TAÜHFD, 2025; 7(2): 435-501
Araştırma Makalesi
Forschungsartikel

Makale Başvuru Tarihi: 24.09.2025
Makale Kabul Tarihi: 01.12.2025
DOI: 10.59933/tauhfd.1851344

Siber Güvenlik Alanında Paralel Bildirim Yükümlülüklerinin Hukuki Çerçevesi: Eşgüdümlü Yönetişim Modeli Önerisi

Der rechtliche Rahmen paralleler Meldepflichten in der Cybersicherheit: Ein Modellvorschlag zur koordinierten Governance

Dr. M. Furkan Akıncı*

ÖZ

Türkiye'de siber güvenlik alanındaki bildirim yükümlülükleri, Siber Güvenlik Başkanlığı Kanunu'nun yürürlüğe girmesiyle yeni bir evreye girmiştir. Ancak mevcut sektörel bildirim rejimleri (BTK, BDDK, SPK, EPDK, SHGM) varlığını sürdürmekte, bu durum paralel ve çakışan yükümlülükler ortaya çıkarmaktadır. Bu çalışma, çok-merkezli bildirim mimarisinin teorik temellerini risk yönetişimi ve merkezsiz regülasyon literatürü çerçevesinde incelemekte, Türkiye'deki mevcut durumu haritalandırmakta ve Avrupa Birliği'ndeki NIS2, DORA, CRA gibi düzenlemelerle karşılaştırmalı analiz sunmaktadır. Makale, farklı kurumların eşzamanlı bildirim taleplerinin oluşturduğu mükerrerlik, uyum maliyetleri ve koordinasyon eksikliğinden kaynaklanan sorunları tespit etmektedir. AB'nin NIS2 Uygulama Tüzüğü'nde standardize edilen şablon ve süre yaklaşımları, DORA'nın EU Hub modeli ve CRA'nın ENISA tek platform çözümü, Türkiye için model teşkil edebilecek örneklerdir. Çalışma, tek giriş-çok çıkış prensibiyle işleyen, ortak veri sözlüğü kullanan ve risk temelli kademeli raporlama sunan eşgüdümlü bir bildirim çerçevesi önermektedir. Bu model, sektörel uzmanlığı korurken mükerrer raporlamayı azaltacak, hukuki öngörülebilirliği artıracak ve siber risk yönetişiminde etkinlik-yük dengesini optimize edecektir.

* Boğaziçi Üniversitesi Hukuk Fakültesi, Bilişim Hukuku Anabilim Dalı, (muhammedfurkan.akinci@bogazici.edu.tr), ORCID: 0009-0007-5851-1128.

Anahtar Kelimeler: *Siber güvenlik hukuku, paralel yükümlülükler, risk yönetişimi, NIS2, siber güvenlik kanunu, eşgüdümlü bildirim, meta-regülasyon, çok-merkezli yönetişim*

Legal Framework of Parallel Notification Obligations in Cybersecurity: A Coordinated Governance Model Proposal

ABSTRACT

Turkey's cybersecurity notification obligations have entered a new phase with the enactment of the Cybersecurity Presidency Law. However, existing sectoral notification regimes (BTK, BDDK, SPK, EPDK, SHGM) continue to operate, creating parallel and overlapping obligations. This study examines the theoretical foundations of polycentric notification architecture within the framework of risk governance and decentered regulation literature, maps the current situation in Turkey, and provides comparative analysis with European Union regulations such as NIS2, DORA, and CRA. The research identifies problems arising from duplication caused by simultaneous notification requests from different authorities, compliance costs, and lack of coordination. The standardized template and timeline approaches in the EU's NIS2 Regulation, DORA's EU Hub model, and CRA's ENISA single platform solution provide exemplary models for Turkey. The study proposes a coordinated notification framework operating on a single-entry-multiple-exit principle, utilizing a common data dictionary, and offering risk-based tiered reporting. This model would preserve sectoral expertise while reducing duplicate reporting, enhance legal predictability, and optimize the efficiency-burden balance in cyber risk governance.

Keywords: *Cybersecurity law, parallel obligations, risk governance, NIS2, CSA, coordinated notification, meta-regulation, polycentric governance*

I. Giriş

Siber güvenlik, yirmi birinci yüzyılın en kritik yönetişim alanlarından biri haline gelmiştir. Dijital dönüşümün hızlanması, kritik altyapıların birbirine bağımlılığının artması ve siber tehditlerin sofistikasyonu, geleneksel düzenleme paradigmalarını zorlamaktadır.[1] Tek bir siber güvenlik olayı, finansal sistemden enerji sektörüne, sağlık hizmetlerinden kamu yönetimine kadar çok sayıda alanı eşzamanlı olarak etkileyebilmektedir. Bu çok boyutlu etki, doğal olarak farklı düzenleyici otoritelerin müdahale alanına girmekte ve paralel yükümlülükleri tetiklemektedir.

Modern düzenleme teorisi, son otuz yılda köklü bir dönüşüm geçirmiştir. Yirminci yüzyılın ortalarında hâkim olan komut-kontrol yaklaşımı, devletin merkezi otoritesine dayanan, yukarıdan aşağıya doğru işleyen ve önceden belirlenmiş kuralların katı uygulamasını öngören bir düzenleme mantığını yansıtmaktaydı.[2] Bu klasik model, düzenleyici otoritenin tüm riskleri öngörebileceği, detaylı kurallar koyabileceği ve bunların uygulanmasını etkin şekilde denetleyebileceği varsayımına dayanıyordu. Sanayi toplumunun nispeten öngörülebilir risk profili ve sınırlı teknolojik karmaşıklığı, bu yaklaşımın belirli bir dönem işlevsel olmasını sağlamıştı.[3]

Ancak yirminci yüzyılın son çeyreğinden itibaren risk kavramının kendisi dönüşüme uğradı. Niklas Luhmann'ın sistem teorisi perspektifinden geliştirdiği risk analizi, modern toplumlarda riskin artık dışsal bir tehlike olmaktan çıkıp, sistemin kendi kararlarının bir sonucu

---

1 Mehmet Bedii Kaya, "Siber Güvenlik Hukuku", *Dijital Baskı*, (ts.), 10.

2 Robert Baldwin vd., *Understanding Regulation: Theory, Strategy, and Practice* (New York: Oxford University Press, 2012), 106-112; Karen Yeung - Sofia Ranchordás, *An Introduction to Law and Regulation: Text and Materials* (Cambridge, UK ; New York: Cambridge University Press, 2024), 169; K.P.V. O'Sullivan - Darragh Flannery, "A Discussion on the Resilience of Command and Control Regulation within Regulatory Behavior Theories", *Journal of Governance and Regulation* 1/1 (2012), 15-24.

3 Ian Ayres - John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992), 26-27;110-112.

haline geldiğini ortaya koymuştur.[4] Luhmann'a göre risk ve tehlike arasındaki temel ayrım, tehlikenin çevresel faktörlerden kaynaklanması, riskin sistemin kendi gözlem ve kararlarından doğmasıdır. Modern sistemler karmaşıklıklarını azaltmak için sürekli seçimler yapmak zorundadır ve her seçim yeni risk alanları oluşturmaktadır. Bu perspektif, riskin modern toplumda kaçınılmaz olduğunu, çünkü her karar alma sürecinin aynı zamanda bir risk üretimi süreci olduğunu göstermektedir.[5] Luhmann'ın analizi, belirsizliğin sistemin dışında değil, içinde olduğunu ve düzenleme mekanizmalarının bu içsel belirsizlikle başa çıkması gerektiğini vurgulamaktadır.[6]

Ulrich Beck'in risk toplumu tezi ise, Luhmann'ın sistem teorik yaklaşımını toplumsal dönüşüm bağlamında genişletmektedir.[7] Beck'e göre sanayi modernleşmesinin ortaya çıkardığı riskler, artık sanayi toplumunun kurumsal yapıları tarafından kontrol edilemez hale gelmiştir. Risk toplumu kavramı, zenginliğin üretimi ve dağıtımı mantığının yerini, risklerin üretimi ve dağıtımı mantığının aldığı yeni bir toplumsal formasyonu ifade etmektedir.[8] Beck'in analizinde modern risklerin beş kritik özelliği öne çıkar: Birincisi, bu riskler mekânsal ve zamansal sınırları aşmaktadır. İkincisi, çoğu zaman algılanamaz niteliktedir ve ancak bilimsel bilgi aracılığıyla görünür hale gelmektedir. Üçüncüsü, potansiyel etkileri geri döndürülemez olabilmektedir. Dördüncüsü, geleneksel sorumluluk ve sigorta sistemlerini aşmaktadır. Beşincisi, demokratik karar alma süreçlerini zorlamaktadır.[9]

---

4 Niklas Luhmann, *Risk: A Sociological Theory*, çev. Rhodes Barrett (Abingdon, Oxon New York, NY: Routledge, Taylor & Francis Group, 2017), 21-23.

5 Luhmann, *Risk*, 28.

6 Luhmann, *Risk*, 27.

7 Ulrich Beck, *Risk Society: Towards a New Modernity* (London: Sage, 2009), 36-38.

8 Beck, *Risk Society*, 19-23; 36-38; Ulrich Beck, *World at Risk* (Polity, 2009), 24-30; 47-50.

9 Beck, *Risk Society*, 24-25; Ulrich Beck vd., *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order* (Stanford University Press, 1994), 8-12.

