

Doç. Dr. Mehmet Bedii Kaya

SİBER GÜVENLİK HUKUKU

İÇİNDEKİLER

ÖNSÖZ	VII
KISALTMALAR.....	XXV
§1. GİRİŞ VE KONUNUN TAKDİMİ.....	1
§2. SİBER TEHDİTLER.....	13
I. Siber Tehditlerin Sınıflandırılması	13
II. Güncel Siber Tehditler.....	16
A. Oltalama saldırısı	18
B. Sosyal mühendislik.....	22
C. Kötü amaçlı yazılımlar (virüsler, solucanlar ve benzeri zararlılar)	22
D. Fidye virüsleri.....	23
E. Servis dışı bırakma saldırısı.....	32
F. Kod enjekte etme saldırısı.....	33
G. Sıfırınca gün açığı istismarı.....	34
H. Güncelleme zafiyetlerinin istismarı	34
I. Varsayılan ayar istismarı	36
J. Tedarik zinciri saldırısı.....	37
K. Şifre kırma saldırısı	39
L. Araya girme saldırısı.....	40
M. İç tehditler	41
N. Fiziksel saldırılar	41
III. Siber Tehditlerin Etkileri.....	42
§3. AVRUPA BİRLİĞİ VE SİBER GÜVENLİK	47
I. Avrupa Birliği Siber Güvenlik Stratejisi.....	47
II. Avrupa Birliği Siber Güvenlik Düzenlemeleri	51

§4. AVRUPA BİRLİĞİ ŞEBEKE VE BİLGİ GÜVENLİĞİ DİREKTİFİ (NIS DİREKTİFİ)	61
I. NIS1 Direktifi.....	61
A. Temel hizmet operatörü.....	63
B. Dijital hizmet sağlayıcı.....	65
II. NIS2 Direktifi.....	67
III. NIS2 Direktifindeki Temel Kavramlar	73
IV. Temel Yükümlülükler.....	74
V. Kurumsal Hesap Verebilirlik İlkesi.....	75
VI. Siber Olay Bildirim Yükümlüğü.....	78
VII. Sorumluluk Rejimi ve Denetim	80
VIII. Yaptırımlar.....	81
IX. NIS1 ve NIS2 Direktifi Karşılaştırması.....	82
§5. AVRUPA BİRLİĞİ SİBER DAYANIKLILIK YASASI (CRA)...85	
I. CRA'nın Temel Çerçevesi	85
II. Kapsam	86
A. Açıkça belirtilen tam istisnalar	87
B. Kısmi veya özel istisnalar.....	88
C. Ulusal güvenlik, kamu güvenliği ve savunmaya ilişkin kısıtlamalar	89
D. Özel tam istisna: Ticari amaçlı hareket etmeme unsuru.....	89
III. CRA'daki Temel Tanımlar.....	91
A. Dijital unsurlu ürün (<i>product with digital element</i>).....	92
B. Üretici (<i>manufacturer</i>)	93
C. İthalatçı (<i>importer</i>).....	93
D. Dağıtıcı (<i>distributor</i>).....	93
E. Statülerin değişmesi kuralı.....	94
IV. Dijital Unsurlu Ürün Türleri	95
A. Dijital unsurlu önemli ürünler	95
B. Dijital unsurlu kritik ürünler	97

