BOSCA
LAW

SCADA ve Endüstriyel Kontrol Sistemleri Kaynaklı Siber Risklerde Enerji Şirketlerinin Hukuki Sorumluluğu

www.bosca.av.tr

SCADA ve Endüstriyel Kontrol Sistemleri Kaynaklı Siber Risklerde Enerji Şirketlerinin Hukuki Sorumluluğu

Özet

Enerji altyapılarının dijitalleşmesi, SCADA ve endüstriyel kontrol sistemleri (EKS) üzerinden gerçekleşen siber olayların etkisini bilgi güvenliği alanından fiziksel dünyaya taşımıştır. Bu çalışma, söz konusu riskleri teknik bir mesele olarak değil, enerji şirketlerinin hukuki sorumluluğunu doğuran bir risk alanı olarak ele almaktadır. Türk Borçlar Kanunu (haksız fiil, adam çalıştıranın ve organizasyonun sorumluluğu, ifa yardımcısı, tehlike sorumluluğu) ve Türk Ticaret Kanunu (yönetim kurulunun özen ve gözetim yükümlülüğü) çerçevesinde, 7545 sayılı Siber Güvenlik Kanunu, EPDK Yetkinlik Modeli Yönetmeliği, IEC 62443 ve NIS2 ile karşılaştırmalı biçimde, enerji şirketlerinden beklenen makul özen ve siber dayanıklılık standardını ortaya koymaktadır. Çalışma ayrıca sigortalanabilirlik ve proje finansmanı (finanse edilebilirlik) boyutlarını değerlendirmekte ve mevzuat boşluklarına ilişkin politika önerileri sunmaktadır.

Anahtar Kelimeler: Kritik altyapı, SCADA/EKS, makul özen, organizasyon kusuru, tehlike sorumluluğu, yönetim kurulu sorumluluğu, siber dayanıklılık, Siber Güvenlik Kanunu, siber sigorta, finanse edilebilirlik.

I. Giriş

Enerji sektörü son yirmi yılda üretimden iletim ve dağıtıma, doğal gaz altyapılarından rafinerilere kadar uzanan operasyonel alanını bilgi ve iletişim teknolojileriyle bütünleştirmiştir. Bu dönüşümün merkezinde, süreçleri izleyen ve fiziksel ekipmana komut veren Denetleyici Kontrol ve Veri Toplama (SCADA) sistemleri ile endüstriyel kontrol sistemleri yer almaktadır. Bu sistemler, enerji altyapısının yalnızca veri katmanını değil, fiilî işletme mantığını taşımaktadır.

Bu nedenle SCADA katmanına yönelik bir ihlal, klasik veri güvenliği probleminden farklı sonuçlar doğurmakta ve üretim kaybına, ekipman hasarına, çevresel zarara, arz kesintisine, hatta can kaybına yol açabilmektedir. Hukuki açıdan asıl mesele de buradadır. Enerji şirketinin karşılaşacağı sorumluluk, saldırının teknik niteliğinden çok, şirketin kendisinden beklenen güvenlik ve dayanıklılık standardını sağlayıp sağlamadığına bağlı olarak şekillenmektedir.

Bu çalışmanın temel tezi, enerji sektöründe siber güvenliğin bir bilgi işlem yükümlülüğü olmaktan çıkıp işletmecinin özen yükümlülüğünün ayrılmaz bir parçası hâline gelmiş olmasıdır. SCADA, OT ve EKS bu çalışmada teknik inceleme konusu olarak değil, hukuki sonuç doğuran risk alanları olarak ele alınmakta ve analizin ekseni enerji şirketlerinin hukuki sorumluluğu üzerine kurulmaktadır. 12/3/2025 tarihli ve 7545 sayılı Siber Güvenlik Kanunu'nun yürürlüğe girmesiyle bu eksen, Türk hukukunda artık yalnızca genel sorumluluk hükümlerine değil, açık bir yasal çerçeveye de dayanmaktadır. Çalışma, mevcut hukuki durumu açıklamakla yetinmeyip mevzuat boşluklarını, düzenleme ihtiyaçlarını ve enerji şirketlerinin bugünden alması gereken önlemleri de değerlendirmeyi amaçlamaktadır.

II. SCADA/EKS, Kritik Altyapı ve OT–IT Ayrımı

SCADA sistemleri; programlanabilir mantık kontrolörleri (PLC), uzak terminal üniteleri (RTU) ve insan-makine arayüzleriyle birlikte endüstriyel kontrol sistemi mimarisini oluşturmaktadır. Bilgi teknolojisi (IT) sistemlerinde gizlilik öncelikliyken, operasyonel teknoloji (OT) sistemlerinde önceliğin erişilebilirlik ve bütünlük olması, riskin niteliğini değiştirmektedir. OT katmanındaki bir manipülasyon doğrudan fiziksel sürece yansımaktadır. Türk hukukunda da bu sistemler düzenleyici çerçevenin konusu hâline gelmiştir.[1]

Kritik altyapı işleten bir kuruluştan beklenen güvenlik seviyesi, sıradan ticari işletmelere uygulanabilecek olandan yüksektir. EPDK Yetkinlik Modeli Yönetmeliği'nin yükümlüleri sektörel kritiklik derecesine göre seviyelere ayırması, bu kademeli özen anlayışının düzenleyici ifadesidir.[2] Aşağıda gösterileceği üzere, bu kademelendirme aynı zamanda hukuki özen standardının somutlaştırılmasında bir ölçüt işlevi görmektedir.

III. Uluslararası Vaka Analizleri

Enerji sektöründe siber riskin neden artık öngörülebilir bir risk olduğunu, son on beş yılın beş dönüm noktası olayı göstermektedir. Bu olayların ortak dersi, riskin bilinir ve öngörülebilir hâle gelmesidir. Bu durum, kusur ve özen değerlendirmesinin merkezindeki ölçütü doğrudan etkilemektedir.

[1]Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği (EPDK) m. 1; Yönetmelik, enerji sektöründe kullanılan endüstriyel kontrol sistemlerinin siber güvenliğini sürekli gelişen ihtiyaç ve tehditlere göre iyileştirmeyi, asgari kabul edilebilir güvenlik seviyesini tanımlamayı ve bu sistemlerin siber dayanıklılık, yeterlilik ve olgunluğuna ilişkin usul ve esasları düzenlemeyi amaçlamaktadır.

[2]Yönetmelik m. 2 (Değişik: RG-28/1/2024-32443); kapsam, elektrik iletim ve dağıtım lisansı sahiplerini, kurulu gücü 100 MWe ve üzeri elektrik üretim tesislerini, boru hattı ile iletim yapan doğal gaz iletim lisansı sahiplerini, sevkiyat kontrol merkezi kurmakla yükümlü doğal gaz dağıtım ve depolama (LNG, yer altı) lisansı sahiplerini, ham petrol iletim ve rafinerici lisansı sahiplerini içermektedir. Black-Start özelliğine sahip ve TEİAŞ SCADA/EMS ile haberleşen üretim tesisleri de kapsamdadır; OSB dağıtım ve üretim lisansı sahipleri kapsam dışıdır.