Çernobil felaketi, Beck'in paradigmatik örneği olarak, bu yeni risk tipinin özelliklerini somutlaştırmaktadır. Radyasyon bulutunun ulusal sınırları tanımaması, etkilerinin nesiller boyu sürebilmesi ve geleneksel risk yönetim mekanizmalarının yetersizliği, risk toplumu tezinin temel argümanlarını doğrular niteliktedir.[10] Beck'in vurguladığı üzere, bu tür riskler karşısında uzman bilgisine olan bağımlılık artarken, paradoksal olarak uzmanlara duyulan güven de aşınmaktadır. Çünkü uzmanlar arasındaki görüş ayrılıkları ve bilimsel belirsizlikler, risk algısını daha da karmaşık hale getirmektedir.[11]

Bu teorik dönüşüm, regülasyon paradigmalarında da köklü değişikliklere yol açmıştır. Komut-kontrol yaklaşımının katı, önceden belirlenmiş kuralları, risk toplumunun belirsizlik ve karmaşıklığı karşısında yetersiz kalmaktadır.[12] Risk temelli regülasyon yaklaşımı, bu yeni gerçekliğe yanıt olarak gelişmiştir. Bu yaklaşımda düzenleme, statik kurallar yerine dinamik süreçlere, kesin yasaklar yerine risk değerlendirmelerine, tek tip standartlar yerine farklılaştırılmış müdahalelere dayanmaktadır.[13] Risk temelli düzenleme, belirsizliğin yönetilemez değil, yönetilmesi gereken bir unsur olduğunu kabul eder ve düzenleme mekanizmalarını bu belirsizlikle başa çıkacak şekilde tasarlar.[14]

Siber güvenlik alanı, bu yeni risk paradigmasının en belirgin örneklerinden birini teşkil etmektedir. Siber risklerin özellikleri, Beck'in tanımladığı modern risk özelliklerini tam anlamıyla yansıtmaktadır: sınır tanımama, görünmezlik, potansiyel felaket etkisi, hızlı yayılma ve

---

10 Beck, *Risk Society*, 7; 23; Klaus Rasborg, *Ulrich Beck: Theorising World Risk Society and Cosmopolitanism* (Cham: Springer International Publishing, 2021), 28-33; Beck, *World at Risk*, 172-173.

11 Beck, *Risk Society*, 29-31; Beck, *World at Risk*, 36–39; 54; 116–117.

12 Ayres - Braithwaite, *Responsive Regulation*, 36-40;110-112; Beck, *World at Risk*, 12.

13 Julia Black - Robert Baldwin, "Really Responsive Risk-Based Regulation", *Law & Policy* 32/2 (15 Mart 2010), 181-213.

14 Christopher Hood vd., *The Government of Risk: Understanding Risk Regulation Regimes* (OUP Oxford, 2001), 23-27;177-179;178-191.

geleneksel sorumluluk mekanizmalarını aşma.[15] Bir siber saldırı milisaniyeler içinde küresel ölçekte yayılabilir, kritik altyapıları felç edebilir ve domino etkisiyle beklenmedik sektörleri etkileyebilir. *WannaCry* ve *NotPetya* saldırıları, siber risklerin bu sistemik karakterini açık şekilde göstermiştir.[16]

Türkiye'de 7545 sayılı Siber Güvenlik Kanunu'nun yürürlüğe girmesi,[17] ulusal siber güvenlik yönetişiminde yeni bir dönem başlatmıştır. Kanun, Siber Güvenlik Başkanlığı'na (SGB) usul ve esas belirleme, bildirimleri alma ve koordinasyon sağlama konularında geniş yetkiler tanımaktadır. Ancak bu yeni kurumsal yapının oluşturulması, mevcut sektörel bildirim rejimlerinin ortadan kalkması anlamına gelmemektedir. Bilgi Teknolojileri ve İletişim Kurumu, Bankacılık Düzenleme ve Denetleme Kurumu, Sermaye Piyasası Kurulu, Enerji Piyasası Düzenleme Kurumu veya Sivil Havacılık Genel Müdürlüğü gibi sektörel düzenleyici kurumlar, kendi özel mevzuatları kapsamında siber olay bildirim sistemlerini sürdürmektedir.[18]

Bu durum, aynı siber güvenlik olayı için birden fazla kuruma, farklı süre ve formatlarda bildirim yapılması zorunluluğunu doğurmaktadır. Bir *ransomware* saldırısı düşünelim: bu olay, operasyonel açıdan Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) bildirilmesi gereken bir şebeke güvenliği ihlali, kişisel veriler etkilenmişse Kişisel Verileri Koruma Kurulu'na (KVKK) bildirilmesi gereken bir veri ihlali, finansal kuruluşlarda Bankacılık Düzenleme ve Denetleme Kurumu'na (BDDK) raporlanması gereken bir operasyonel

---

15 Ronald J. Deibert - Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security", *International Political Sociology* 4/1 (01 Mart 2010), 16-18.

16 Daha detaylı analiz için bkz. Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019).

17 7545 sayılı Siber Güvenlik Kanunu, RG: 19.03.2025-32846.

18 BTK Şebeke ve Bilgi Güvenliği Yönetmeliği, RG: 13.07.2014-29059; BDDK Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, RG: 15.03.2020-31069; SPK VII-128.10 sayılı Bilgi Sistemleri Yönetimi Tebliği, RG: 13.03.2025-32840.

risk olayı ve halka açık şirketlerde SPK üzerinden kamuya açıklanması gereken bir bilgi niteliğinde olabilir. Her bir kurum, kendi perspektifinden olayı değerlendirmekte ve farklı bildirim süreleri, formatları ve eşikleri uygulamaktadır.

Paralel bildirim mimarisi, bir yandan farklı kurumların uzmanlık ve hızlı müdahale kapasitelerinden yararlanma imkânı sunarken, diğer yandan koordinasyon maliyetleri, bilgi parçalanması ve uyum yükü ortaya çıkarmaktadır.[19] Bu durum, risk toplumu bağlamında regülasyon teorisinin temel sorularından birini gündeme getirmektedir: Belirsizlik ve karmaşıklığın hâkim olduğu bir ortamda, çok merkezli düzenleme mimarisi nasıl optimize edilebilir?

Avrupa Birliği'nde benzer sorunlara yönelik çözüm arayışları önemli dersler sunmaktadır. Ağ ve Bilgi Sistemleri Güvenliği Direktifi 2'nin (Network and Information Security Directive 2 - NIS2) ve özellikle 2024/2690 sayılı Uygulama Tüzüğü'nün getirdiği standardizasyon,[20] Dijital Operasyonel Dayanıklılık Yasası'nın (Digital Operational Resilience Act - DORA) finansal sektör için öngördüğü konsolide yaklaşım[21] ve Siber Dayanıklılık Yasası'nın (Cyber Resilience Act - CRA) Avrupa Birliği Siber Güvenlik Ajansı (European Union Agency for Cybersecurity - ENISA) üzerinden tek platform modeli,[22] paralel bildirim sorununa sistematik çözümler geliştirmektedir. Bu düzenlemeler, sektörel uzmanlığı korurken mükerrer raporlamayı azaltmayı hedefleyen hibrit modeller önermektedir.

Bu çalışmanın temel araştırma sorusu şudur: Çok merkezli ve çok kanallı bildirim mimarisi, siber risk yönetişiminde etkinlik-yük

---

19 Elinor Ostrom, "Beyond Markets and States: Polycentric Governance of Complex Economic Systems", *The American Economic Review* 100/3 (2010), 641–645, 652–653, 655, 665.

20 Commission Implementing Regulation (EU) 2024/2690 laying down rules for the application of Directive (EU) 2022/2555, OJ L, 2024/2690, 18.10.2024.

21 Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA), OJ L 333, 27.12.2022.

22 Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024.

dengesi açısından nasıl optimize edilebilir? Bu soruyu yanıtlamak için, düzenleme teorisinin sunduğu kavramsal araçlardan yararlanarak, Türkiye'deki siber güvenlik bildirim sisteminin optimal tasarımı için analitik bir çerçeve geliştirilecektir.

Çalışmanın ikinci bölümünde, merkezsiz regülasyon, çok merkezli yönetişim ve meta-regülasyon teorileri çerçevesinde paralel yükümlülüklerin teorik temelleri derinlemesine incelenecektir. Üçüncü bölüm, Türkiye'deki mevcut rejimini kapsamlı bir şekilde haritalandırarak, sektörel düzenleyicilerin siber güvenlik mekanizmalarını ve bunların kesişim noktalarını analiz edecektir. Dördüncü bölümde, paralel siber güvenlik rejimlerinin avantaj ve dezavantajları, Avrupa Birliği deneyimi ile karşılaştırmalı olarak değerlendirilecektir. Beşinci bölüm, meta-regülasyon ilkeleri ışığında, tek giriş-çok çıkış prensibiyle işleyen eşgüdümlü bir siber güvenlik olay bildirim çerçevesi önerisi sunacaktır. Sonuç bölümünde ise, önerilen modelin uygulanabilirliği ve politika önerileri tartışılacaktır.