V.	Dijital Unsurlu Ürünlerin Birlik İçerisinde Serbest Dolaşımına İlişkin Kurallar	97
VI.	CRA'nın Diğer Düzenlemelerle İlişkisi	100
	A. Ürün güvenliği kurallarıyla ilişki.....	100
	B. Yapay zekâ kurallarıyla ilişki.....	101
VII.	Üreticinin CRA Yükümlülükleri.....	101
	A. Üreticinin siber güvenlik yükümlülükleri	102
	1. CRA'nın EK 1 bölümünde yer alan gerekliliklere uygun tasarım, geliştirme ve üretim yapma yükümlülüğü.....	105
	2. Siber güvenlik risk değerlendirmesi yapma yükümlülüğü.....	105
	3. Siber güvenlik risk değerlendirmesini belgelendirme ve risk değerlendirmesini güncelleme yükümlülüğü.....	106
	4. Siber risk değerlendirmesine ilişkin şeffaflık yükümlülüğü.....	107
	5. Üçüncü taraflara ait bileşenlerin siber güvenlik uyumluluğuna dair özen gösterme yükümlülüğü...	107
	6. Güvenlik açığını bildirme yükümlülüğü	108
	7. Siber güvenlik risklerini sistematik şekilde belgelendirme yükümlülüğü.....	108
	8. Siber güvenlik açıklarını etkin şekilde yönetme yükümlülüğü.....	109
	9. Siber güvenlik için destek süresi belirleme yükümlülüğü.....	109
	10. Güvenlik açığı ifşa politikası başta olmak üzere uygun politika ve prosedürleri hazırlama yükümlülüğü.....	110
	11. Güvenlik güncellemelerini en az 10 yıl boyunca kullanılabilir kılma yükümlülüğü.....	111
	12. Yazılımların son sürümünde temel siber güvenlik gerekliliklerini sağlama yükümlülüğü	111

13. Halka açık yazılım arşivlerinde desteklenmeyen yazılım kullanımıyla ilgili riskler hakkında bilgilendirme yapma yükümlülüğü 111
 14. Teknik dokümantasyon hazırlama yükümlülüğü ... 112
 15. Seçili uygunluk değerlendirme prosedürlerini yerine getirme yükümlülüğü 112
 16. Uygunluk beyanı hazırlama yükümlülüğü 112
 17. Teknik dokümantasyonu ve AB uygunluk beyanını 10 yıl boyunca hazır tutma yükümlülüğü 113
 18. Seri üretimin parçası olan dijital unsurlu ürünlerin CRA'ya uyumlu kalması için tedbir alma yükümlülüğü 113
 19. Belirleyici kullanma yükümlülüğü..... 113
 20. Tanıtıcı bilgilerini paylaşma ve erişilebilir kılma yükümlülüğü..... 114
 21. Tek iletişim noktası belirleme ve bunu şeffaf şekilde duyurma yükümlülüğü..... 114
 22. Teknik bir dokümantasyon sağlama ve 10 yıl boyunca bu dokümantasyonu erişilebilir kılma yükümlülüğü..... 115
 23. Destek süresini belirtme yükümlülüğü..... 115
 24. AB uygunluk beyanını sunma yükümlülüğü 116
 25. CRA'ya uyumsuzlukta geri çağırma dahil derhal düzeltici eylemde bulunma yükümlülüğü 116
 26. Piyasa gözetimi ve denetimi otoritelerine ilgili bilgi ve belgeleri verme ve iş birliği yapma yükümlülüğü..... 116
 27. Faaliyetleri durdurmadan önce bunu duyurma yükümlülüğü..... 117
- B. Üreticinin Siber Güvenlik Açığını Bildirim Yükümlülüğü..... 117
1. Genel siber güvenlik açığı bildirim yükümlülüğü .. 118

