dayanıklılık.....	193
A. Lisans İlişkisinde Güvenlik Beklentisinin Hukuki Temeli	193
B. Açık Kaynak Bileşenleri, SBOM ve Kod İncelemesinin Sınırları	194
C. Yaşam Döngüsü Hükümleri: Güncelleme, Destek Süresi ve Kritik Zafiyet	196
D. Lisans Alanın Yükümlülükleri, Kaynak Kodun Tevdii ve Sorumluluk	197
III. Bulut, SaaS ve Dışarıdan Hizmet Alımı Sözleşmeleri	198
A. Bulut Hizmetinin Hukuki Niteliği ve Edimlerin Dağılımı	198
B. Süreklilik ve Güvenlik Taahhütleri	200
C. Bilgilendirme, Alt Sağlayıcılar ve Denetim	200
D. Verilerin Taşınması, Hizmetin Sona Ermesi ve Uyuşmazlıklar	201
IV. Teknoloji Transferi ve Ar-Ge Sözleşmelerinde Siber Dayanıklılık	202
A. Korunan Bilginin Hukuki Niteliği ve Siber Riskler	203
B. Bilginin Paylaşılmasında Alınacak Tedbirler.....	204
C. Aktarımdan Sonra Devam Eden Yükümlülükler ve CRA ile İlişki	205
D. Sözleşmeye Aykırılığın Sonuçları ve Siber Dayanıklılık Eki	205
V. Dijital Ürün Satışı, Tedarik ve Dağıtım Sözleşmeleri	206

XIV

A. Ürün Güvenliği Hükümleri ile Sözleşmenin Birlikte Uygulanması.....	207
B. Güncellemelerin Müşteriye Ulaştırılması ve Destek Süresi	207
C. Zafiyet, Ayıp ve Geri Çağırma.....	208
D. Ticari İşlemler ile Tüketici İşlemlerinde Sorumluluk	208
VI. Bakım, Destek, Yönetilen Hizmet ve Uzaktan Erişim Sözleşmeleri.....	209
A. Bakım ve Yönetilen Hizmet Sözleşmelerine Özgü Riskler	209
B. Uzaktan Erişim: Yetkilendirme, Kayıt ve Kimlik Doğrulama	209
C. Sağlayıcının Güvenlik Yükümlülükleri ve Sağlayıcı Kaynaklı Olaylar.....	210
D. Sözleşmenin Sona Ermesi: Erişimlerin Kapatılması ve Devir	211
VII. Şirket Birleşmeleri, Devralmalar ve Yatırım İşlemlerinde Siber Durum Tespiti	211
A. Kavram ve Kapsam.....	211
B. İnceleme Sonuçlarının Bedele, Beyanlara ve Kapanış Koşullarına Etkisi	212
C. 7545 Sayılı Kanun Uyarınca Bildirim ve Onay	213
D. Satıcının Hazırlığı ve Veri Odası Güvenliği	213

ALTINCI KISIM

SİBER OLAYLARDA SORUMLULUK, YAPTIRIM, SİGORTA VE UYUŞMAZLIK ÇÖZÜMÜ

I. Siber Olaylardan Doğan Özel Hukuk Sorumluluğu	215
A. Sorumluluk Kaynakları.....	215
B. Kusur Ölçüsü, Öngörülebilirlik ve Zafiyetin Ayıp Niteliği.....	219
C. Zarar Kalemleri, Müteselsil Sorumluluk ve Rücu.....	221
D. Sorumluluk Sınırlamalarının Geçerliliği ve İspat Sorunları.....	224
E. Kişisel Veri İhlalinden Doğan Sorumluluk	224
II. İdari Yaptırımlar ve Ceza Hukuku.....	227
A. İdari Yaptırımların Hukuki Çerçevesi.....	227
B. 7545 Sayılı Kanun'un Suç Tipleri.....	228
C. Çalışan Kaynaklı Gizlilik İhlalleri ve Haksız Rekabet.....	230
D. İdari ve Cezai Süreçlerde Şirketin Savunması	231
III. Siber Sigorta Yoluyla Riskin Devri	232