1. Stuxnet (2010)

Natanz zenginleştirme tesisindeki Siemens PLC'leri hedef alan Stuxnet, santrifüjlerin çalışma parametrelerini değiştirirken operatör ekranlarına normal değerler yansıtmış ve fiziksel ekipman hasarına yol açmıştır.[3] Olayın önemi, bir siber saldırının ilk kez doğrudan fiziksel tahribat doğurabildiğinin kanıtlanmasıdır. Buradan çıkan hukuki ders, siber ile fiziksel güvenlik arasındaki ayrımın ortadan kalkması ve OT kaynaklı zararların maddi hasar sorumluluğu doğurabileceğinin görünür hâle gelmesidir.

2. BlackEnergy (2015)

Ukrayna dağıtım şebekesine yönelik saldırı yaklaşık 225.000 aboneyi etkilemiştir.[4] Bir siber olayın doğrudan arz kesintisine yol açabildiğini gösteren bu olay; arz güvenliği, kamu hizmetinin sürekliliği, mücbir sebep savunmasının sınırları ve işletmecinin abonelere karşı sorumluluğu tartışmalarını gündeme taşımıştır.

3. Industroyer / CrashOverride (2016)

Industroyer, enerji sektörüne özgü IEC 60870-5-104 ve IEC 61850 protokollerini kullanabilen ilk modüler saldırı aracı olarak kesici ve röleleri doğrudan yönetebilmiştir.[5] Bu olay, saldırganın artık yalnızca bilişim sistemlerini değil, enerji altyapısının teknik dilini ve işletme mantığını da hedef aldığını ortaya koymuş ve işletmeciden beklenen savunmanın da OT'ye özgü hâle gelmesini gerektirmiştir.

[3]R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon", IEEE Security & Privacy, 2011; Stuxnet, Natanz tesisindeki Siemens S7 PLC'leri ve frekans çeviricileri (VFD) hedef alarak santrifüjleri tahrip edici hızlarda döndürürken operatör ekranlarına normal değerler yansıtmıştır.
[4]U.S. Department of Homeland Security / ICS-CERT, "Cyber-Attack Against Ukrainian Critical Infrastructure" (IR-ALERT-H-16-056-01), 2016; SANS ICS & E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid", 2016. Yaklaşık 225.000 abone elektriksiz kalmıştır.
[5]ESET, "Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet", 2017; Dragos Inc., "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations", 2017. Zararlı yazılım IEC 60870-5-101/104, IEC 61850 ve OPC DA protokollerini kullanarak kesici ve röleleri doğrudan yönetebilmiştir.

4. Triton / Trisis (2017)

Bir petrokimya tesisinde hedef, üretim değil Güvenlik Enstrümante Sistemleri (SIS) olmuştur. Saldırı başarılı olsaydı toksik gaz salımı, patlama ve can kaybı doğabilirdi.[6] Triton, siber güvenlik ile iş sağlığı ve güvenliği, çevre hukuku ve yönetici sorumluluğu arasındaki bağı somutlaştırmıştır. Güvenlik fonksiyonunun hedef alınması, tehlike sorumluluğu tartışmasını doğrudan ilgilendirmektedir.

5. Colonial Pipeline (2021)

ABD'nin en büyük akaryakıt boru hattı işletmecilerinden birine yönelik fidye yazılımı saldırısı faaliyetlerin durdurulmasına ve bölgesel arz krizine yol açmıştır. Şirket yaklaşık 4,4 milyon USD fidye ödemiş; düzenleyici otorite kontrol odası ihlalleri nedeniyle idari para cezası önermiş ve TSA bağlayıcı güvenlik direktifleri yayımlamıştır.[7] Olay, BT sistemlerine yönelik bir saldırının dahi OT faaliyetini durdurabileceğini ve sorunun ulusal arz güvenliği boyutu taşıdığını göstermiştir. Düzenleyici tepkinin hızı, zorunlu bildirim yükümlülüklerinin yaygınlaşacağına işaret etmektedir.[8]

[6]FireEye/Mandiant, "TRITON Malware Analysis Report", 2017; saldırı, Schneider Electric Triconex Güvenlik Enstrümante Sistemlerini (SIS) hedef almış, başarılı olması hâlinde toksik gaz salımı veya patlama riski doğurabilecekti. Triton, endüstriyel güvenlik sistemlerini hedef alan ilk zararlı yazılım olarak nitelenmektedir.
[7]U.S. DOJ, basın açıklaması, 7 Haziran 2021 (fidyenin bir kısmının geri alınması); DarkSide grubuna ödenen fidye 75 BTC (~4,4 milyon USD); PHMSA, kontrol odası ihlalleri nedeniyle ~1 milyon USD idari para cezası önermiş; TSA, Mayıs ve Temmuz 2021 tarihli Güvenlik Direktifleri ile boru hattı işletmecilerine olay bildirim ve dayanıklılık yükümlülükleri getirmiştir.
[8]Cyber Incident Reporting for Critical Infrastructure Act of 2022 (ABD); kritik altyapı kuruluşlarına önemli siber olayları 72 saat, ödenen fidyeleri 24 saat içinde CISA'ya bildirme yükümlülüğü getirmiştir.

IV. Düzenleyici Çerçeve ve Özen Standardının Kaynakları

Türkiye'de enerji sektörünün siber güvenliği iki katmanlı bir düzenleyici çerçeveye oturmaktadır. Yatay ve genel düzlemde 7545 sayılı Siber Güvenlik Kanunu, dikey ve sektörel düzlemde ise EPDK Yetkinlik Modeli Yönetmeliği yer almakta ve bunlara uluslararası standartlar ile Avrupa düzenlemesi eşlik etmektedir. Bu metinler doğrudan tazminat doğurmamaktadır. Asıl işlevleri, enerji şirketinden beklenen makul özen, organizasyon yükümlülüğü ve kurumsal gözetim borcunun içeriğini somutlaştırmalarıdır.

1. 7545 Sayılı Siber Güvenlik Kanunu

12/3/2025 tarihli ve 7545 sayılı Siber Güvenlik Kanunu, Türk hukukunda siber güvenliği ilk kez genel ve çatı bir kanun düzeyinde düzenlemiştir. Kanun, Siber Güvenlik Başkanlığı ile Cumhurbaşkanı başkanlığındaki Siber Güvenlik Kurulu'nu kurmakta ve "kritik altyapı"yı, işlediği verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapı olarak tanımlamaktadır.[9] Enerji üretim, iletim ve dağıtım altyapılarının bu tanım kapsamına girdiği açıktır. Kritik altyapı sektörlerini belirleme yetkisi ise Siber Güvenlik Kurulu'na aittir.