2. Dijital unsurlu ürünün güvenliği üzerinde etkisi olan ciddi olayların bildirimini	119
3. Ortak hükümler.....	121
a. Yetkili makamlara bildirim	121
b. Kullanıcıları bilgilendirme	122
c. Gönüllü bildirim	123
d. Üreticinin temsilci kullanmasına ilişkin özel kurallar	124
VIII. İthalatçının CRA Yükümlülükleri.....	125
A. CRA'ya uygun dijital unsurlu ürünü piyasaya arz etme yükümlülüğü.....	127
B. Dijital unsurlu ürünü piyasaya sürmeden önce teknik kontrol yapma yükümlülüğü	127
C. CRA'ya uyuma ilişkin belgeleri sağlama yükümlülüğü	128
D. CRA'ya uyumsuzluk durumunda piyasaya arzı durdurma yükümlülüğü	128
E. Dijital unsurlu üründe önemli bir siber güvenlik riski tespit edilmesi durumunda üretici ve piyasa gözetimi ve denetimi makamlarına bildirimde bulunma yükümlülüğü.....	129
F. Tanıtıcı bilgilerini paylaşma ve erişilebilir kılma yükümlülüğü.....	129
G. CRA'ya uyumsuzluğu tespit etmesi durumunda düzeltici önlemleri alma yükümlülüğü.....	130
H. AB uygunluk beyanını 10 yıl boyunca bulundurma yükümlülüğü.....	130
I. CRA'ya uygunluğa ilişkin piyasa gözetimi ve denetimi makamlarına bilgi ve belge verme yükümlülüğü.....	130
J. Üreticinin faaliyetlerini durdurması halinde ilgili piyasa gözetimi ve denetimi makamları ile kullanıcılara bunu duyurma yükümlülüğü	131
IX. Dağıtıcının CRA Yükümlülükleri.....	131

A.	CRA'ya uyumlu dijital unsurlu ürünü piyasaya sürme yükümlülüğü	133
B.	CRA'ya uyumsuzluk durumunda piyasaya arzı durdurma yükümlülüğü	133
C.	Dijital unsurlu üründe ciddi siber güvenlik riski tespit edilmesi durumunda üreticiyi ve piyasa gözetimi ve denetimi makamlarını derhal bilgilendirme yükümlülüğü	134
D.	CRA'ya uyumsuzluğu tespit etmesi durumunda düzeltici önlemler alma yükümlülüğü	134
E.	Dijital unsurlu üründe güvenlik açığı tespit edilmesi durumunda üreticiye ve piyasa gözetimi ve denetimi makamlarına bildirimde bulunma yükümlülüğü	134
F.	CRA'ya uygunluğa ilişkin piyasa gözetimi ve denetimi makamlarına bilgi ve belge verme yükümlülüğü	135
G.	Üreticinin faaliyetlerini durdurması halinde ilgili piyasa gözetimi ve denetimi makamları ile kullanıcılara bunu duyurma yükümlülüğü	135
X.	Açık Kaynak Yazılım Sorumlusunun CRA Yükümlülükleri	136
A.	Piyasa gözetimi ve denetimi makamlarıyla iş birliği yükümlülüğü	138
B.	Siber güvenlik açıklarını bildirim yükümlülüğü	138
C.	Açık kaynak yazılımların güvenlik onayı	138
XI.	Ortak Yükümlülükler	139
XII.	Uyum Yöntemleri	140
XIII.	Uygunluk Karinesi	141
XIV.	Yaptırımlar	142
XV.	Değerlendirmeler	145
XVI.	CRA'nın Temel Ekleri	148
A.	EK 1 - Temel siber güvenlik gereklilikleri	148
B.	EK 2 - Kullanıcılara bilgi ve talimatlar	151

C. EK 7 - Teknik dokümantasyonun içeriği.....	153
§6. AVRUPA KONSEYİ VE SİBER GÜVENLİK	155
I. Sözleşmenin Amacı ve Kapsamı	157
II. Suçsallaştırma: Sözleşmedeki Maddi Ceza Hukuku Kuralları	158
III. Dijital Delillere Yönelik Özel Usuller ve Koruma Tedbirleri.....	161
IV. Uluslararası İş Birliği ve 7/24 İş Birliği Ağı	162
V. Birinci Ek Protokol.....	163
VI. İkinci Ek Protokol.....	164
VII. Değerlendirme	168
§7. BİRLEŞMİŞ MİLLETLER VE SİBER GÜVENLİK.....	169
I. Sözleşmenin Amacı, Kapsamı ve Temel İlkeleri.....	174
II. Suçsallaştırma: Sözleşmedeki Maddi Ceza Hukuku Kuralları	176
III. Dijital Delillere Yönelik Özel Usuller ve Koruma Tedbirleri.....	178
IV. Uluslararası İş Birliği	179
A. 7/24 İş Birliği Ağı	180
B. İş Birliği Yapılırken Kişisel Verilerin Korunması	181
V. Önleyici Tedbirler	182
§8. TÜRKİYE’DE SİBER GÜVENLİĞİN TARİHSEL GELİŞİMİ.....	187
§9. TÜRKİYE’DE SİBER GÜVENLİĞİN POLİTİK ÇERÇEVESİ.....	193
I. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.....	193
II. 2016-2019 Siber Güvenlik Stratejisi ve 2016-2019 Siber Güvenlik Eylem Planı.....	196
III. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023).....	199