A. Siber Sigortanın İşlevi ve Teminatın Kapsamı	232
B. Savaş, Devlet Destekli Saldırı ve Fidyeye Ödemesi	237
C. Sözleşmeden Doğan Külfetler: Beyan, Bildirim ve Güvenlik Şartları	238
D. Sigorta ile Güvenlik ve Uyum Tedbirleri Arasındaki İlişki	242
IV. Siber Uyuşmazlıklarda Deliller, İspat ve Alternatif Çözüm Yolları	243
A. Dijital Kayıtların Delil Değeri	243
B. Olay Sonrasında Delillerin Korunması ve Uzman Raporları	246
C. Kusur ve Nedenselliğin İspatı	248
D. Tahkim ve Arbuluculuk	249

YEDİNCİ KISIM

AVRUPA BİRLİĞİ İLE TİCARİ İLİŞKİ İÇİNDEKİ TÜRKİYE'DE YERLEŞİK ŞİRKETLERİN UYUMU

I. AB Siber Dayanıklılık Mevzuatının Türkiye'de Yerleşik Şirketlere Uygulanması	251
A. Hukuki Bağlantının Belirlenmesi	251
B. Hukuki Bağlantı Hâlleri	252
C. Uyum Çalışmalarında Önceliğin Belirlenmesi	254
II. Faaliyet Alanlarına Göre Uyum	254
A. Teknoloji Sağlayıcıları: Yazılım, SaaS, Bulut ve Veri Merkezi Hizmetleri	255
B. Ürün Üreticileri: IoT, Otomotiv, Makine ve Savunma	255
C. Hizmet Sektörleri: Finansal Teknolojiler, Sağlık, Elektronik Ticaret, Enerji ve Lojistik	256
D. Üniversiteler, Teknoparklar, Ar-Ge Kuruluşları ve KOBİ'lerde Riskle Orantılı Uyum Çalışmaları	257
III. Uyum Çalışmasının Planlanması ve Sürdürülmesi	258
A. Hazırlık ve İnceleme	258
B. Tedbirlerin Uygulanması	259
C. Uygulamanın Doğrulanması ve Uyumun Sürdürülmesi	259

SEKİZİNCİ KISIM
KONTROL LİSTELERİ, ÖRNEK SÖZLEŞME HÜKÜMLERİ VE
KURUMSAL BELGELER

I. Kontrol Listeleri.....	261
A. Yönetim Kurulu için Siber Dayanıklılık Kontrol Listesi	262
B. Hukuk ve Uyum Birimi için Kontrol Listesi	263
C. Bilgi İşlem Birimi için Hukuki Uyum Kontrol Listesi.....	264
D. Tedarikçi Seçimi ve Kritik Tedarikçilerin İncelenmesi	265
E. Sözleşme Türlerine Göre Kontrol Listeleri	266
F. Siber Olay Sonrasında Yapılacak Hukuki İşlemler	268
G. VII-128.10 Sayılı Tebliğ Kapsamındaki Kuruluşlara Yönelik Kontrol Listesi.....	269
H. Kurum İçi Bildirim ve Şirket İçi Soruşturma Kontrol Listesi	277
II. Örnek Sözleşme Hükümleri.....	279
A. Tanımlar ve Standartlara Uyum	280
1. Tanımlar	280
2. Standart ve Sertifika	281
B. Tedbirler, Zafiyet Yönetimi ve Güncellemeler	281
1. Teknik ve İdari Tedbirler	281
2. Zafiyet Yönetimi	282
3. Güncelleme ve Destek Süresi.....	282
C. Olay Bildirimi, Denetim ve Alt Yükleniciler	283
1. Olay ve Tehdit Bildirimi	283
2. Denetim Hakkı	284
3. Alt Yükleniciler.....	285
D. Üçüncü Taraf Bileşenleri, İş Sürekliliği ve Sigorta	286
1. Üçüncü Taraf Bileşenleri ve SBOM.....	286
2. Yedekleme ve İş Sürekliliği	286
3. Siber Sigorta.....	287
E. Sorumluluğun Dağılımı ve Sözleşmenin Sona Ermesi.....	288
1. Sorumluluk ve Tazminat	288