Kanun'un enerji şirketleri bakımından en kritik hükmü, m. 7'de düzenlenen yükümlülüklerdir. Buna göre kapsamdaki kuruluşlar, tespit ettikleri zafiyet veya siber olayları gecikmeksizin Başkanlığa bildirmek ve mevzuatın öngördüğü tedbirleri almakla yükümlüdür. Bu yükümlülüklerin ihlali, m. 16 uyarınca ağır idari para cezalarına bağlanmıştır.

[9]Siber Güvenlik Kanunu, Kanun No. 7545, Kabul Tarihi 12/3/2025, RG 19/3/2025, S. 32846. Kanun, Siber Güvenlik Başkanlığı ile Cumhurbaşkanı başkanlığındaki Siber Güvenlik Kurulu'nu kurmaktadır (m. 5, m. 9). m. 3/d, "kritik altyapı"yı, işlediği verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapı olarak tanımlamaktadır; kritik altyapı sektörlerini belirleme yetkisi Siber Güvenlik Kurulu'ndadır (m. 9/4-ç).

İlgili yükümlülükleri yerine getirmeyenlere bir milyon ila on milyon Türk lirası, denetim yükümlülüğünü ihlal eden ticari şirketlere ise brüt satış hasılatının yüzde beşine kadar idari para cezası uygulanmaktadır. Dahası, kabahatten menfaat sağlanması veya zarar doğması hâlinde ceza, bu menfaat veya zararın üç ila beş katına çıkarılmaktadır.[10]

Bu düzenleme, makul özen analizi bakımından bir eşik değişimi yaratmaktadır. Olay bildirimi ve makul güvenlik tedbiri alma artık yalnızca iyi uygulama değil, kanuni bir yükümlülüktür. Bu yükümlülüğün ihlali, idari yaptırımın yanında, özel hukuk düzleminde de kusur ve özellikle organizasyon kusuru değerlendirmesinde güçlü bir gösterge oluşturmaktadır. Kanun'un öngördüğü idari para cezası rejimi ile özel hukuk tazminat sorumluluğu birbirinden bağımsız işleyen, ancak aynı özen standardını besleyen iki ayrı rejimdir. İdari ceza Başkanlığa, tazminat ise zarar gören üçüncü kişilere karşı gündeme gelmektedir.

2. EPDK Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği

4628 sayılı Kanun'a dayanan Yönetmelik, sektörel düzlemde enerji şirketlerinden beklenen güvenlik içeriğini somutlaştırmaktadır. Kapsamı, elektrik iletim ve dağıtım lisansı sahiplerini, kurulu gücü 100 MWe ve üzeri üretim tesislerini, doğal gaz iletim lisansı sahiplerini, sevkiyat kontrol merkezi kurmakla yükümlü doğal gaz dağıtım lisansı sahiplerini, doğal gaz depolama lisansı sahiplerini, ham petrol iletim ve rafinerici lisansı sahiplerini içermektedir. Black-Start özelliğine sahip ve TEİAŞ SCADA/EMS ile haberleşen üretim tesisleri de kapsamdadır. Yönetmelik, yetkinlik modelini on bir ana kontrol başlığında düzenlemektedir.

[10]7545 sayılı Kanun m. 7/1: kapsamdakiler, hizmet sundukları alanda tespit ettikleri zafiyet veya siber olayları "gecikmeksizin" Başkanlığa bildirmek ve mevzuatın öngördüğü tedbirleri almakla yükümlüdür; m. 8 denetim yetkisini düzenlemektedir. m. 16/10 uyarınca m. 7/1-(b) ve (c) yükümlülüklerini yerine getirmeyenlere 1.000.000–10.000.000 TL idari para cezası; m. 16/11 uyarınca denetim yükümlülüğünü ihlal eden ticari şirketlere brüt satış hasılatının %5'ine kadar idari para cezası; m. 17/2 uyarınca kabahatten menfaat temin edilmesi veya zarar doğması hâlinde ceza, menfaat veya zararın üç ila beş katı olarak uygulanmaktadır.

Modelin ana başlıkları endüstriyel ağ güvenliği, istemci ve sunucu güvenliği, tehdit ve zafiyet yönetimi, risk yönetimi, varlık ve konfigürasyon yönetimi, kimlik ve erişim yönetimi, olay yönetimi ve süreklilik, akıllı cihaz güvenliği, operasyon güvenliği, insan kaynakları güvenliği, fiziksel güvenlik, tedarikçi yönetimi ve PLC güvenliğidir. Bu başlıklar, sektörel kritiklik derecesine göre belirlenen ve uygulanması zorunlu üç yetkinlik seviyesine dağıtılmakta ve model, TS ISO/IEC 27001 ile EKS odaklı TS EN ISO/IEC 27019 ile uyumludur.[11]

Bu kontrol başlıkları, sorumluluk hukuku bakımından doğrudan işlevseldir. Varlık yönetimi, erişim yönetimi, olay yönetimi, tedarikçi yönetimi, insan kaynakları güvenliği ve PLC güvenliği gibi alanların düzenleyici metinde ayrı başlıklar olarak sayılması tesadüf değildir. Bu başlıklar, TBK m. 66/III anlamında beklenen organizasyon standardının doğrudan ölçütleridir. Bir siber olayda mahkeme, hakem heyeti veya bilirkişi, enerji şirketinin çalışma düzenini bu başlıklar ekseninde değerlendirebilir ve ilgili kontrolün hiç uygulanmamış olması, organizasyon kusurunun karinesi gibi işlev görebilir.

[11]Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği m. 6, yetkinlik modelini on bir ana kontrol başlığında düzenlemektedir: endüstriyel ağ güvenliği; endüstriyel istemci ve sunucu güvenliği; tehdit ve zafiyet yönetimi; siber güvenlik risk yönetimi; varlık, değişim ve konfigürasyon yönetimi; kimlik ve erişim yönetimi; olay yönetimi ve süreklilik; akıllı cihaz güvenliği; operasyon güvenliği; insan kaynakları güvenliği; fiziksel güvenlik; tedarikçi yönetimi ve PLC güvenliği. m. 7, sektörel kritiklik derecesine göre belirlenen ve uygulanması zorunlu üç yetkinlik seviyesi öngörmektedir; m. 5 uyarınca model TS ISO/IEC 27001, TS EN ISO/IEC 27019 ve Bilgi ve İletişim Güvenliği Rehberi ile uyumludur; dayanağı 4628 sayılı Kanun'dur (m. 3). Kontrol maddeleri üç yıllık periyotlarla güncellenebilir.