II. Teorik Çerçeve

Paralel siber güvenlik yükümlülüklerinin analizi, geleneksel regülasyon teorisinin sunduğu kavramsal araçların ötesine geçmeyi gerektirmektedir. Bir siber güvenlik olayı, aynı anda birden fazla düzenleyici kurumun yetki alanına girebilmekte ve her kurum kendi mevzuatı çerçevesinde farklı yükümlülükler öngörebilmektedir. Bu yükümlülükler, bildirim zorunluluğundan risk yönetim sistemleri kurma mecburiyetine, sürekli denetim raporlamasından olay sonrası iyileştirme planı sunma gerekliliğine kadar geniş bir yelpazede ortaya çıkmaktadır. Bu makalenin odağı, bu geniş yükümlülük yelpazesi içinde bildirim yükümlülüklerinin çakışması ve eşgüdümüdür. Ancak bildirim yükümlülüklerinin anlaşılması, daha genel paralel yükümlülükler olgusunun teorik temellerinin incelenmesini gerektirmektedir.[23]

---

[23] Julia Black, "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World", *Current Legal Problems* 54/1 (01 Ocak 2001), 104-106; Julia Black, "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes", *Regulation & Governance* 2/2 (2008), 137-139.

Bu makalenin temel iddiası, paralel yükümlülüklerin anlaşılabilmesi için üç birbiriyle ilişkili teorik perspektifin entegre edilmesi gerektiğidir. İlk olarak, siber risklerin niteliği ve bunların düzenleme paradigmasında oluşturduğu dönüşüm incelenmelidir; zira paralel yükümlülüklerin varlığı, riskin kendisinin çok boyutlu ve parçalı doğasından kaynaklanmaktadır.[24] İkinci olarak, bu çok boyutluluğun kurumsal düzeyde nasıl yansıdığı ve merkezsiz düzenleme yapılarının mantığı açıklanmalıdır.[25] Üçüncü olarak ise merkezsizliğin oluşturduğu koordinasyon sorununa yönelik teorik çözümler tartışılmalıdır.[26] Bu üçlü analitik çerçeve, mevcut bildirim rejiminin neden bu şekilde yapılandığını anlamayı ve optimal tasarım için normatif öneriler geliştirmeyi mümkün kılmaktadır.

A. Risk Toplumunda Siber Güvenlik ve Regülasyon Paradigmasının Dönüşümü

Yirminci yüzyılın son çeyreğinden itibaren düzenleme teorisinde yaşanan paradigma değişimi, piyasa başarısızlıklarının düzeltilmesinden risk yönetimine doğru köklü bir kayma ile karakterize edilebilir. Klasik kamu yararı teorisi, düzenlemenin temel gerekçesini dışsallıklar, doğal tekeller, bilgi asimetrisi ve ölçek ekonomileri gibi piyasa aksaklıklarının düzeltilmesinde görmekteydi.[27] Bu yaklaşım, devletin rasyonel bir aktör olarak piyasa başarısızlıklarını tespit edip

---

[24] Beck, *Risk Society*, 19-38; Luhmann, *Risk*, 21-28; Black - Baldwin, "Really Responsive Risk-Based Regulation", 181-190; Hood vd., *The Government of Risk*, 23-27, 177-179.

[25] Black, "Decentring Regulation", 110-112; L. Hancher - M. Moran, "Organizing Regulatory Space", *A Reader on Regulation*, ed. Robert Baldwin vd. (Oxford University Press, 1998), 153-155.

[26] Ostrom, "Beyond Markets and States", 641-643; Black, "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes", 140-141.

[27] Oliver James, "Regulation Inside Government: Public Interest Justifications and Regulatory Failures", *Public Administration* 78/2 (2000), 330; Coşkun Can Aktan - Serdar Yay, "REGÜLASYON İKTİSADINA GİRİŞ", *Ekonomi Bilimleri Dergisi* 8/1 (31 Aralık 2016), 127-132; Baldwin vd., *Understanding Regulation*, 106-112.

düzelteceği normatif varsayımına dayanıyordu.[28] Ancak 1980'lerden itibaren gelişen kamu tercihi teorisi ve düzenleyici yakalama literatürü bu iyimser yaklaşımı sorgulamış ve düzenlemenin kendi başarısızlıklarını gündeme getirmiştir.[29] Risk temelli düzenleme paradigması, bu eleştirel gelişmenin bir sonucu olarak ortaya çıkmakla birlikte, yalnızca düzenleme başarısızlığına bir yanıt değildir. Daha temel olarak, modern toplumun karşı karşıya olduğu risklerin niteliğindeki dönüşümün bir yansımasıdır.[30]

Üretilmiş belirsizlik kavramı bu dönüşümü kavramsal olarak ifade etmektedir.[31] Geleneksel toplumlar dışsal tehlikelerle karşı karşıyayken, modern toplumlar kendi kararlarından kaynaklanan risklerle yüzleşmektedir.[32] Siber güvenlik bu dinamiğin paradigmatik örneğidir; dijital dönüşüm kararı alan her kurum, aynı zamanda siber saldırı riskini de üretmektedir. Bulut bilişime geçiş operasyonel verimlilik sağlarken veri ihlali riskini artırmakta, nesnelerin interneti teknolojileri yeni hizmetler sunarken saldırı yüzeyini genişletmekte, yapay zekâ sistemleri karar süreçlerini hızlandırırken yeni zafiyet türleri ortaya çıkarmaktadır. Bu risk türü, bilimsel bilginin ilerlemesiyle birlikte artan belirsizlik paradoksunu içermektedir; ne kadar çok bilirsek, bilmediğimiz şeylerin farkına o kadar çok varırız. *Sıfırıncı gün zafiyetleri*[33] bu paradoksun teknik karşılığıdır; güvenlik uzmanları yeni açıklar

---

[28] Hood vd., *The Government of Risk*, 62; James, "Regulation Inside Government", 330.

[29] James, "Regulation Inside Government", 335-337; O'Sullivan - Flannery, "A Discussion on the Resilience of Command and Control Regulation within Regulatory Behavior Theories".

[30] Bridget M. Hutter, *The attractions of risk-based regulation: accounting for the emergence of risk ideas in regulation* (CARR London, 2005), 33/1-3.

[31] Michael Power, *Organized Uncertainty: Designing a World of Risk Management* (Oxford University Press, 2007), 5-6.

[32] Beck, *Risk Society*, 36-38; Anthony Giddens, "Risk and Responsibility", *The Modern Law Review* 62/1 (1999), 1-10.

[33] Sıfırıncı gün (zero-day) zafiyetleri, bir yazılım veya donanımda bulunan ancak üretici ya da geliştirici tarafından henüz tespit edilmemiş veya tespit edilmiş olsa bile henüz yaması yayımlanmamış güvenlik açıklarıdır.

keşfettikçe, henüz bilinmeyen açıkların varlığı ve boyutu hakkındaki belirsizlik de artmaktadır.[34]

Risk toplumu tezi bu analizi daha da ileri götürmektedir. Sanayi modernleşmesinin ortaya çıkardığı riskler, artık sanayi toplumunun kurumsal yapıları tarafından kontrol edilemez hale gelmiştir.[35] Risk toplumu kavramı, zenginliğin üretimi ve dağıtımı mantığının yerini risklerin üretimi ve dağıtımı mantığının aldığı yeni bir toplumsal formasyonu ifade etmektedir.[36] Modern risklerin beş kritik özelliği siber güvenlik alanında paradigmatik bir şekilde somutlaşmaktadır.

İlk olarak bu riskler mekânsal ve zamansal sınırları aşmaktadır. İkinci olarak siber riskler çoğu zaman görünmez ve ancak teknik uzmanlıkla tespit edilebilir niteliktedir. Üçüncü olarak siber risklerin potansiyel etkileri geri döndürülemez olabilmektedir. Dördüncü olarak bu riskler geleneksel sorumluluk ve sigorta sistemlerini aşmaktadır. Beşinci olarak da siber riskler demokratik karar alma süreçlerini zorlamaktadır.

Bu risk profilinin düzenleme teorisi açısından kritik sonucu, geleneksel komut-kontrol modelinin yetersizliğidir.[37] Detaylı teknik standartlar belirleme yaklaşımı, tehdit ortamının sürekli değiştiği bir alanda süratle modası geçen ve katı kurallara dönüşmektedir. Örneğin belirli bir şifreleme algoritmasının veya güvenlik duvarı konfigürasyonu zorunlu kılınması, yeni nesil saldırı tekniklerine karşı etkisiz kalabilmektedir. Gerçekten duyarlı regülasyon yaklaşımı bu yetersizliğe normatif bir yanıt sunmaktadır. Bu yaklaşım, regülasyonun yalnızca düzenlenen tarafın davranışına değil, aynı zamanda düzenleyici ortamın karmaşıklığına, düzenleyici kurumun kapasitesine, düzenlenen endüstrinin kültürüne ve siyasi-sosyal bağlama duyarlı olması

---

34 Kaya, "Siber Güvenlik Hukuku", 25.

35 Beck, *Risk Society*, 19-23.

36 Beck, *World at Risk*, 24-30.

37 Ayres - Braithwaite, *Responsive Regulation*, 26-27, 110-112; O'Sullivan - Flannery, "A Discussion on the Resilience of Command and Control Regulation within Regulatory Behavior Theories", 16-17; Yeung - Ranchordás, *An Introduction to Law and Regulation*, 268-270.

gerektiğini vurgulamaktadır.[38] Risk temelli regülasyon, bu çok boyutlu duyarlılığı operasyonelleştirmenin bir aracı olarak öne çıkmaktadır.[39]

Ancak gerçekten duyarlı regülasyon yaklaşımı normatif bir çerçeve sunmakla birlikte, bu çerçevenin pratikte nasıl işlediği ayrı bir soru teşkil etmektedir. Düzenleyici risk yönetimi analizi tam da bu noktada devreye girmekte ve risk temelli düzenlemenin uygulanmasındaki fiili dinamikleri ortaya koymaktadır.[40] Düzenleyici kurumlar belirsizlik altında karar alırken, risk değerlendirmesi hem teknik bir süreç hem de sosyal bir inşa olmaktadır.[41] Hangi risklerin yüksek sayılacağı yalnızca objektif verilerle değil, kurumsal kültür, politik baskılar ve medya gündeminin etkileşimiyle belirlenmektedir. Örneğin 2017 Equifax veri ihlali sonrasında kişisel veri koruması odaklı düzenleyici kurumlar bildirim yükümlülüklerini sıkılaştırırken, finansal istikrar odaklı kurumlar operasyonel direnç gerekliliklerini güçlendirmiştir.[42] Aynı olay farklı risk perspektifleri üzerinden farklı düzenleyici yanıtlara yol açmıştır.