2. Mücbir Sebep ve Risk Dağıtımı	288
3. Sözleşmenin Sona Ermesinde Güvenlik	289
4. Mevzuat Değişikliği	290
5. AB Mevzuatıyla Bağlantılı Sözleşme Hükümleri	290
III. Kurumsal Belgelerin İçeriği	292
SONUÇ	299
EKLER	303
Ek 1: NIS2 Kapsamının İncelenmesi	304
Ek 2: CRA Kapsamı ve Ürün Sınıflandırması	306
Ek 3: Hizmet Sağlayıcısının DORA Kapsamındaki Durumu	309
Ek 4: 7545 Sayılı Kanun Bakımından Kapsam İncelemesi	311
Ek 5: Türkiye’de Yerleşik Şirketler için İlk Doksan Güne İlişkin Örnek Çalışma Takvimi	313
Ek 6: Tedarikçilerin Siber Risklerinin İncelenmesi	315
Ek 7: Siber Olaya Müdahale Süreci	317
Ek 8: Sözleşmelerin Gözden Geçirilmesi	319
Ek 9: Yönetim Kuruluna Sunulacak Siber Dayanıklılık Raporunun İçeriği	320
Ek 10: Siber Dayanıklılık Terimleri Sözlüğü	321
Ek 11: Kurum İçi Bildirim ve İlk Değerlendirme Formu	332
Ek 12: Şirket İçi Soruşturmanın Planlanması, Yürütülmesi ve Raporlanması	334
Ek 13: Çakışan Yükümlülüklerin İncelenmesi	337
KAYNAKÇA	347
KARAR DİZİNİ	363
MEVZUAT LİSTESİ	367

KISALTMALAR

A.Ş.	: Anonim şirket
AB	: Avrupa Birliği
ABA	: Avrupa Birliği Antlaşması
ABAD	: Avrupa Birliği Adalet Divanı
ABD	: Amerika Birleşik Devletleri
ABİHA	: Avrupa Birliği'nin İşleyişi Hakkında Antlaşma
ACSC	: Australian Cyber Security Centre (Avustralya Siber Güvenlik Merkezi)
AET	: Avrupa Ekonomik Topluluğu
AFAD	: Afet ve Acil Durum Yönetimi Başkanlığı
AG	: Aktiengesellschaft (Alman anonim şirketi)
AI Act	: (AB) 2024/1689 sayılı Yapay Zekâ Tüzüğü
AİHM	: Avrupa İnsan Hakları Mahkemesi
Ar-Ge	: Araştırma ve Geliştirme
Art.	: Artikel/Article (madde)
ASD	: Australian Signals Directorate (Avustralya Sinyal Müdürlüğü)
AT	: Avrupa Topluluğu
AvK	: 1136 sayılı Avukatlık Kanunu
AY	: 2709 sayılı Türkiye Cumhuriyeti Anayasası