3. Uluslararası Standartlar ve Karşılaştırmalı Çerçeve: IEC 62443 ve NIS2

IEC 62443 standart serisi, güvenlik seviyeleri (SL1–SL4) ve bölge/iletim kanalı (zone/conduit) yaklaşımıyla EKS güvenliğinin uluslararası teknik referansıdır ve Yönetmelik'in kademeli yetkinlik mantığıyla örtüşmektedir.[12] NIS2 Direktifi ise siber güvenlik sorumluluğunu açıkça yönetim organı seviyesine taşıyarak yöneticinin kişisel sorumluluğunu öngörmektedir.[13] Türk hukuku bakımından NIS2, bağlayıcı olmamakla birlikte, 7545 sayılı Kanun'un hesap verebilirlik ilkesi ile TTK m. 369–553 ekseninde mevcut gözetim yükümlülüğünü pekiştiren karşılaştırmalı bir ölçüttür.

Üç düzenleme birlikte değerlendirildiğinde, enerji şirketlerinden beklenen uluslararası özen standardı giderek yakınsamaktadır. 7545 sayılı Kanun ve Yönetmelik'e uyum, bu standardın yalnızca asgari eşiğini oluşturmaktadır. Uyumun varlığı sorumluluğu tek başına bertaraf etmemektedir. Buna karşılık uyumun yokluğu, kusur ve organizasyon kusuru lehine güçlü bir karine sağlamaktadır. Bu nedenle gelecekteki bir uyuşmazlıkta temel tartışma, saldırının nasıl gerçekleştiği değil, enerji şirketinin kendi faaliyet alanı bakımından bu düzenlemelerin somutlaştırdığı makul siber dayanıklılık seviyesine ulaşıp ulaşmadığı olacaktır.

[12]IEC 62443 Serisi (Industrial communication networks – Network and system security), özellikle 62443-3-3 (sistem güvenlik gereksinimleri ve güvenlik seviyeleri SL1–SL4) ve 62443-2-1 (güvenlik yönetim sistemi); bölge ve iletim kanalı (zone/conduit) ayrımı.

[13]Directive (EU) 2022/2555 (NIS2), m. 20: temel ve önemli kuruluşların yönetim organları siber güvenlik risk yönetim tedbirlerini onaylamak ve uygulanmasını gözetmekle yükümlü olup ihlalden kişisel olarak sorumlu tutulabilir; ağır ihmal hâllerinde yöneticiler için geçici yönetim yasağı dâhil yaptırımlar öngörülmüştür.

V. Türk Borçlar Kanunu Çerçevesinde Sorumluluk

SCADA kaynaklı bir siber olay teknik görünse de, doğurduğu sorumluluğun değerlendirilmesinde temel başvuru kaynağı Türk Borçlar Kanunu hükümleridir. Her bir hüküm bakımından sorulması gereken soru, bu risk veya olayın enerji şirketi bakımından hangi hukuki sonucu doğurduğudur.

1. Haksız Fiil Sorumluluğu ve Kusurun Objektifleşmesi

TBK m. 49 uyarınca kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür. Doktrinde hukuka aykırılığın objektif, kusurun ise sübjektif unsur olduğu kabul edilmektedir. Ancak kusur değerlendirmesinde ölçüt giderek objektifleşmiş ve makul ve özenli bir işletmecinin göstereceği davranışa bağlanmıştır.[14] Bir enerji tesisinde kritik varlık envanterinin oluşturulmaması, bilinen açıkların kapatılmaması veya yetkisiz erişimlerin engellenmemesi sonucu üçüncü kişiler zarara uğrarsa, sorumluluk öncelikle bu hüküm kapsamında değerlendirilmektedir. Risklerin Stuxnet sonrası öngörülebilir hâle geldiği dikkate alındığında, gerekli tedbirlerin alınmaması kusur değerlendirmesinde belirleyici olmaktadır.

[14]İ. Erdoğan, "Haksız Fiilde Kusurlu Sorumluluk ve Özellikle Kusur Unsuru", Selçuk Üniversitesi Hukuk Fakültesi Dergisi. Yazar, hukuka aykırılığın objektif, kusurun ise sübjektif unsur olduğunu; her kusurlu fiilin hukuka aykırı olduğunu vurgulamaktadır.

2. Adam Çalıştıranın Sorumluluğu ve Organizasyon Kusuru

Olayların önemli bölümü, yetkisiz uzaktan erişim verilmesi, OT ağına kontrolsüz cihaz bağlanması veya varsayılan parolaların değiştirilmemesi gibi insan ve organizasyon kaynaklı eksikliklerden doğmaktadır. TBK m. 66 uyarınca adam çalıştıran, çalışanının iş görürken üçüncü kişilere verdiği zarardan sorumludur. Bu sorumluluk, çalışanın kusuruna değil, işverenin objektif özen ve gözetim ödevinin ihlaline dayanan kusursuz bir sorumluluktur.[15]

Asıl güçlü dayanak m. 66/III'teki organizasyon sorumluluğudur. Bu hüküm, işletmede adam çalıştırana çalışma düzenini zararın doğmasını önleyecek biçimde kurma yönünde genel ve objektif bir özen ödevi yüklemektedir. Söz konusu sorumluluk yalnızca çalışanların değil, işletme faaliyetinin sebep olduğu tüm zararları kapsamakta ve kurtuluş kanıtı dardır.[16] Bir enerji şirketinin varlık envanteri tutmaması, ağ segmentasyonu uygulamaması, üçüncü taraf erişimlerini denetlememesi, olay müdahale planı bulundurmaması veya personeline OT siber güvenlik eğitimi vermemesi, meydana gelen zararın organizasyon kusuru olarak nitelenmesine elverişlidir. Bir mühendisin telefonundan hotspot açarak OT ağını internete bağlaması gibi bir olay, münferit bir çalışan hatası değil, kurumsal denetim eksikliğinin tezahürü olarak değerlendirilebilir. Yukarıda anılan Yönetmelik kontrol başlıkları ve 7545 sayılı Kanun'un tedbir alma yükümlülüğü, beklenen organizasyon standardının ölçütü olarak burada işlevseldir.

[15]D. Deniz, "Adam Çalıştıranın Sorumluluğu Bakımından Nedensellik Bağı Unsuru", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C. XVIII, 2021/2, s. 1155–1176. Sorumluluk, çalışanın kusuruna değil, adam çalıştıranın objektif özen ve gözetim ödevinin (seçme, talimat, denetim) ihlaline dayanan bir kusursuz sorumluluktur.