IV.	Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028).....	201
A.	Siber dayanıklılık.....	202
B.	Proaktif siber savunma ve caydırıcılık.....	203
C.	İnsan odaklı siber güvenlik yaklaşımı	203
D.	Teknolojinin güvenli kullanımı ve siber güvenliğe katkısı	204
E.	Siber tehditlerle mücadelede yerli ve millî teknolojiler	204
F.	Uluslararası alanda Türkiye markası	204
V.	Diğer Politika Belgelerinde Siber Güvenlik Atıfları.....	205
A.	On İkinci Kalkınma Planı (2024-2028).....	205
B.	Orta Vadeli Program (2025-2027)	207
VI.	Değerlendirme	208
§ 10. TÜRK SİBER GÜVENLİK HUKUKU		211
§ 11. SİBER GÜVENLİK KANUNU’NUN AMACI		213
I.	Siber Tehditleri Tespit ve Bertaraf Etmek.....	214
II.	Siber Olayların Etkisini Azaltmak	214
III.	Siber Saldırlara Karşı Koruyucu Düzenlemeler Yapmak... 214	
IV.	Siber Güvenlik Stratejilerini ve Politikalarını Belirlemek... 215	
V.	Siber Güvenliğe İlişkin İdari Teşkilatı Kurmak.....	215
§ 12. TEMEL SİBER GÜVENLİK KAVRAMLARI		217
§ 13. SİBER GÜVENLİK KANUNU’NUN KAPSAMI		223
I.	Yasanın Genel Kapsamı	223
II.	İstisnalar ve Kapsam Dışı Faaliyetler	224
III.	Kapsamın Değerlendirilmesi.....	225
§ 14. TEMEL SİBER GÜVENLİK İLKELERİ		227
I.	Güvenliğin Bütünlüğü İlkesi.....	228
II.	Koruma ve Güvenlik İlkesi	229
III.	Kurumsallık, Süreklilik ve Sürdürülebilirlik İlkeleri.....	230
IV.	Yaşam Döngüsünü Gözetme İlkesi	232
V.	Sürekli Gelişim İlkesi	233

VI.	Kapasite Geliştirme İlkesi	233
VII.	Tüm Paydaşların Sorumluluğu İlkesi.....	235
VIII.	Hesap Verebilirlik İlkesi.....	236
IX.	Yerlilik ve Millilik İlkesi	239
X.	Yaygınlaştırma İlkesi.....	240
XI.	Hukukun Üstünlüğü, Temel İnsan Hak ve Hürriyetleri ile Mahremiyetin Korunması İlkeleri	241
§ 15.	SİBER GÜVENLİK BAŞKANLIĞI	247
I.	Başkanlık Görev ve Yetkilerin Temel Çerçevesi	248
A.	Strateji, Politika ve Koordinasyon	248
B.	Eğitim, Bilinçlendirme ve Kapasite Geliştirme	249
C.	Teknik Güvenlik ve Operasyonel Müdahale	249
D.	Altyapı ve Sistem Güvenliği.....	249
E.	Standartlar, Sertifikasyon ve Denetim.....	250
F.	İş Birliği ve Uluslararası İlişkiler.....	250
G.	Dijital Dönüşüm ve Yapay Zekâ.....	250
II.	Başkanlığın Görev ve Yetkilerinin Kapsamı	251
A.	Siber güvenlikle ilgili görev ve yetkiler	251
B.	Dijital dönüşüm ve e-devletle ilgili görev ve yetkiler....	259
C.	Açık kaynak kodlu yazılımlarla ilgili görev ve yetkiler..	261
D.	Yapay zekayla ilgili görev ve yetkiler.....	262
III.	Başkanlığın Teşkilat Yapısı	263
A.	Genel olarak	263
B.	Başkanlığın hizmet birimleri	264
C.	Çalışma grupları	264
D.	Başkanlığın personel rejimi.....	265
E.	Başkanlığın gelirleri	266
F.	Başkanlığa tanınan özel muafiyetler	267
§ 16.	SİBER GÜVENLİK KURULU	269
I.	SG Kurulu'nun Tarihsel Gelişimi	269
II.	Yeni SG Kurulu'nun Yapısı.....	272