XX

AYM	: Anayasa Mahkemesi
B. No.	: Bireysel Başvuru Numarası
B2C	: Business-to-Consumer (işletmeden tüketiciye)
BBSY	: Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik
BDDK	: Bankacılık Düzenleme ve Denetleme Kurumu
BGH	: Bundesgerichtshof (Alman Federal Mahkemesi)
BGHZ	: Entscheidungen des Bundesgerichtshofes in Zivilsachen
BİT	: Bilgi ve İletişim Teknolojileri (ICT)
BKR	: Zeitschrift für Bank- und Kapitalmarktrecht
bkz.	: bakınız
BSIG	: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (Alman Bilgi Teknolojileri Güvenliği Kanunu)
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
C.	: Cilt
CCZ	: Corporate Compliance Zeitschrift
CE	: Conformité Européenne (AB uygunluk işareti)
CEN	: Avrupa Standardizasyon Komitesi
CENELEC	: Avrupa Elektroteknik Standardizasyon Komitesi
CEO	: Chief Executive Officer (icra kurulu başkanı)
CER	: (AB) 2022/2557 sayılı Kritik Kuruluşların Dayanıklılığı Direktifi
CGL	: Commercial General Liability (ticari genel sorumluluk sigortası)
CIA	: Confidentiality, Integrity, Availability (gizlilik, bütünlük, erişilebilirlik)
CISA	: ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı

CMK	: 5271 sayılı Ceza Muhakemesi Kanunu
CMS	: Compliance Management System (uyum yönetim sistemi)
Co.	: Company (şirket)
COBIT	: Control Objectives for Information and Related Technologies
COM	: Avrupa Komisyonu belge dizisi/numarası
COSO	: Committee of Sponsoring Organizations of the Treadway Commission
CRA	: Cyber Resilience Act; (AB) 2024/2847 sayılı Siber Dayanıklılık Tüzüğü
C-SCRM	: Cybersecurity Supply Chain Risk Management (Siber Güvenlik Tedarik Zinciri Risk Yönetimi)
CSF	: NIST Cybersecurity Framework (Siber Güvenlik Çerçevesi)
CSIRT	: Computer Security Incident Response Team (Bilgisayar Güvenliği Olaylarına Müdahale Ekibi)
CSRB	: Cyber Safety Review Board (Siber Güvenlik İnceleme Kurulu)
CSWP	: Cybersecurity White Paper (NIST Siber Güvenlik Beyaz Kitabı)
CTPP	: Critical ICT Third-Party Service Provider (Kritik BİT Üçüncü Taraf Hizmet Sağlayıcısı)
CVD	: Coordinated Vulnerability Disclosure (Koordineli Zafiyet Açıklaması)
CVE	: Common Vulnerabilities and Exposures (Ortak Zafiyetler ve Etkilenmeler)
Cybersecurity Act	: (AB) 2019/881 sayılı Siber Güvenlik Tüzüğü
Data Act	: (AB) 2023/2854 sayılı Veri Tüzüğü
DMA	: (AB) 2022/1925 sayılı Dijital Piyasalar Tüzüğü
dn.	: dipnot
DNS	: Alan Adı Sistemi

DORA	: Digital Operational Resilience Act; (AB) 2022/2554 sayılı Dijital Operasyonel Dayanıklılık Tüzüğü
DSA	: (AB) 2022/2065 sayılı Dijital Hizmetler Tüzüğü
DS-GVO	: Datenschutz-Grundverordnung (Almanca Genel Veri Koruma Tüzüğü kısaltması)
E.	: Esas
EBA	: Avrupa Bankacılık Otoritesi
EDPB	: Avrupa Veri Koruma Kurulu
EİK	: 5070 sayılı Elektronik İmza Kanunu
EIOPA	: European Insurance and Occupational Pensions Authority (Avrupa Sigorta ve Mesleki Emeklilik Otoritesi)
EN	: European Standard (Avrupa standardı)
ENISA	: European Union Agency for Cybersecurity (Avrupa Birliği Siber Güvenlik Ajansı)
EnWZ	: Zeitschrift für das gesamte Recht der Energiewirtschaft
EPRS	: European Parliamentary Research Service (Avrupa Parlamentosu Araştırma Servisi)
ERA	: Europäische Rechtsakademie/Academy of European Law (Avrupa Hukuk Akademisi)
ESAs	: European Supervisory Authorities (Avrupa Denetim Otoriteleri)
ESG	: Zeitschrift für nachhaltige Unternehmensführung
ESGYMY	: Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği
ESMA	: European Securities and Markets Authority (Avrupa Menkul Kıymetler ve Piyasalar Otoritesi)
et al.	: et alii/aliae/alía (ve diğerleri)
ETSI	: European Telecommunications Standards Institute (Avrupa Telekomünikasyon Standartları Enstitüsü)
EU	: European Union (Avrupa Birliği)