[16]A. Türkmen, "6098 Sayılı Türk Borçlar Kanununa Göre Organizasyon Sorumluluğu (TBK m. 66/III)", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. LXX, S. 2, 2012, s. 257–284. TBK m. 66/III, işletmede adam çalıştırana çalışma düzenini zararın doğmasını önleyecek biçimde kurma yönünde genel ve objektif bir özen ödevi yüklemektedir; sorumluluk yalnızca çalışanların değil, işletme faaliyetinin sebep olduğu tüm zararları kapsamakta ve kurtuluş kanıtı dardır.

3. İfa Yardımcılarının Fiillerinden Sorumluluk ve Tedarik Zinciri Riski

Enerji projeleri, SCADA tedarikçileri, OEM üreticileri, EPC yüklenicileri, bakım firmaları ve uzaktan erişim sağlayan hizmet sağlayıcıları gibi çok sayıda üçüncü tarafın yer aldığı yapılardır. Bu aktörler çoğu zaman enerji şirketinin ifa yardımcısı konumundadır. TBK m. 116, sözleşmeden doğan bir kusursuz sorumluluk öngörmektedir. Bu sorumlulukta borçlu ile yardımcı kişi arasında bağımlılık veya hizmet ilişkisi aranmaz ve farazi kusur ölçütü esas alınmaktadır.[17] Bir OEM mühendisinin hatalı uzaktan erişimi, bir bakım yüklenicisinin bıraktığı açık veya SCADA yazılımının hatalı yapılandırılması sonucu doğan zarardan enerji şirketi alacaklıya karşı sorumlu olmakta ve ardından yardımcı kişiye rücu edebilmektedir. Siber riskin önemli kısmının tedarik zinciri kaynaklı olduğu dikkate alındığında, bu hüküm önümüzdeki yıllarda merkezî bir rol oynayacaktır.

[17]F. Gültekin, "Yardımcı Kişinin Fiillerinden Borçlunun Sorumluluğu", Türkiye Adalet Akademisi Dergisi, Yıl 9, S. 35, Temmuz 2018, s. 373 vd.; ayrıca S. Yünlü, Yardımcı Kişilerin Fiillerinden Sorumluluk, 2018. TBK m. 116, sözleşmeden doğan bir kusursuz sorumluluk olup borçlu ile ifa yardımcısı arasında bağımlılık veya hizmet ilişkisi aranmaz; "farazi kusur" ölçütü esastır.

4. Tehlike Sorumluluğu

TBK m. 71, önemli ölçüde tehlike arz eden işletmeler bakımından kusursuz sorumluluk öngörmektedir. İşleten kurtuluş kanıtı getirememekte, yalnızca illiyet bağını kesen sebepleri ispatlayarak sorumluluktan kurtulabilmektedir.[18] Elektrik iletim sistemleri, yüksek kapasiteli üretim tesisleri, doğal gaz iletim hatları, LNG terminalleri ve rafineriler, doktrinde tipik tehlikeli işletme örnekleri arasında sayılmaktadır.[19] Bir siber olayın geniş çaplı kesinti, patlama, yangın, çevresel zarar veya can kaybına yol açması hâlinde, zarar bu işletmelerin tipik tehlikesinin gerçekleşmesi olarak nitelenebilmekte ve sorumluluk kusurdan bağımsızlaşmaktadır.[20] Bu, enerji şirketleri için en ağır sonuç doğuran ihtimaldir. Siber tedbirlerin eksiksizliği dahi, illiyet bağı kurulduğunda sorumluluğu tek başına bertaraf etmeyebilir. Organizasyon sorumluluğundan farkı, kaynağın çalışma düzeninin elverişsizliği değil, işletmenin tipik tehlikesinin gerçekleşmesi olmasıdır.

5. Müteselsil Sorumluluk ve Çok Faillilik

Siber olaylarda zarar genellikle birden çok aktörün (işletmeci, tedarikçi, OEM, bakım yüklenicisi) katkısıyla doğmaktadır. TBK m. 61–62 uyarınca zarardan sorumlu olanlar müteselsilen sorumludur ve zarar gören, tazminatın tamamını dilediği sorumludan isteyebilmektedir.[21] Bu durum, enerji şirketini çoğu kez ilk muhatap hâline getirir. İç ilişkideki rücu ve risk dağılımı ise sözleşmesel kurguya bağlıdır ve bu da VI. bölümde ele alınan sözleşmesel risk tahsisinin önemini artırmaktadır.

[18]Y. Durak, "Tehlike Sorumluluğu", Erciyes Üniversitesi Hukuk Fakültesi Dergisi, C. IX, S. 1, 2014, s. 23 vd. TBK m. 71, tehlike sorumluluğunu ilk kez genel kural olarak düzenlemiş olup unsurları tehlikenin varlığı, tipik tehlikenin gerçekleşmesi ve illiyet bağıdır; nükleer, elektrik ve doğal gaz işletmeleri örnek gösterilmektedir.

[19]M. H. Korkusuz, "Tehlike Sorumluluğunun Hukukumuzdaki Yeri", Dicle Üniversitesi Hukuk Fakültesi Dergisi, 2010–2011, s. 89 vd.; M. İkizler, "Avrupa Haksız Fiil Hukuku İlkelerinde Tehlike Sorumluluğu ve Türk Hukuku ile Kısaca Karşılaştırılması", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 16, Özel Sayı, 2014, s. 3241–3260. İşleten kurtuluş kanıtı getiremez; ancak illiyet bağını kesen sebepleri ispatlayarak sorumluluktan kurtulabilir.

[20]Krş. S. Saraç, Türk Borçlar Kanunu'nda Tehlike Sorumluluğu ve Denkleştirme (TBK m. 71), Yüksek Lisans Tezi, İstanbul Üniversitesi, 2012.

[21]P. Çavuşoğlu Işıntan, "Türk Borçlar Kanunu Tasarısında Yer Alan Haksız Fiillerde Teselsül Düzenlemesi Üzerine Düşünceler", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Erden Kuntalp'e Armağan, 2004/1, s. 499 vd. TBK m. 61–62 uyarınca birden çok kişinin sorumluluğunda her biri zararın tamamından müteselsilen sorumludur.