Risk temelli düzenlemenin paralel siber güvenlik yükümlülükleri açısından doğurduğu sonuç kritiktir. Siber riskin çok boyutlu doğası, her boyutun farklı bir perspektiften değerlendirilmesini gerektirmektedir. Bir *ransomware*[43] saldırısı aynı anda operasyonel bir

---

38 Black, "Decentring Regulation", 105-106.

39 Julia Black, "The Emergence of Risk-Based Regulation and the New Public Risk Management in the United Kingdom", *Public Law*, (2005), 513.

40 Hood vd., *The Government of Risk*, 23-27, 177-179; Power, *Organized Uncertainty*, 48.

41 Power, *Organized Uncertainty*, 13, 195; Robert Baldwin vd., *LSE Research Online Documents on Economics*, "Risk Management and Business Regulation", *LSE Research Online Documents on Economics*, (Ekim 2000), 2-3; Hutter, *The attractions of risk-based regulation*, 33/10-11.

42 *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach* (United State Government Accountability Office, 2018).

43 Ransomware (fidye yazılımı), bir bilgisayar sistemine veya ağa sızarak verileri şifreleyen ya da sisteme erişimi engelleyen ve bu kısıtlamanın

süreklilik sorunu, bir veri koruma ihlali, bir finansal istikrar riski ve bir piyasa bilgisi niteliği taşıyabilmektedir. Örneğin bir bankanın kripto-kilitlenmesi durumunda BDDK operasyonel risk perspektifinden müdahale ederken, KVKK müşteri verilerinin sızıp sızmadığını değerlendirmekte, SPK halka açık bir bankaysa piyasa bilgilendirme zorunluluğunu tetiklemekte ve BTK kritik altyapı kesintisi açısından incelemektedir. Her bir perspektif farklı bir uzmanlık alanını, farklı bir risk değerlendirme metodolojisini ve farklı bir düzenleme mantığını içermektedir. Dolayısıyla paralel yükümlülüklerin varlığı, riskin kendisinin çok boyutlu yapısının kurumsal düzeyde bir yansımasıdır. Bu tespit, teorik analizin ikinci katmanına geçişi gerektirmektedir; çok boyutlu risk nasıl çok merkezli bir düzenleme mimarisine dönüşmektedir ve bu dönüşümün mantığı nedir?

B. Merkezsiz Regülasyon ve Çok Merkezli Yönetişim

Merkezsiz regülasyon teorisi, riskin çok boyutluluğundan düzenlemenin çok merkezliliğine geçişi kavramsal olarak ifade etmektedir. Bu teoriye göre düzenleme artık merkezi bir otoritenin tek taraflı faaliyeti değil, çok sayıda aktörün, bilgi akışının ve güç ilişkisinin karmaşık etkileşiminden ortaya çıkmaktadır. Merkezi idare modelinin varsaydığı hiyerarşik ve yukarıdan aşağıya doğru işleyen düzenleme şeması modern toplumun karmaşıklığını yansıtmamaktadır.[44] Merkezsiz regülasyon yaklaşımı epistemik merkezsizlik ve kurumsal merkezsizlik olmak üzere iki temel boyut üzerinden işlemektedir ve bu boyutlar birbirini tamamlayarak paralel yükümlülüklerin teorik temellerini oluşturmaktadır.[45]

Epistemik merkezsizlik boyutu, toplumun farklı alt sistemlerinin kendi iç mantıkları ve iletişim kodlarıyla işlediğini vurgular.[46] Hukuk, ekonomi, bilim ve siyaset sistemleri farklı rasyonalitelerle çalışmakta ve

---

kaldırılması karşılığında mağdurdan fidye talep eden kötü amaçlı yazılım türüdür.

44 Black, "Decentring Regulation", 110-112; Hancher - Moran, "Organizing Regulatory Space", 148-172.

45 Black, "Decentring Regulation", 105-108.

46 Luhmann, *Risk*, 74-82; Black, "Decentring Regulation", 110-113.

düzenleyici otorite bu sistemlerin dışından doğrudan müdahale edememektedir. Siber güvenlik bağlamında bu, düzenleyici otoritenin teknik sistemlerin karmaşıklığını tam olarak kavrayamayacağı ve dolayısıyla özel sektör uzmanlığına, sektör standartlarına ve piyasa mekanizmalarına güvenmesi gerektiği anlamına gelmektedir. Ancak epistemik merkezsizlik yalnızca devlet-özel sektör ayrımıyla sınırlı değildir. Devletin kendi içinde de farklı epistemik topluluklar bulunmaktadır.[47]

Bankacılık düzenlemesinin finansal istikrar odağı sistematik risk ve bulaşma etkisi kavramlarıyla çalışmaktadır. Bir bankanın siber saldırıya uğraması, ödeme sistemleri aracılığıyla diğer bankalara yayılabilecek bir likidite krizi tetikleyebileceğinden, BDDK'nın risk değerlendirmesi sistemik etki analizi içermektedir. İletişim düzenlemesinin teknik altyapı perspektifi ise şebeke süreklilik metrikleri, servis kesinti süreleri ve teknik uyumluluk standartlarıyla çalışmaktadır. BTK için aynı siber olay, haberleşme altyapısının kesintiye uğraması ve toplumsal iletişimin aksama riski açısından değerlendirilmektedir. Sermaye piyasası düzenlemesinin şeffaflık-piyasa bütünlüğü mantığı ise içsel bilgi asimetrisi ve yatırımcı koruması çerçevesinde işlemektedir. SPK açısından kritik olan, siber olayın piyasa fiyatlarını etkileyecek bir bilgi niteliği taşıyıp taşımadığı ve bu bilginin kamuya zamanında ve eşit şekilde açıklanıp açıklanmadığıdır.

Her bir düzenleyici kurum kendi epistemik topluluğunun ürettiği bilgi, kavramlar ve değerlendirme kriterleriyle çalışmaktadır. Dolayısıyla paralel yükümlülükler, farklı epistemik toplulukların aynı riski kendi perspektiflerinden değerlendirme ihtiyacının kurumsal tezahürüdür. Örneğin bir veri merkezi yangını sonrası hizmet kesintisinde, BTK teknik altyapı dayanıklılığı açısından kesinti süresini ve yedekleme kapasitesini değerlendirirken, KVKK kişisel veri kaybı olup olmadığını ve yedek sistemlerin veri koruma standartlarına uyumunu incelemekte, ilgili sektördeki düzenleyici kurum ise iş sürekliliği planlarının yeterliliğini sorgulamaktadır. Her kurum aynı olguya farklı bir epistemik merceğinden bakmaktadır.

---

47 Black, “Decentring Regulation”, 113-115.

Kurumsal merkezsizlik boyutu ise düzenlemenin yalnızca devlet tarafından değil, çok sayıda aktör tarafından üretildiğini vurgulamaktadır.[48] Uluslararası Standardizasyon Örgütü/Uluslararası Elektroteknik Komisyonu (International Organization for Standardization/International Electrotechnical Commission - ISO/IEC) 27001 gibi uluslararası standartlar, NIST (National Institute of Standards and Technology) Siber Güvenlik Çerçevesi gibi endüstri rehberleri ve CIS Controls (Critical Security Controls) gibi topluluk temelli normlar, devlet düzenlemesinin dışında ama onunla etkileşim halinde işlemektedir.[49] Siber güvenlik alanında bu etkileşim özellikle belirgindir; birçok düzenleyici kurum doğrudan teknik standart koymak yerine ISO 27001 sertifikasyonu veya NIST çerçevesine uyum gibi özel sektör standartlarına atıfta bulunmaktadır.[50] Daha önemlisi, devletin kendisi de tek bir otorite değil, farklı yetki alanlarına, perspektiflere ve düzenleme araçlarına sahip çoklu kurumlar topluluğudur.[51]

Her bir sektörel düzenleyici kurum kendi alanında özerk bir düzenleme kapasitesine sahiptir ve bu özerklik tarihsel, hukuki ve işlevsel nedenlerle meşrulaşmıştır. BDDK'nın finansal istikrar misyonu önemli misyonlarından birisidir; krize yol açan zayıf bankacılık

---

48 Black, "Decentring Regulation", 112-118.

49 Örneğin 10.10.2021 tarihinde yayınlanan Bilgi ve İletişim Güvenliği Denetim Rehberi BGYS'yi ISO / IEC 27001 uyumlu Bilgi Güvenliği Yönetim Sistemi olarak tanımlamaktadır.