EU-CyCLONe	: European Cyber Crises Liaison Organisation Network (Avrupa Siber Kriz İrtibat Kuruluşları Ağı)
EUCC	: European Cybersecurity Certification Scheme on Common Criteria (Avrupa Ortak Kriterler Temelli Sertifikasyon Şeması)
EUCS	: European Cybersecurity Certification Scheme for Cloud Services (Bulut Hizmetleri için Avrupa Siber Güvenlik Sertifikasyon Şeması)
EuZW	: Europäische Zeitschrift für Wirtschaftsrecht
FBI	: Federal Bureau of Investigation (ABD Federal Soruşturma Bürosu)
FIPS	: Federal Information Processing Standards (Federal Bilgi İşleme Standartları)
FSEK	: 5846 sayılı Fikir ve Sanat Eserleri Kanunu
GAO	: Government Accountability Office (ABD Sayıştay Ofisi)
GDPR	: (AB) 2016/679 sayılı Genel Veri Koruma Tüzüğü
GmbH	: Gesellschaft mit beschränkter Haftung (Alman limited şirketi)
GmbHG	: Gesetz betreffend die Gesellschaften mit beschränkter Haftung (Alman Limited Şirketler Kanunu)
GNU	: GNU's Not Unix (GNU Projesi)
GPL	: GNU Genel Kamu Lisansı
GWR	: Gesellschafts- und Wirtschaftsrecht
HGK	: Hukuk Genel Kurulu
HMK	: 6100 sayılı Hukuk Muhakemeleri Kanunu
HUAK	: 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu
IaaS	: Hizmet Olarak Altyapı
ICC	: Milletlerarası Ticaret Odası
ICO	: Information Commissioner's Office (Birleşik Krallık Veri Koruma Otoritesi)

ICT	: Information and Communications Technology (Bilgi ve İletişim Teknolojileri; bkz. BİT)
IEC	: International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)
IIA	: The Institute of Internal Auditors (İç Denetçiler Enstitüsü)
IMEI	: International Mobile Equipment Identity (Uluslararası Mobil Cihaz Kimliği)
Inc.	: Incorporated (sermaye şirketi)
IoT	: Nesnelerin İnterneti (Internet of Things)
IP	: İnternet Protokolü
ISO	: International Organization for Standardization (Uluslararası Standardizasyon Örgütü)
İSTAC	: İstanbul Tahkim Merkezi
İşK	: 4857 sayılı İş Kanunu
IT	: Information Technology (Bilgi Teknolojileri)
ITIL	: Information Technology Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi)
JIPITEC	: Journal of Intellectual Property, Information Technology and E-Commerce Law
K.	: Karar
KabK	: 5326 sayılı Kabahatler Kanunu
KI	: Künstliche Intelligenz (yapay zekâ)
KOBİ	: Küçük ve Orta Büyüklükteki İşletmeler
KVKK	: 6698 sayılı Kişisel Verilerin Korunması Kanunu
LG	: Landgericht (Alman eyalet mahkemesi)
LKV	: Landes- und Kommunalverwaltung
Ltd	: Limited Şirket