VI. Yönetim Kurulunun Gözetim Yükümlülüğü ve Sözleşmesel Risk Tahsisi

Siber dayanıklılık, artık bilgi işlem biriminin değil, kurumsal yönetişimin konusudur. TTK m. 369, yönetim kurulu üyelerine tedbirli bir yöneticinin özenini gösterme yükümü yüklemektedir. TTK m. 553 ise bu yükümlülüklerin kusurla ihlali hâlinde hukuki sorumluluk öngörmektedir.[22] Buna göre yönetim kurulu, şirket faaliyetlerinin güvenli yürütülmesini sağlayacak siber risk yönetimi organizasyonunu kurmak ve gözetmekle yükümlüdür. Sorumluluğun sınırı, m. 553/III uyarınca üyenin kontrolü dışındaki hukuka aykırılıklardır. Görevin özenle ve uygun kişilere devri ile gözetim mekanizmalarının kurulmuş olması, savunmanın eksenini oluşturmaktadır.[23]

7545 sayılı Kanun'un hesap verebilirlik ilkesi ve NIS2'nin siber güvenliği doğrudan yönetim organı seviyesinde ele alan yaklaşımı, TTK m. 369–553 ekseninde zaten mevcut olan gözetim yükümlülüğünü güçlendirmektedir. Çok failli yapılarda yönetim kurulu üyeleri arasındaki sorumluluğun farklılaştırılmış teselsül (TTK m. 557) ilkesiyle bireyselleştirilmesi de ayrıca dikkate alınmalıdır.[24]

Sözleşmesel düzlemde risk tahsisi kritik önemdedir. EPC, O&M, bakım ve teknoloji tedarik sözleşmelerinde IEC 62443 uyumu, uzaktan erişim güvenliği, yama yönetimi ve olay bildirim yükümlülükleri açıkça düzenlenmeli ve bu yükümlerin ihlali sözleşmeye aykırılık olarak kurgulanmalıdır. Ancak sorumsuzluk kayıtlarının sınırı gözetilmelidir.

[22]M. Topaloğlu, "Anonim Şirket Yönetim Kurulu Üyelerinin Hukuki Sorumluluğu", Hukuki Sorumluluk Uluslararası Konferansı tebliği, 2019. TTK m. 553/I sorumluluğu kusur esasına bağlamaktadır; özen yükümü TTK m. 369'daki "tedbirli bir yöneticinin özeni" ölçütüyle somutlaşmaktadır; m. 553/III uyarınca hiç kimse kontrolü dışındaki hukuka aykırılıklardan sorumlu tutulamaz.

[23]Krş. O. Okay, Anonim Şirket Yönetim Kurulu Üyelerinin Özen Borcundan Doğan Hukuki Sorumluluğunun Sınırlanması, Yüksek Lisans Tezi, Ankara Üniversitesi, 2008.

[24]Krş. Y. Yördem, Anonim Şirket Yönetim Kurulu Üyelerinin Hukuki Sorumluluğunda Farklılaştırılmış Teselsül İlkesi (TTK m. 557), Doktora Tezi, Selçuk Üniversitesi, 2014.

TBK m. 116/III uyarınca, sorumluluğun kanun veya yetkili makamca verilen bir imtiyazın icrasından doğduğu hâllerde sorumsuzluk anlaşması geçersizdir.[25] Enerji faaliyetlerinin büyük bölümü lisans ve imtiyaz rejimine tabi olduğundan, bu istisna enerji sözleşmelerinde sorumluluğu sözleşmeyle bertaraf etme imkânını önemli ölçüde daraltmaktadır. Kurumsal raporlama ve gözetim yükümlülüklerinin genişlemesi de bu eğilimi pekiştirmektedir.[26]

VII. Sektörel Risk Haritası

Enerji alt sektörleri tek bir özen standardına değil, farklı tipik tehlike profillerine sahiptir ve her birinde ağırlık taşıyan sorumluluk ekseni de değişmektedir. Aşağıdaki değerlendirme, sektörleri taşıdıkları hukuki risk ağırlığına göre üç grupta ele almaktadır.

Birinci grubu, elektrik iletim sistemi, doğal gaz iletim hatları, LNG terminalleri ve rafineriler gibi yüksek tipik tehlike taşıyan iletim ve işleme altyapıları oluşturmaktadır. Bu varlıklarda RTU/SCADA üzerinden kesici açma, basınç ve vana parametrelerinin manipülasyonu ya da proses ve güvenlik sistemlerine (SIS) müdahale; geniş çaplı kesinti, patlama, yangın, toksik salım ve can kaybı gibi sonuçlar doğurabilir. Hukuki ağırlık TBK m. 71 tehlike sorumluluğu ekseninde toplanmakta ve buna çevre sorumluluğu ile iş sağlığı ve güvenliği boyutları eklenmektedir. Sigorta açısından bu grup, düşük frekanslı ve yüksek şiddetli risk profili nedeniyle fiziksel hasar istisnası ve reasürans kapasitesi sorunlarıyla karşı karşıyadır.

[25]Ö. O. Meral, "Türk Borçlar Kanunu ve Türk Medeni Kanunu Kapsamında Sorumsuzluk Anlaşmalarının Geçerliliği"; E. Rüzgar, "İfa Yardımcısının Sorumluluğunu Kaldıran Sorumsuzluk Anlaşmaları". TBK m. 116/III uyarınca, alacaklının borçlunun hizmetinde olması veya sorumluluğun kanun ya da yetkili makamca verilen bir imtiyazın icrasından doğması hâlinde sorumsuzluk kaydı geçersizdir.
[26]E. Rüzgar, "Sürdürülebilirlik Raporlaması: Hukuki Niteliği, Finansal Önemliliği ve Denetimi", İstanbul Barosu Dergisi, s. 165 vd.

İkinci grubu, kamu hizmeti sürekliliği ve organizasyon kusuru ağırlıklı olan elektrik üretim ve dağıtım altyapıları oluşturmaktadır. Üretim tesislerinde türbin veya jeneratör kontrolünün ya da koruma rölelerinin manipülasyonu, ekipman tahribine ve üretim taahhüdünün ihlaline yol açmaktadır. Dağıtım sisteminde kesici ve şalt yönetiminin ele geçirilmesi ise abonelerde kesintiye ve üçüncü kişi zararlarına neden olmaktadır. Burada ağırlık, TBK m. 49 ve m. 66/III organizasyon kusuru ile üretim ve tedarik taahhütlerinin ihlalindedir. Sigorta düzleminde ise makine kırılması ile siber teminatın çakışması ve toplu tüketici tazminat talepleri öne çıkmaktadır.

Üçüncü grubu, tedarik zinciri ve yeni risk sınıfları ağırlıklı olan yenilenebilir santraller, depolamalı enerji tesisleri (BESS) ve akıllı şebekeler oluşturmaktadır. Yenilenebilir santrallerde uzaktan izleme ve OEM erişimi açıkları, depolama tesislerinde batarya ve enerji yönetim sistemlerinin (BMS/EMS) manipülasyonu ile termal kaçış riski, akıllı şebekelerde ise sayaç ve IoT cihazlarının oluşturduğu geniş saldırı yüzeyi belirleyicidir. Hukuki ağırlık TBK m. 116 tedarik zinciri sorumluluğu ile m. 66/III'tedir ve sorun, kişisel veri boyutuyla KVKK ile kesişmektedir. Sigorta ve finansman açısından bu grup, sınırlı aktüeryal veri, kümül risk yoğunlaşması ve OEM/O&M risk tahsisi nedeniyle finanse edilebilirlik değerlendirmesinde özel dikkat gerektirmektedir.