50 S. Adams vd., "The Governance of Cybersecurity : A Comparative Quick Scan of Approaches in Canada, Estonia, Germany, the Netherlands and the UK", *Tilburg University / WODC, Lahey*, (2015), 147-148 Rapor, siber güvenlik düzenlemesinin katmanlı yapısını ve yasal çerçevelerin idari kodlar, teknik standartlar ve yumuşak hukuk mekanizmalarıyla nasıl tamamlandığını detaylı olarak incelemektedir. Alper Işık, *İnternet Aktörleri ve Egemenliğin Değişen Boyutları* (İstanbul: On İki Levha Yayıncılık, 2025), 151-158.

51 Black, "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes", 139-141; Türk hukukunda bağımsız idari otoritelerin özerklik ve bağımsızlık statüsünün anayasal temellerinin eksikliğine dair bkz. Mustafa Akgün, "Bağımsız İdari Otoritelerin Anayasal Statüsünün Belirlenmesi İhtiyacı: Teorik ve Pratik Gerekçeler", *Amme İdaresi Dergisi* 57/2 (2024), 29-60.

denetimine yanıt olarak kurulan BDDK, operasyonel risklere karşı katı kontrol mekanizmaları geliştirmiştir.[52] BTK'nın iletişim altyapısı sorumluluğu ise kesintisiz haberleşme hizmetlerinin stratejik önemi ve toplumsal ihtiyaçla ilişkilidir.[53] SPK'nın piyasa gözetim yetkisi sermaye piyasalarının bilgi asimetrisi sorununa yönelik geliştirilmiş bir denetim kapasitesidir.[54] Her birinin siber güvenlik olaylarına ilişkin bildirim mekanizması geliştirmesinin gerekçesi, bu farklılaşmış misyon ve uzmanlık alanlarından kaynaklanmaktadır.

Merkezsiz regülasyon teorisinin paralel siber güvenlik yükümlülükleri açısından kritik katkısı, merkezsizliğin kaçınılmaz ve belirli ölçüde meşru olduğunu göstermesidir.[55] Sorun, merkezsizliğin kendisinde değil, koordinasyonun yokluğundadır. Örneğin farazi bir senaryoda, bir finans kuruluşunun tedarik zinciri saldırısına uğraması durumunda, kurum aynı olayı BDDK'ya operasyonel risk bildirimi olarak, KVKK'ya veri ihlali bildirimi olarak, SPK'ya içsel bilgi açıklaması olarak ve BTK'ya kritik altyapı kesintisi olarak raporlamak zorunda kalacaktır. Her bildirim farklı format, farklı zaman penceresi ve farklı detay düzeyi gerektirmiştir. Koordinasyon olmaksızın merkezsizlik, mükerrer raporlama yükü ve tutarsız uygulama oluşturmaktadır.[56] Merkezsiz regülasyonlarda koordinasyon mekanizmalarının yokluğu, farklı düzenleyici kurumlar arasında tutarsızlıklara, izleme ve uygulama farklılıklarına yol açmaktadır. [57]

---

52 Simay Burnukara, *2001 krizi sonrası Türk bankacılık sisteminde BDDK'nın rolü ve fonksiyonu* (İstanbul Ticaret Üniversitesi, 2012).

53 5809 sayılı Elektronik Haberleşme Kanunu md. 1

54 6362 sayılı Sermaye Piyasası Kanunu md. 1

55 Black, "Decentring Regulation", 105-106.

56 Baldwin vd., *Understanding Regulation*, 159-163.

57 David P. Carter - Nadia Mahallati, "Coordinating Intermediaries: The Prospects and Limitations of Professional Associations in Decentralized Regulation", *Regulation & Governance* 13/1 (2019), 2-4. Carter ve Mahallati, merkezsiz düzenlemelerde koordinasyon eksikliğinin izleme ve uygulama farklılıklarına, tutarsızlıklara ve düzenleyici boşluklara yol açtığını göstermektedir.

Çok merkezli yönetişim teorisi, merkezsizlik olgusunu normatif bir çerçeveye dönüştürmekte ve merkezsizliğin optimal yönetimini tartışmaya açmaktadır.[58] Bu teori, ne tamamen merkezi ne de tamamen merkezsiz, aksine çok sayıda özerk ama birbirine bağlı karar alma merkezinin koordineli çalıştığı sistemlerin en etkin sonuçları verdiğini ortaya koymaktadır.[59] Çok merkezli regülasyon rejimleri, koordinasyon olmadan işlevsel, sistemik ve demokratik zorluklar oluşturmaktadır; bu rejimlerde karmaşık bağımlılıklar nedeniyle merkezi bir otorite eksikliği koordinasyon sorunlarını öne çıkarmaktadır.[60] Bu bulgu, paralel yükümlülüklerin analizinde teorik bir çıkış noktası sunmaktadır. Merkezsizlik, yalnızca tanımlanması gereken bir olgu değil, belirli koşullar altında tercih edilmesi gereken bir tasarım tercihi olmaktadır.

Çok merkezli sistemlerin avantajları, siber güvenlik yükümlülüklerinin neden tamamen merkezi bir yapıya dönüştürülmemesi gerektiğini açıklamaktadır. İlk olarak her karar alma merkezinin kendi bağlamına özgü bilgi ve uzmanlığa sahip olması, etkin düzenleme için kritik öneme sahiptir. BDDK'nın finansal risk perspektifi, stres testleri, senaryo analizleri ve Basel standartları çerçevesinde geliştirilmiş sofistike bir metodoloji içermektedir. BTK'nın teknik altyapı bilgisi ise ağ mimarisi, protokol standartları ve elektromanyetik uyumluluk gibi mühendislik alanlarında uzmanlaşmış bir kapasite gerektirmektedir. SPK'nın piyasa dinamikleri anlayışı içsel bilgi tespiti, önemli etki değerlendirmesi ve yatırımcı psikolojisi konularında deneyim içermektedir. Bu uzmanlaşmış bilgi stokları merkezi bir otorite tarafından tam olarak içselleştirilemez.[61]

---

58 Tartışma için bkz. Ostrom, "Beyond Markets and States".

59 Ostrom, "Beyond Markets and States", 641-645, 652-653.

60 Black, "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes", 140-144. Black, çok merkezli düzenleme rejimlerinin işlevsel zorluklarının koordinasyon sorunlarında yoğunlaştığını, karmaşık bağımlılıklar içeren ağlarda merkezi bir otoritenin yokluğunda koordinasyon mekanizmalarının kritik önem taşıdığını vurgulamaktadır.

61 Ömür Kadri Sarı, "TÜRK HUKUKUNDA DÜZENLEYİCİ VE DENETLEYİCİ KURUMLARIN TEMEL İLKELERİ", *Danıştay Dergisi* 152 (2020), 287.

İkinci olarak çok merkezli sistemler farklı yaklaşımların aynı anda denenmesine imkân tanır. Örneğin, BDDK, bankalara siber olayları mümkün olan en kısa sürede kuruma raporlama yükümlülüğü getirmiştir;[62] SPK, içsel bilgi niteliği taşıyan olaylarda derhal kamuya açıklama zorunluluğu öngörür;[63] EPDK, 2023 tarihli Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği ile olgunluk seviyesine göre farklılaştırılmış siber güvenlik yükümlülükleri belirlemiştir.[64] Bu farklı yaklaşımlar, düzenleyicilerin sektörün risk profiline göre bildirim süreleri ve içeriklerini çeşitlendirdiğini göstermektedir. Avrupa'da ise NIS2 Direktifi'nin 24 saat erken uyarı – 72 saat ayrıntılı bildirim – 1 ay nihai rapor modeli yaygınlaşmış olup, bu deneysel öğrenme süreci çok merkezli düzenlemenin karakteristiğini ortaya koymaktadır.[65]

Üçüncü olarak tek merkezli sistemlerde merkez başarısız olduğunda tüm sistem çökebilirken, çok merkezli sistemlerde bir merkezin başarısızlığı diğer merkezler tarafından telafi edilebilir.[66] Örneğin bir siber güvenlik olayı yaşandığında merkezi koordinasyon mekanizması gecikmeli yanıt verirse, sektörel düzenleyici kurumlar kendi kanallarından hızlı müdahale edebilmektedir. 2020 pandemi döneminde merkezi kurumların kapasitesi zorlanırken, sektörel düzenleyici kurumlar kendi alanlarında siber güvenlik uyarıları ve rehberler yayınlamaya devam etmiştir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 24 Temmuz 2020'de Bilgi ve İletişim Güvenliği Rehberi'ni yayımlarken, BDDK 15 Mart 2020'de Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'te güncellemeler gerçekleştirmiş, BTK ise USOM koordinasyonunda siber güvenlik operasyonlarını sürdürmüştür.

---

62 Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, RG 15 Mart 2020, Sayı 31069, m 18(1).