m.	: madde
MMR	: MultiMedia und Recht
MÖHUK	: 5718 sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun
MPR	: MedizinProdukteRecht
MSP	: Managed Service Provider (Yönetilen Hizmet Sağlayıcısı)
MTK	: 4686 sayılı Milletlerarası Tahkim Kanunu
MÜHF	: Marmara Üniversitesi Hukuk Fakültesi
NAO	: National Audit Office (Birleşik Krallık Ulusal Denetim Ofisi)
NDK	: Nükleer Düzenleme Kurumu
NFT	: Non-Fungible Token (değiştirilemez token)
NHS	: National Health Service (Birleşik Krallık Ulusal Sağlık Hizmeti)
NIS1	: (AB) 2016/1148 sayılı Ağ ve Bilgi Sistemleri Güvenliği Direktifi (mülga)
NIS2	: (AB) 2022/2555 sayılı Ağ ve Bilgi Güvenliği Direktifi
NIS2UmsuC G	: NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2'nin Aktarılması ve Siber Güvenliğin Güçlendirilmesi Kanunu)
NIST	: National Institute of Standards and Technology (ABD Ulusal Standartlar ve Teknoloji Enstitüsü)
NJOZ	: Neue Juristische Online-Zeitschrift
NJW	: Neue Juristische Wochenschrift
NJW- Spezial	: Neue Juristische Wochenschrift Spezial
No.	: Number/numara
NSA	: National Security Agency (ABD Ulusal Güvenlik Ajansı)
NTSGY	: Nükleer Tesislerde Siber Güvenliğe İlişkin Yönetmelik

NVwZ	: Neue Zeitschrift für Verwaltungsrecht
OECD	: Organisation for Economic Co-operation and Development (İktisadi İşbirliği ve Kalkınma Teşkilatı)
OJ	: Official Journal of the European Union (AB Resmî Gazetesi)
OLG	: Oberlandesgericht (Alman eyalet yüksek mahkemesi)
OT	: İşletim Teknolojisi (Operational Technology)
OWiG	: Gesetz über Ordnungswidrigkeiten (Alman Kabahatler Kanunu)
ÖBST	: Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ
PaaS	: Platform as a Service (Hizmet Olarak Platform)
par.	: paragraf
PE-CONS	: Avrupa Parlamentosu ve Konseyinin kabul metinlerine ait belge dizisi/kodu
PharmR	: Pharma Recht
PLD	: (AB) 2024/2853 sayılı Ürün Sorumluluğu Direktifi
r+s	: Recht und Schaden
RDİ	: Recht Digital
RED	: 2014/53/AB sayılı Telsiz Ekipmanları Direktifi
RG.	: Resmî Gazete
RPO	: Recovery Point Objective (Kurtarma Noktası Hedefi)
RTO	: Recovery Time Objective (Kurtarma Süresi Hedefi)
S.	: Sayı
s.	: sayfa
SaaS	: Software as a Service (Hizmet Olarak Yazılım)
SBOM	: Yazılım Malzeme Listesi (Software Bill of Materials)

SE	: Societas Europaea (Avrupa şirketi)
SEDDK	: Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu
SHGM	: Sivil Havacılık Genel Müdürlüğü
SiGüK	: 7545 sayılı Siber Güvenlik Kanunu
SIM	: Subscriber Identity Module (Abone Kimlik Modülü)
SLA	: Service Level Agreement (Hizmet Seviyesi Anlaşması)
SMBv1	: Server Message Block version 1 (Sunucu İleti Bloğu sürüm 1)
SMK	: 6769 sayılı Sınai Mülkiyet Kanunu
SMS	: Kısa Mesaj Servisi
SOME	: Siber Olaylara Müdahale Ekibi
SP	: Special Publication (NIST Özel Yayını)
SPK	: Sermaye Piyasası Kurulu
SSDF	: Güvenli Yazılım Geliştirme Çerçevesi (Secure Software Development Framework)
StPO	: Strafprozessordnung (Alman Ceza Muhakemesi Kanunu)
ŞBGY	: Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği
TBB	: Türkiye Barolar Birliği
TBK	: 6098 sayılı Türk Borçlar Kanunu
TCK	: 5237 sayılı Türk Ceza Kanunu
TCMB	: Türkiye Cumhuriyet Merkez Bankası
TİTCK	: Türkiye İlaç ve Tıbbi Cihaz Kurumu
TKHK	: 6502 sayılı Tüketicinin Korunması Hakkında Kanun
TL	: Türk lirası