Bu tasnifin pratik sonucu, hem sigorta programının hem de sözleşmesel risk tahsisinin alt sektöre göre farklılaştırılması gereğidir. Tehlike sorumluluğu ağırlıklı varlıklarda öncelik, fiziksel hasar teminatı ve illiyet savunmasıdır. Organizasyon kusuru ağırlıklı varlıklarda kontrol başlıklarına uyumun belgelenmesi, tedarik zinciri ağırlıklı varlıklarda ise üçüncü taraf yükümlülüklerinin sözleşmeyle netleştirilmesi önceliklidir.

VIII. Sigorta ve Proje Finansmanı Boyutu

1. Siber Riskin Sigortalanabilirliği ve Fiziksel Hasar Sorunu

Enerji sektöründe siber olayların fiziksel hasara dönüşebilmesi, sigorta hukuku bakımından bir teminat çakışması ve boşluğu sorunu yaratmaktadır. Bir siber olay sonucu türbin hasarı, trafo arızası veya üretim kaybı meydana geldiğinde, bunun siber risk, makine kırılması, elektronik ekipman, iş durması (business interruption) veya fiziksel hasar teminatlarından hangisine gireceği çoğu zaman açık değildir. Uygulamada siber poliçelerin önemli bir kısmı, siber kaynaklı fiziksel hasarları ve gerekli güvenlik önlemleri alınmadığında doğan kayıpları kapsam dışı bırakmaktadır. Bazı poliçeler ise ISO 27001 gibi bir sertifikasyonu ön koşul kılmaktadır.[27] Bu sessiz siber (silent cyber) sorunu nedeniyle, geleneksel mülk/makine poliçeleri ile siber poliçeler arasında zarar görenin tazminatsız kalabileceği bir aralık doğmaktadır.

Buradaki hukuki sonuç çiftedir. Birincisi, yetersiz önlem istisnası doğrudan organizasyon kusuru tartışmasıyla örtüşmektedir. Makul özeni göstermeyen işletmeci hem sorumlulukla hem de teminat kaybıyla karşılaşmaktadır. İkincisi, enerji şirketlerinin sigorta programları kurgulanırken OT/SCADA kaynaklı risklerin ayrıca değerlendirilmesi ve teminat boşluklarının fiziksel hasar genişletmeleriyle kapatılması gerekmektedir.

2. İş Durması Zararları

Enerji tesislerinde asıl zarar çoğu kez fiziksel hasardan değil, faaliyetin durmasından kaynaklanmaktadır. İş durması (BI) ve bağımlı iş durması (contingent BI, tedarikçi kaynaklı) teminatlarının siber tetikleyicileri açıkça kapsayıp kapsamadığı, bekleme süreleri ve azami tazminat süresi gibi koşullar, gerçek zararı karşılama kapasitesini belirlemektedir. Colonial Pipeline örneği, fiziksel hasar olmaksızın dahi faaliyetin günlerce durabileceğini göstermiştir.

[27]S. Polat, “Siber Riskler ve Siber Sigortalar”, Bankasürans Türkiye, 21 Mart 2025, https://bankasurans.com.tr/siber-riskler-ve-siber-sigortalar/. Yazıda, siber saldırıların neden olduğu fiziksel hasarların ve gerekli güvenlik önlemlerinin (örn. ISO 27001) alınmadığı hâllerde doğan kayıpların poliçelerce genellikle kapsam dışı bırakıldığı belirtilmektedir.

3. EPC/O&M Sözleşmelerinde Risk Tahsisi ve Finanse Edilebilirlik

Proje finansmanında kreditörler, geçmişte ağırlıklı olarak lisans durumu, arazi hakları, EPC yapısı ve gelir modeline odaklanmaktaydı. Bugün siber dayanıklılık, finanse edilebilirlik (bankability) değerlendirmesinin bir bileşeni hâline gelmiştir. Kritik kontrol sistemlerinin korunması, üçüncü taraf erişimlerinin yönetimi, olay müdahale planları ve uluslararası standartlara uyum, kredi incelemesinin (due diligence) kapsamındadır. Finansörler tipik olarak IEC 62443 ve Yönetmelik uyumunu temsil ve taahhütlerle (representations & warranties), olay bildirimini bilgi yükümlülükleriyle ve asgari sigorta teminatını kredi sözleşmesinin ön koşullarıyla güvence altına almaya yönelmektedir.

Risk tahsisi açısından EPC ve O&M sözleşmeleri, siber yükümlülükleri net biçimde dağıtmalıdır. Gecikme ve performans cezaları, kabul testlerine güvenlik kriterlerinin eklenmesi ve geri-besleme (step-in) hakları siber senaryoları da kapsamalıdır. Aksi hâlde, TBK m. 116 ve m. 61–62 uyarınca enerji şirketi üçüncü kişilere karşı ilk muhatap olurken, iç ilişkide rücu imkânı sözleşmesel boşluk nedeniyle zayıflamaktadır.

IX. Değerlendirme

7545 sayılı Kanun'un yürürlüğe girmesiyle, daha önce yalnızca genel sorumluluk hükümleri ve sektörel yönetmelik üzerinden karşılanan siber risk artık çatı bir kanuni zemine kavuşmuştur. Bununla birlikte enerji sektörüne özgü bazı boşluklar varlığını sürdürmekte ve birkaç düzenleyici adımı gerekli kılmaktadır.

İlk mesele, rejimler arasındaki koordinasyondur. 7545 sayılı Kanun kapsamındaki Siber Güvenlik Başkanlığı bildirim ve denetim rejimi ile EPDK Yetkinlik Modeli rejiminin kapsam, bildirim ve denetim bakımından uyumlaştırılması, mükerrer bildirim ve çifte denetim yükünün önlenmesi ve yetki sınırlarının netleştirilmesi gerekmektedir.

İkinci mesele, idari yaptırım ile özel hukuk sorumluluğu arasındaki ilişkidir. Kanun'un öngördüğü idari para cezalarının, zarar gören üçüncü kişilerin tazminat talepleri ile kusur ve organizasyon kusuru değerlendirmesi bakımından taşıyacağı delil değeri, doktrin ve içtihatla açıklığa kavuşturulmalıdır.

Üçüncü boşluk, tehlike sorumluluğunun sınırlarına ilişkindir. Hangi enerji varlıklarının TBK m. 71 anlamında önemli ölçüde tehlike arz eden işletme sayılacağı, siber kaynaklı zararları da kapsayacak biçimde netleştirilmelidir. Dördüncü olarak, sigortalanabilirlik altyapısı geliştirilmelidir; siber kaynaklı fiziksel hasar ve iş durması için standart teminat tanımları oluşturulmalı, sessiz siber boşluğu giderilmeli ve enerjiye özgü teminat modelleri tartışılmalıdır.