63 Sermaye Piyasası Kurulu, Özel Durumlar Tebliği (II-15.1), RG 23 Ocak 2014, Sayı 28891, m 5–6.

64 Enerji Piyasası Düzenleme Kurumu, Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği, RG 6 Haziran 2023, Sayı 32213.

65 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), OJ L333, 27.12.2022, Arts 23–30.

66 Ostrom, "Beyond Markets and States", 652-655.

Ancak çok merkezli yönetişim teorisinin en kritik katkısı, bu sistemlerin başarısının koordinasyon mekanizmalarına bağlı olduğunu vurgulamasıdır. Koordinasyon olmadan çok merkezlilik parçalanma, çelişkili kurallar, mükerrer yükümlülükler ve düzenleyici boşluklar oluşturabilmektedir. Örneğin farklı kurumların siber güvenlik olay tanımları uyumsuz olabilmekte; bir kurum için raporlanabilir eşiği aşan olay diğeri için ihmal edilebilir görülebilmektedir. Bildirim zamanlamaları çakışabilmekte; aynı günde farklı kurumlar ayrı raporlar talep edebilmektedir. Format farklılıkları tekrar veri girişi gerektirmektedir. Bu maliyetler özellikle küçük ve orta ölçekli işletmeler için orantısız yük oluşturmaktadır. Bu tespit, teorik analizin üçüncü katmanına geçişi gerektirmektedir; merkezsiz düzenleme yapılarının avantajlarından yararlanırken koordinasyon maliyetleri nasıl minimize edilebilir ve optimal denge noktası nasıl tasarlanabilir?

C. Meta-Regülasyon ve Koordineli Düzenleme Rejimleri

Ağ regülasyonu kavramı, merkezsizliğin avantajlarını korurken koordinasyon sorununa çözüm aramanın teorik temelini sunmaktadır.[67] Ağ regülasyonu yaklaşımında düzenleyici otorite kurallar koymaktan ziyade ağları yönetmektedir.[68] Düzenleyici otorite bir orkestra şefi gibi farklı düzenleme aktörlerinin koordinasyonunu sağlar, bilgi akışını kolaylaştırır ve ortak standartları teşvik eder ancak tüm düzenleme sürecini tek başına kontrol etmez.[69] ENISA'nın AB'deki rolü bu yaklaşımın somut örneğidir; doğrudan düzenleme yetkisi olmadan ulusal Bilgisayar Güvenliği Olay Müdahale Ekipleri (Computer Security Incident Response Team - CSIRT) arasında koordinasyon platformu işletmekte, ortak tatbikatlar düzenlemekte ve bilgi paylaşım altyapısı sağlamaktadır.[70]

---

67 Baldwin vd., *Understanding Regulation*, 159; Black, "Decentring Regulation", 103-108.

68 Yannis Papadopoulos, "How Does Knowledge Circulate in a Regulatory Network? Observing a European Platform of Regulatory Authorities Meeting", *Regulation & Governance* 12/4 (2018), 432.

69 Baldwin vd., *Understanding Regulation*, 159-160.

70 Papadopoulos, "How Does Knowledge Circulate in a Regulatory Network?", 433-436; Adams vd., "The Governance of Cybersecurity : A

Meta-regülasyon kavramı bu koordinasyon yaklaşımını operasyonelleştirebilecek bir çerçeve sunmaktadır.[71] Meta-regülasyon, devletin doğrudan davranış kuralları belirlemesi yerine, düzenlenen aktörlerin kendi kendini düzenleme sistemlerini kurmasını zorunlu kılması ve denetlemesi anlamına gelmektedir.[72] Siber güvenlik bağlamında bu, belirli güvenlik teknolojileri emretmek yerine risk yönetim süreçleri, güvenlik yönetim sistemleri ve sürekli iyileştirme döngüleri kurulmasını gerektirmektedir. ISO 27001 sertifikasyonu zorunluluğu bu yaklaşımın tipik örneğidir; standart, belirli kontroller değil, yönetim sisteminin varlığı ve etkinliği üzerinde durmaktadır.[73]

Ancak kamu sektörü bağlamında meta-regülasyon farklı bir anlam kazanmaktadır.[74] Birden fazla düzenleyici kurumun aynı risk alanında yetki sahibi olduğu durumlarda meta-regülasyon, düzenleme regülasyonu anlamına gelmektedir.[75] Bir üst düzey koordinasyon mekanizması alt düzey düzenleyici kurumların aktivitelerini koordine

---

Comparative Quick Scan of Approaches in Canada, Estonia, Germany, the Netherlands and the UK", 98-99.

71 Cary Coglianese - Evan Mendelson, "Meta-Regulation and Self-Regulation", *The Oxford Handbook of Regulation*, ed. Robert Baldwin vd. (Oxford University Press, 2010), 146-168; Cary Coglianese - David Lazer, "Management-Based Regulation: Prescribing Private Management to Achieve Public Goals", *Law & Society Review* 37/4 (Aralık 2003), 691-695.

72 Coglianese - Mendelson, "Meta-Regulation and Self-Regulation", 148; Baldwin vd., *Understanding Regulation*, 146-147; Black, "Decentring Regulation", 112; Coglianese - Lazer, "Management-Based Regulation", 693-698.

73 Adams vd., "The Governance of Cybersecurity : A Comparative Quick Scan of Approaches in Canada, Estonia, Germany, the Netherlands and the UK", 71; Robert Baldwin vd. (ed.), *The Oxford handbook of regulation* (Oxford, U. K: Oxford University Press, 2012), 110-114.

74 Christopher J. Koliba vd., *Governance Networks in Public Administration and Public Policy* (New York: Routledge, 2018), 179.

75 Koliba vd., *Governance Networks in Public Administration and Public Policy*, 179; Christine Parker, *The Open Corporation: Effective Self-Regulation and Democracy* (Cambridge University Press, 2002), 15; Martino Maggetti, "De Facto Independence after Delegation: A Fuzzy-Set Analysis", *Regulation & Governance* 1/4 (2007), 271-278.

etmekte ve tutarlılık sağlamaktadır. Bu perspektiften düzenleyici kurumlar kendileri de düzenlenen olmakta ve kurumlar arası koordinasyon bir tür üst düzey düzenleme işlevi görmektedir.

Düzenleme rejimi analizi bu teorik unsurları bütüncül bir çerçeveye entegre etmektedir. Bir düzenleme rejimi yalnızca kurallardan ibaret değildir; aynı zamanda kuralları koyan kurumlar, uygulama süreçleri, uygulama araçları ve paydaşlar arası ilişkileri de kapsamaktadır.[76] Bir düzenleme rejiminin etkinliği bu unsurların uyumuna bağlıdır. Çok kurumlu düzenleme ortamlarında koordinasyon eksikliği ve aşırı koordinasyon olmak üzere iki temel risk ortaya çıkmaktadır.[77]

Koordinasyon eksikliği farklı kurumların çelişkili kurallar koyması, bilgi paylaşmaması ve mükerrer yükümlülükler oluşturması olarak tezahür etmektedir. Örneğin bir kurum 24 saat içinde bildirim gerektirirken diğeri 72 saat penceresi tanıyabilmektedir. Bir kurum olay şiddeti sınıflandırmasında etkilenen kullanıcı sayısını kriter alırken diğeri hizmet kesinti süresini esas alabilmektedir. Bir kurum çevrimiçi portal üzerinden bildirim isterken diğeri e-posta veya fiziksel belge talep edebilmektedir. Bu tutarsızlıklar özellikle çok sektörlü platformlar için ciddi uyum zorluğu ortaya çıkarmaktadır; bir fintech şirketi hem finansal hem teknoloji mevzuatına tabi olduğunda koordinasyon eksikliği katlanarak artmaktadır.

Aşırı koordinasyon ise koordinasyon çabasının karar alma süreçlerini yavaşlatması, esnekliği azaltması ve kurumsal uzmanlığı köreltmesi anlamına gelmektedir. Tüm kararların merkezi onaya tabi tutulması hantal bir bürokrasi oluşturabilir ve sektörel kurumların uzmanlığından yararlanmayı engelleyebilir. Örneğin her siber güvenlik olayı bildiriminin önce merkezi bir kurumda değerlendirilip sonra ilgili

---

[76] Baldwin vd., *The Oxford handbook of regulation*, 105; Hood vd., *The Government of Risk*.

[77] Baldwin vd., *The Oxford handbook of regulation*, 159; Black, "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes", 140; Black, "Decentring Regulation", 103-108.

sektörel kuruma yönlendirilmesi, acil müdahale gerektiren durumlarda kritik gecikmelere yol açabilir.