TLD	: Üst Düzey Alan Adı (Top-Level Domain)
TLPT	: Threat-Led Penetration Testing (Tehdit Odaklı Sızma Testi)
TMK	: 4721 sayılı Türk Medeni Kanunu
TRIPS	: Agreement on Trade-Related Aspects of Intellectual Property Rights (Ticaretle Bağlantılı Fikrî Mülkiyet Hakları Anlaşması)
TS	: Türk Standardı
TSD	: (AB) 2016/943 sayılı Ticari Sırlar Direktifi
TSE	: Türk Standardları Enstitüsü
TTK	: 6102 sayılı Türk Ticaret Kanunu
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
U.S.	: United States (Amerika Birleşik Devletleri)
UNCITRAL	: United Nations Commission on International Trade Law (Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu)
USOM	: Ulusal Siber Olaylara Müdahale Merkezi
ÜGTDK	: 7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanunu
v.	: versus (karşı)
vd.	: ve devamı
VSA	: Virtual System Administrator (Kaseya'nın Uzaktan İzleme ve Yönetim Platformu)
VUK	: 213 sayılı Vergi Usul Kanunu
ZfDR	: Zeitschrift für Digitalisierung und Recht
ZRP	: Zeitschrift für Rechtspolitik

CYBER RESILIENCE IN COMPANIES

Compliance, Contracts and Liability

Cybersecurity Law No. 7545, NIS2, CRA and DORA

ÖZET

Dijital sistemlere olan bağımlılık arttıkça siber güvenlik, yalnızca şirketlerin bilgi işlem birimlerini ilgilendiren teknik bir mesele olmaktan çıkmış; idare hukukundan sözleşme hukukuna, veri korumadan ürün güvenliğine kadar uzanan bir kurallar bütünü hâline gelmiştir. Bu çalışmada şirketlerin siber dayanıklılığı; 7545 sayılı Siber Güvenlik Kanunu başta olmak üzere Türk Ticaret Kanunu, Türk Borçlar Kanunu, Kişisel Verilerin Korunması Kanunu, Fikir ve Sanat Eserleri Kanunu ve sektörel düzenlemeler ışığında incelenmiştir. Avrupa Birliği ile ticari ilişki içindeki şirketler bakımından NIS2 Direktifi, Siber Dayanıklılık Tüzüğü (CRA) ve Dijital Operasyonel Dayanıklılık Tüzüğü (DORA) ele alınmış; bu kuralların şirketlere kanun, sözleşme ve piyasa beklentisi yoluyla yansıyan etkileri incelenmiştir. Bu etkilerin uygulamada nasıl karşılanacağını göstermek üzere kontrol listelerine ve örnek sözleşme hükümlerine yer verilmiştir.

Anahtar Kelimeler: Siber dayanıklılık, 7545 sayılı Siber Güvenlik Kanunu, NIS2, CRA, DORA, hukuka uyum, siber olaydan doğan sorumluluk.

ABSTRACT

As dependence on digital systems grows, cybersecurity has ceased to be a technical matter concerning only a company's information technology department; it has become a body of rules extending from administrative law to contract law, and from data protection to product safety. This study examines the cyber resilience of companies in the light of Cybersecurity Law No. 7545, the Turkish Commercial Code, the Turkish Code of Obligations, the Personal Data Protection Law, the Law on Intellectual and Artistic Works and the relevant sectoral regulations. For companies trading with the European Union, the NIS2 Directive, the Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA) are also addressed; the effects these rules produce by statute, by contract and by market expectation are examined separately. Checklists and model contract clauses are provided to show how those effects are to be met in practice.

Keywords: Cyber resilience, Cybersecurity Law No. 7545, NIS2, CRA, DORA, legal compliance, liability for cyber incidents.