Son olarak, tedarik zinciri güvenliği bakımından OEM ve uzaktan erişim hizmetlerine ilişkin asgari sözleşmesel güvenlik şartları sektörel tip sözleşme ve kılavuzlarla standartlaştırılmalıdır. Yönetişim düzleminde ise yönetim kurulu düzeyindeki siber risk gözetimi, TTK m. 369 ve 553 ile uyumlu biçimde, raporlama ve iç kontrol yükümlülükleri içine açıkça yerleştirilmelidir.

X. Sonuç

SCADA ve endüstriyel kontrol sistemleri artık yalnızca mühendislik altyapısının değil, enerji arz güvenliğinin, çevresel güvenliğin ve işletme sürekliliğinin taşıyıcısıdır. Stuxnet'ten Colonial Pipeline'a uzanan çizgi, siber riskin bir veri güvenliği problemi olmaktan çıkıp fiziksel hasara, çevresel zarara ve arz kesintilerine yol açan bir sorumluluk kaynağına dönüştüğünü göstermiştir.

Bu çerçevede enerji şirketinden beklenen yükümlülük, yalnızca saldırıyı önlemek değil; saldırı altında güvenli biçimde faaliyetini sürdürebilen ve hızla toparlanabilen bir siber dayanıklılık seviyesine ulaşmaktır. Türk hukukunda bu beklenti, TBK'nin haksız fiil, organizasyon, ifa yardımcısı ve tehlike sorumluluğu hükümleri ile TTK'nin yönetim kurulu sorumluluğu rejimi üzerinden temellendirilebilir. 7545 sayılı Siber Güvenlik Kanunu, EPDK Yetkinlik Modeli Yönetmeliği, IEC 62443 ve NIS2 ise bu yükümlülüğün içeriğini somutlaştırmakta ve kısmen yasal yaptırıma bağlamaktadır.

Önümüzdeki dönemde enerji sektöründe doğacak uyuşmazlıkların eksenini, siber saldırının nasıl gerçekleştiği değil, enerji şirketinin kendisinden beklenen makul güvenlik ve siber dayanıklılık standardını sağlayıp sağlamadığı oluşturacaktır. Siber dayanıklılık; sorumluluk hukuku, sigortalanabilirlik ve finanse edilebilirlik boyutlarıyla, enerji hukukunun önümüzdeki on yıldaki en belirleyici gelişim alanlarından biri olmaya adaydır. Bu nedenle enerji şirketleri, yatırımcılar, finansörler ve sigortacılar için doğru strateji, bu standardı bir uyum yükü olarak değil, hukuki ve ticari riskin yönetim aracı olarak içselleştirmektir.

Kaynakça

- Çavuşoğlu Işıntan, P., "Türk Borçlar Kanunu Tasarısında Yer Alan Haksız Fiillerde Teselsül Düzenlemesi Üzerine Düşünceler", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Erden Kuntalp'e Armağan, 2004/1, s. 499 vd.
- Deniz, D., "Adam Çalıştıranın Sorumluluğu Bakımından Nedensellik Bağı Unsuru", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C. XVIII, 2021/2, s. 1155–1176.
- Directive (EU) 2022/2555 (NIS2 Directive).
- Dragos Inc., CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations, 2017.
- Durak, Y., "Tehlike Sorumluluğu", Erciyes Üniversitesi Hukuk Fakültesi Dergisi, C. IX, S. 1, 2014.
- Erdoğan, İ., "Haksız Fiilde Kusurlu Sorumluluk ve Özellikle Kusur Unsuru", Selçuk Üniversitesi Hukuk Fakültesi Dergisi.
- ESET, Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet, 2017.
- FireEye/Mandiant, TRITON Malware Analysis Report, 2017.
- Gültekin, F., "Yardımcı Kişinin Fiillerinden Borçlunun Sorumluluğu", Türkiye Adalet Akademisi Dergisi, Yıl 9, S. 35, 2018, s. 373 vd.
- IEC 62443 Standards Series (Industrial communication networks – Network and system security).
- İkizler, M., "Avrupa Haksız Fiil Hukuku İlkelerinde Tehlike Sorumluluğu ve Türk Hukuku ile Kısaca Karşılaştırılması", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 16, Özel Sayı, 2014, s. 3241–3260.
- Korkusuz, M. H., "Tehlike Sorumluluğunun Hukukumuzdaki Yeri", Dicle Üniversitesi Hukuk Fakültesi Dergisi, 2010–2011.
- Langner, R., "Stuxnet: Dissecting a Cyberwarfare Weapon", IEEE Security & Privacy, 2011.
- Meral, Ö. O., "Türk Borçlar Kanunu ve Türk Medeni Kanunu Kapsamında Sorumsuzluk Anlaşmalarının Geçerliliği".
- Okay, O., Anonim Şirket Yönetim Kurulu Üyelerinin Özen Borcundan Doğan Hukuki Sorumluluğunun Sınırlanması, YL Tezi, Ankara Üniversitesi, 2008.
- Polat, S., "Siber Riskler ve Siber Sigortalar", Bankasürans Türkiye, 21 Mart 2025.
- Rüzgar, E., "İfa Yardımcısının Sorumluluğunu Kaldıran Sorumsuzluk Anlaşmaları".
- Rüzgar, E., "Sürdürülebilirlik Raporlaması: Hukuki Niteliği, Finansal Önemliliği ve Denetimi", İstanbul Barosu Dergisi.
- SANS ICS & E-ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid, 2016.
- Saraç, S., Türk Borçlar Kanunu'nda Tehlike Sorumluluğu ve Denkleştirme (TBK m. 71), YL Tezi, İstanbul Üniversitesi, 2012.
- Topaloğlu, M., "Anonim Şirket Yönetim Kurulu Üyelerinin Hukuki Sorumluluğu", Hukuki Sorumluluk Uluslararası Konferansı (tebliğ), 2019.

- Türkmen, A., “6098 Sayılı Türk Borçlar Kanununa Göre Organizasyon Sorumluluğu (TBK m. 66/III)”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. LXX, S. 2, 2012, s. 257–284.
- U.S. Department of Homeland Security / ICS-CERT, Cyber-Attack Against Ukrainian Critical Infrastructure (IR-ALERT-H-16-056-01), 2016.
- Yördem, Y., Anonim Şirket Yönetim Kurulu Üyelerinin Hukuki Sorumluluğunda Farklılaştırılmış Teselsül İlkesi, Doktora Tezi, Selçuk Üniversitesi, 2014.
- Yünlü, S., Yardımcı Kişilerin Fiillerinden Sorumluluk, 2018.

BOSCA
LAW

Tekstilciler Cad. No: 33/5-8
Balgat, Çankaya / ANKARA
Tel: +90 312 473 95 70 (Pbx)
E-posta: info@bosca.av.tr