Optimal regülasyon rejimi tasarımı bu iki risk arasında denge kurmaktadır. Koordineli çoğulculuk kavramı bu dengenin teorik ifadesidir.[78] Bu yaklaşımda farklı kurumlar özerkliklerini korurken, ortak standartlar, bilgi paylaşım protokolleri ve uyuşmazlık çözüm mekanizmaları aracılığıyla koordinasyon sağlanmaktadır.[79] Düzenleyici ağlar literatürü bu koordinasyonun hangi mekanizmalarla gerçekleştirilebileceğini göstermektedir. Düzenli toplantılar ve iletişim kanalları kurumlar arası güven oluşturmakta ve gayri resmi koordinasyonu kolaylaştırmaktadır.[80] Ortak veri toplama ve analiz standartları, farklı kurumların aynı veri dilini konuşmasını sağlamaktadır. Personel değişimi ve ortak eğitim programları kurumlar arası kültürel yakınlaşma oluşturmaktadır. En iyi uygulama paylaşımı başarılı modellerin hızla yayılmasını sağlamaktadır. Ortak risk değerlendirme metodolojileri ise benzer olayların tutarlı şekilde sınıflandırılmasını mümkün kılmaktadır.[81]

ENISA'nın AB'deki rolü bu teorik çerçevenin pratik uygulamasını göstermektedir. ENISA doğrudan düzenleme yetkisine

---

78 Baldwin vd., *The Oxford handbook of regulation*, 381-382; Black, "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes", 137-164; Black, "Decentring Regulation", 103-112, 142-146; Sandra Eckert - Tanja A. Börzel, "Experimentalist Governance: An Introduction", *Regulation & Governance* 6/3 (2012), 372-374.

79 Baldwin vd., *The Oxford handbook of regulation*, 159-163; David Coen - Mark Thatcher, "Network Governance and Multi-Level Delegation: European Networks of Regulatory Agencies", *Journal of Public Policy* 28/1 (Nisan 2008), 49-71; Kutsal Yesilkagit, "Institutional compliance, European networks of regulation and the bureaucratic autonomy of national regulatory authorities", *Journal of European Public Policy* 18/7 (01 Ekim 2011), 963-965.

80 Julia Black, "Regulatory Conversations", *Journal of Law and Society* 29/1 (2002), 163-196; Papadopoulos, "How Does Knowledge Circulate in a Regulatory Network?"

81 Papadopoulos, "How Does Knowledge Circulate in a Regulatory Network?", 438-445; Coglianese - Lazer, "Management-Based Regulation", 710-715.

sahip olmamakla birlikte, ulusal siber olay müdahale ekipleri arasında koordinasyon sağlama, ortak standartlar ve tatbikatlar geliştirme, bilgi paylaşım platformları oluşturma ve en iyi uygulamaları yaygınlaştırma rolü oynamaktadır.[82] NIS2 Direktifi ve özellikle 2024/2690 sayılı Uygulama Tüzüğü'nün getirdiği standart bildirim formatları, meta-regülasyon yaklaşımının somut bir ürünüdür. Bu düzenlemeler ulusal düzenleyici otoritelerin özerkliğini korurken, bildirim süreçlerini, sınıflandırma kriterlerini ve format standartlarını uyumlaştırmaktadır. Bir siber olay tüm AB'de aynı kategorilere göre sınıflandırılmakta, aynı zaman pencerelerinde bildirilmekte ve aynı veri alanlarını içeren formatlarda raporlanmaktadır.

Bu teorik çerçevenin Türkiye bağlamındaki uygulanması, çalışmanın temel araştırma sorusunu yanıtlamak için gerekli analitik araçları sağlamaktadır. Paralel siber güvenlik yükümlülükleri ve özelde bildirim rejimleri, riskin çok boyutluluğunun epistemik ve kurumsal düzeyde yansımasıdır. Her bir sektörel düzenleyici kurum farklı bir risk perspektifini, farklı bir uzmanlık alanını ve farklı bir meşruiyet temelini temsil etmektedir. Bu merkezsiz yapının avantajları, uzmanlaşmış bilgi, deneysel öğrenme, sistem direnci ve hesap verebilirlik çeşitliliği olarak somutlaşmaktadır. Ancak koordinasyon mekanizmalarının yokluğu veya yetersizliği, bu avantajları mükerrer raporlama yükü, bilgi parçalanması ve tutarsız uygulama gibi maliyetlerle gölgelemektedir.

Dolayısıyla optimal tasarım sorunu merkezsizlik ve koordinasyon arasında denge kurmaktır. Meta-regülasyon yaklaşımı ve koordineli çoğulculuk perspektifi bu dengenin nasıl tasarlanabileceğine ilişkin teorik bir çerçeve sunmaktadır. Siber Güvenlik Başkanlığı'nın rolü bu perspektiften yeniden tanımlanmalıdır; Başkanlık, operatörlerden doğrudan bildirim alan bir kurum olmaktan öte, sektörel kurumların bildirim mekanizmalarını koordine eden, ortak standartlar

[82] Adams vd., "The Governance of Cybersecurity : A Comparative Quick Scan of Approaches in Canada, Estonia, Germany, the Netherlands and the UK", 98-99; Papadopoulos, "How Does Knowledge Circulate in a Regulatory Network?", 433-435; Yesilkagit, "Institutional compliance, European networks of regulation and the bureaucratic autonomy of national regulatory authorities", 965-970.

geliştiren, bilgi akışını kolaylaştıran ve uyumu sağlayan bir meta-regülatör işlevi görmelidir. Bu teorik çerçeve, çalışmanın ilerleyen bölümlerinde mevcut Türk siber güvenlik rejiminin analizini ve reform önerilerinin geliştirilmesini yönlendirecektir.

III. Türkiye'deki Çok Katmanlı Bildirim Mimarisi

Türkiye'de siber güvenlik alanındaki bildirim yükümlülükleri, çok katmanlı ve parçalı bir yapı arz etmektedir. Bu parçalı yapının kökenleri, teorik çerçevede incelendiği üzere, riskin çok boyutlu doğasında ve farklı düzenleyici kurumların tarihsel olarak gelişen uzmanlık alanlarında yatmaktadır. Siber güvenlik olayları, aynı anda operasyonel bir süreklilik sorunu, bir veri koruma ihlali, bir finansal istikrar riski ve bir piyasa bilgisi niteliği taşıyabilmektedir. Riskin bu çok boyutluluğu, merkezsiz regülasyon teorisinin öngördüğü gibi, farklı epistemik toplulukların devreye girmesini gerektirmekte ve her topluluk kendi perspektifinden düzenleme mekanizmaları geliştirmektedir.

7545 sayılı Siber Güvenlik Kanunu'nun yürürlüğe girmesi, ulusal siber güvenlik mimarisinde yeni bir merkezi koordinasyon otoritesi olan Siber Güvenlik Başkanlığı'nı getirmiştir.[83] Ancak Kanun, sektörel düzenleyici kurumların mevcut bildirim mekanizmalarını ortadan kaldırmamış, aksine bunların üzerine yeni bir katman eklemiştir. Bu durum, çok merkezli yönetişim literatüründe tartışılan koordinasyon sorununu somut olarak gündeme getirmektedir. Aynı siber güvenlik olayı, farklı zamanlarda, farklı formatlarda ve farklı kurallara tabi olarak birden fazla kuruma bildirilmek zorundadır.

A. Siber Güvenlik Başkanlığı'nın Merkezi Koordinasyon Çerçevesi

7545 sayılı Kanun'un yürürlüğe girmesiyle birlikte Siber Güvenlik Başkanlığı, Türkiye'nin siber güvenlik yönetişiminde merkezi bir rol üstlenmiştir. Meta-regülasyon perspektifinden değerlendirildiğinde, SGB'nin iki farklı rol üstlenme potansiyeli

[83] 7545 sayılı Siber Güvenlik Kanunu, RG: 19.03.2025-32846.

bulunmaktadır: düzenleme düzenleyicisi (meta-regülatör) veya paralel düzenleyici.

Birinci senaryoda, Başkanlık sektörel kurumların bildirim sistemlerini koordine ederek tek giriş noktası işlevi görebilir. İkinci senaryoda ise, mevcut sektörel mekanizmaların yanına eklenen başka bir bildirim kanalı olur. Kanun metni ve geçiş hükümleri incelendiğinde, ikinci senaryonun şu anda ağır bastığı düşünülebilir ancak ikincil düzenlemeler ile birinci senaryonun da gerçekleşmesi mümkündür.

Kanun'un 7. maddesi, bilişim sistemleri kullanmak suretiyle hizmet sunan, veri toplayan, işleyen ve benzeri faaliyet yürütenlerin siber güvenliğe ilişkin görev ve sorumluluklarını düzenlemektedir.[84] Bu hükmün kapsamı son derece geniştir ve neredeyse tüm bilişim sistemi kullanan kurum ve kuruluşları içerir. E-ticaret siteleri, sağlık kuruluşları, eğitim kurumları, küçük ve orta boy işletmeler bu kapsamda değerlendirilebilir. Söz konusu kişi ve kuruluşlar, hizmet sundukları alanda tespit ettikleri zafiyet veya siber olayları gecikmeksizin Başkanlığa bildirmekle yükümlüdür.[85]

Gecikmeksizin ifadesi, belirli bir saat veya gün cinsinden süre öngörmemekte, olayın tespit edilmesiyle birlikte derhal bildirim yapılması gerektiğini ima etmektedir. SGB'nin gecikmeksizin standardı ile BDDK'nın operasyonel risk bildirimi, SPK'nın derhal, BTK'nın en kısa sürede ve KVKK'nın 72 saat kuralları arasında potansiyel uyumsuzluk gözükmektedir. Ancak Kanun'un 7. maddesinin üçüncü fıkrasının SGB'ye tanıdığı ikincil düzenleme yetkisi, bu koordinasyon sorununa çözüm potansiyeli taşımaktadır. Başkanlık, çıkaracağı usul ve esaslarla ortak bildirim standartları, birleştirilmiş zaman pencereleri ve tek giriş-çok çıkış mekanizması kurabilir. Bu durumda SGB, sektörel kurumların uzmanlığını koruyarak üst düzey koordinasyon sağlayan gerçek bir meta-regülatör haline gelebilir. Dolayısıyla mevcut parçalı yapı, geçici bir durum olarak değerlendirilebilir; ikincil düzenlemelerin yayımlanmasıyla eşgüdümlü bildirim mekanizmasına evrilebilir.