§ 17. ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ (USOM).....	277
I. Kurumsal SOME	279
II. Sektörel SOME	280
III. Ortak Kurallar	283
IV. SOME ve USOM ilişkisi	284
§ 18. SİBER GÜVENLİK AKTÖRLERİNİN SORUMLULUĞU....	287
I. SGB ile İş Birliği Yapma Yükümlülüğü	289
II. Siber Güvenlik Tedbirleri Alma Yükümlülüğü	290
III. Zafiyet ve Siber Olayları Gecikmeksizin SGB'ye Bildirim Yükümlülüğü	290
IV. Yetkilendirilmiş ve Belgelendirilmiş Tedarikçi Kullanma Yükümlülüğü.....	292
V. Siber Güvenlik Şirketlerine Yönelik Faaliyet İzni Yükümlülüğü.....	294
§ 19. SİBER GÜVENLİK ÜRÜN VE ŞİRKETLERİNE İLİŞKİN YÜKÜMLÜLÜKLER.....	297
§ 20. SİBER GÜVENLİK DENETİMLERİ.....	301
I. Siber Güvenlik Denetimlerinde Usul	301
II. Siber Güvenlik Denetimlerinde Arama, Kopya Çıkarma ve El Koyma	303
§ 21. SİBER GÜVENLİK FAALİYETLERİNDE KİŞİSEL VERİLERİN KORUNMASI	305
§ 22. İDARİ PARA CEZALARI	311
I. İdari Para Cezası Türleri.....	311
II. İdari Para Cezalarının Muhatabı.....	313
III. İdari Para Cezalarında Usul	318
IV. Kabahatlerde İctima	318
V. İdari Para Cezalarının Ödenmesi.....	319
VI. İdari Para Cezalarına Karşı Yargı Yolu	320
§ 23. SİBER GÜVENLİK SUÇLARI: SİBER CEZA HUKUKU.....	321
I. Siber Yasada Siber Güvenlik Suçları.....	321

A.	Siber güvenlik denetimi sırasında iş birliğinde bulunmama suçu.....	324
B.	İzinsiz siber güvenlik faaliyetinde bulunma suçu.....	326
C.	Sır ifşası suçu.....	328
D.	Kişisel veya kurumsal verileri ifşa suçu.....	329
E.	Veri sızıntısı söylentisi çıkarma suçu.....	331
	1. Genel olarak suçun incelenmesi.....	332
	2. Sosyal medyada beğenme veya paylaşma durumunda sorumluluk.....	336
F.	Milli unsurlara yönelik siber saldırı suçu.....	341
G.	Milli unsurlara ait verileri ifşa suçu.....	343
H.	İlk grup siber suçlar için ortak hükümler	344
I.	SGB personeline getirilen yasaklamalara aykırı davranılması suçu.....	346
J.	Veri ihlaline sebebiyet verme suçu	349
II.	Türk Ceza Kanunu'nda Siber Güvenlik Suçları.....	352
III.	Siber Suç İstatistikleri	355
IV.	Değerlendirme	359

§24. TARİHSEL BAĞLAMDA SİBER GÜVENLİK KURUM

	VE KURULUŞLARI	363
I.	Ulaştırma ve Altyapı Bakanlığı.....	363
II.	Bilgi Teknolojileri ve İletişim Kurumu (BTK)	368
	A. Anayasa Mahkemesi'nin 2017/16 esas ve 24.07.2019 tarihli kararı	371
	B. Anayasa Mahkemesi kararının değerlendirilmesi	373
	C. BTK'nın 5651 sayılı İnternet Kanunu kapsamındaki siber güvenlik yetkileri.....	377
	D. BTK'nın genel siber güvenlik yetkilerinin ilgası.....	377
III.	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi	378
	A. Dijital Dönüşüm Ofisi'nin genel görev ve yetkileri.....	378
	B. Dijital Dönüşüm Ofisi'nin kapatılması.....	382

IV.	Afet ve Acil Durum Yönetimi Başkanlığı (AFAD).....	383
V.	BTK ve Dijital Dönüşüm Ofisi İçin Devir ve Geçiş Hükümleri	384
§25. SİBER GÜVENLİKLE İLGİLİ YETKİLİ DİĞER KURUM VE KURULUŞLAR.....		387
I.	Cumhurbaşkanlığı.....	387
A.	Güvenlik ve Dış Politikalar Kurulu	387
B.	Milli Güvenlik Kurulu.....	388
II.	Savunma Sanayii Başkanlığı.....	389
III.	Devlet Arşivleri Başkanlığı.....	392
IV.	Millî İstihbarat Teşkilâtı.....	393
A.	Anayasa Mahkemesi'nin MİT Kanunu'na ilişkin 2014/122 esas ve 30.12.2015 tarihli kararı	395
B.	MİT'in diğer siber güvenlik faaliyetleri.....	399
V.	Türk Silahlı Kuvvetleri.....	400
VI.	Sanayi ve Teknoloji Bakanlığı.....	401
A.	Siber güvenliğe ilişkin temel görev ve yetkiler	401
B.	2023 Sanayi ve Teknoloji Stratejisi.....	403
C.	2024-2028 Stratejik Planı.....	405
D.	2030 Sanayi ve Teknoloji Stratejisi.....	405
VII.	Türk Standartları Enstitüsü.....	407
VIII.	Kişisel Verileri Koruma Kurumu	408
IX.	İçişleri Bakanlığı.....	411
A.	Emniyet Genel Müdürlüğü.....	411
1.	Avrupa Konseyi Siber Suç Sözleşmesi 7/24 İş Birliği Ağı faaliyetleri.....	411
2.	Polisin sanal ortamda istihbarat faaliyetleri.....	412
3.	Sanal devriye faaliyetleri.....	412
B.	Jandarma Genel Komutanlığı.....	415
C.	Sahil Güvenlik Komutanlığı	416
X.	Adalet Bakanlığı	416

XI.	Mesleki Yeterlilik Kurumu	417
	A. Siber Güvenlik Elemanı.....	418
	B. Etik Hacker.....	419
XII.	Devlet Malzeme Ofisi	420
XIII.	Bankacılık Düzenleme ve Denetleme Kurumu	421
XIV.	Sermaye Piyasası Kurulu	423
XV.	Türkiye Cumhuriyet Merkez Bankası.....	424
XVI.	Enerji Piyasası Düzenleme Kurumu	426
XVII.	Sivil Havacılık Genel Müdürlüğü	427
XVIII.	Gelir İdaresi Başkanlığı.....	431
XIX.	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu.....	433
XX.	Yükseköğretim Kurulu.....	434
XXI.	Millî Eğitim Bakanlığı.....	436
XXII.	Muhtelif Siber Güvenlik Yapıları ve Birimleri	436
§ 26.	YÜRÜRLÜK VE GEÇİŞ SÜRECİ.....	439
§ 27.	SONUÇ VE DEĞERLENDİRME.....	441
	KAYNAKÇA.....	451