---

84 7545 sayılı Kanun, m. 7.

85 7545 sayılı Kanun, m. 7(1)(b).

Kanun'un 7. maddesinin (a) bendi ise Başkanlığın görev ve faaliyetleri kapsamında talep ettiği her türlü veri, bilgi, belge, donanım, yazılım ve diğer katkının öncelikle ve zamanında Başkanlığa iletilmesi yükümlülüğünü getirmektedir.[86] Bu hüküm, reaktif bildirim ile proaktif veri paylaşımı arasında bir ayrıma işaret etmektedir. Başkanlık, ihtiyaç duyduğu her türlü teknik veriyi, sistem konfigürasyonunu, zafiyet raporlarını veya risk değerlendirmelerini ilgili kurum ve kuruluşlardan talep edebilmektedir.

Siber güvenlik tedbirlerini almama ve zafiyet veya siber olayları gecikmeksizin bildirmeme gibi yükümlülüklerin ihlali ise idari para cezasına tabidir. Kanun'un 16. maddesinin onuncu fıkrası, idari yaptırımları düzenlemektedir. Bu hükme göre, 7. maddenin birinci fıkrasının (b) ve (c) bentlerindeki görev ve sorumlulukları yerine getirmeyenlere bir milyon Türk Lirasından on milyon Türk Lirasına kadar idari para cezası uygulanmaktadır.[87] Ancak Kanun, bildirim yükümlülüğünün detaylarını ikincil düzenlemelere bırakmış durumdadır.[88]

SGB'nin koordinasyon fonksiyonu teorik düzeyde güçlü görünmekle birlikte, mevcut sektörel bildirim mekanizmalarıyla etkileşimi henüz netleşmemiştir. Başkanlık bir bildirim aldığında ilgili sektörel düzenleyiciyi bilgilendirecek mi? Sektörel düzenleyicilerden gelen bildirimleri merkezileştirecek tek pencere işlevi görecek mi? Yoksa sektörel düzenleyicilerin kendi bildirim mekanizmalarını sürdürmesi ve SGB'ye paralel bir bildirim kanalı olarak işlemesi mi öngörülmektedir? Bu sorular, Kanun'un Geçici 1. maddesinin beşinci fıkrası uyarınca geçiş sürecinde daha da önem kazanmaktadır. Bu hükme göre, yürürlükten kaldırılan hükümler kapsamında faaliyet gösteren kurumlar, Başkanlığın teşkilatlanmasının tamamlanmasına kadar görevlerini sürdürecektir.[89] Bu düzenleme, geçiş döneminde paralel yükümlülüklerin devam edeceğini açıkça göstermektedir.

---

86 7545 sayılı Kanun, m. 7(1)(a).

87 7545 sayılı Kanun, m. 16(10).

88 7545 sayılı Kanun, m. 7(3).

89 7545 sayılı Kanun, Geçici m. 1(5).

Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) yapısal konumu ve SGB'ye devri, merkezi koordinasyon çerçevesinin anlaşılması açısından ayrı bir önem taşımaktadır. USOM, 20 Haziran 2013 tarihinde yayımlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı çerçevesinde BTK bünyesinde kurulmuş ve Türkiye'nin ulusal CSIRT işlevini yerine getirmiştir. 11 Kasım 2013 tarihli SOME (Siber Olaylara Müdahale Ekibi) Tebliği, USOM'un görev ve yetkilerini düzenlemiştir.[90] Bu Tebliğ uyarınca, kritik sektörlerde sektörel SOME'lerin kurulması öngörülmüştür. Enerji, elektronik haberleşme, finans, su yönetimi, kritik kamu hizmetleri ve ulaştırma sektörleri bu kapsamda tanımlanmıştır. SOME Tebliği kapsamında üç katmanlı bir bildirim hiyerarşisi oluşturulmuştur. Kurumsal SOME'ler, kendi organizasyonlarındaki siber güvenlik olaylarını tespit ettiklerinde bu olayları sektörel SOME'lere bildirmekte, sektörel SOME'ler ise USOM'a iletmektedir.[91]

7545 sayılı Kanun'un yürürlüğe girmesiyle birlikte, USOM'un yapısal konumu köklü bir değişime uğramıştır. Kanun'un Geçici 1. maddesi uyarınca, BTK ve Dijital Dönüşüm Ofisi'ne ait ve münhasıran ulusal siber güvenlik faaliyetleri kapsamında kullanılan her türlü taşınır, bilgi işlem altyapısı, taşıt ve diğer varlıklar ile bunlardan doğan hak ve yükümlülükler, Kanun'un yayımından itibaren altı ay içerisinde (19 Eylül 2025 tarihine kadar) SGB'ye devredilmek zorundadır.[92] Bu kapsamda USOM'un tüm yetkileri SGB'ye geçmiş, böylece ulusal CSIRT fonksiyonu artık SGB bünyesinde icra edilmektedir.

SOME yapılanmasının geleceği de netlik kazanmayı beklemektedir. Sektörel SOME'ler kaldırılacak mı, yoksa SGB'ye bağlı alt birimler olarak yeniden yapılandırılacak mı? Kurumsal SOME'ler artık doğrudan SGB'ye mi raporlayacak, yoksa sektörel SOME'ler aracılığıyla mı bildirim yapacak? Bu sorular, SOME Tebliği'nin güncellenmesi ve SGB'nin ikincil düzenlemelerinin yayımlanmasıyla cevaplanacaktır. Ancak geçiş sürecinde BTK'nın sektörel düzenleme yetkisi ve SOME

---

90 Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ (SOME Tebliği), RG: 11.11.2013-28818.

91 SOME Tebliği, m. 7; Sektörel SOME Kurulum ve Yönetim Rehberi, 14-15.

92 7545 sayılı Kanun, Geçici m. 1(1).

ekosisteminin işleyişi devam etmekte, bu durum elektronik haberleşme işletmecilerinin bildirim kanalları açısından geçici belirsizlik getirmektedir.

B. Sektörel Düzenleyici Kurumlar ve Bildirim Mekanizmaları

Sektörel düzenleyici kurumlar, kendi uzmanlık alanlarında tarihsel olarak gelişmiş bildirim mekanizmalarına sahiptir. Bu mekanizmaların varlığı, teorik çerçevede tartışılan epistemik merkezsizlik ve kurumsal merkezsizlik olgusunun somut tezahürüdür. Her bir kurum, siber güvenlik olaylarını kendi risk perspektifinden değerlendirmekte ve buna uygun bildirim yükümlülükleri öngörmektedir. Bu bölümde, başlıca sektörel düzenleyici kurumların siber güvenlik bildirim mekanizmaları incelenecektir.

1. Bankacılık Sektöründe BDDK'nın Operasyonel Risk Yaklaşımı

Bankacılık Düzenleme ve Denetleme Kurumu, 5411 sayılı Bankacılık Kanunu çerçevesinde bankacılık sektöründe düzenleyici ve denetleyici yetkiye sahiptir.[93] BDDK'nın siber güvenlik alanındaki temel düzenlemesi, 15 Mart 2020 tarihli Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'tir.[94]

Yönetmelik'in 18. maddesi, bilgi güvenliği olay yönetimine ilişkin hükümleri içermektedir. Madde uyarınca, bankalar bilgi sistemlerinde meydana gelen güvenlik ihlalleri ve önemli olaylar hakkında siber olay yönetim prosedürü çerçevesinde hem Kuruma hem de sektörel SOME'ye raporlama yapmakla yükümlüdür.[95] Yönetmelik ayrıca bankaların bilgi güvenliği ihlallerine müdahale planı hazırlamasını, siber olay müdahale ekipleri oluşturmasını ve düzenli tatbikatlar yapmasını zorunlu kılmaktadır. BDDK, bankaların bilgi sistemlerini düzenli olarak denetlemekte ve siber güvenlik uygulamalarını yakından takip etmektedir.

---

93 5411 sayılı Bankacılık Kanunu, RG: 01.11.2005-25983.

94 Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik (BDDK Yönetmeliği), RG: 15.03.2020-31069.

95 BDDK Yönetmeliği, m. 18(1).

BDDK'nın yaklaşımı, operasyonel risk yönetimi perspektifinden şekillenmiş olup, siber güvenlik olayları bir operasyonel risk kategorisi olarak ele alınmaktadır. Ancak bu sıkı düzenleme rejimi, bankaların aynı zamanda SGB'ye (hem siber olay hem de siber zafiyet bakımından) ve KVKK'ya (kişisel veri ihlali durumunda) ayrı ayrı bildirim yapma yükümlülüğü altında olduğu gerçeğini değiştirmemektedir.

2. Sermaye Piyasasına Yönelik İki Bildirim Sistemi

SPK, 6362 sayılı Sermaye Piyasası Kanunu çerçevesinde sermaye piyasalarında düzenleyici ve denetleyici yetkiye sahiptir.[96] SPK'nın siber güvenlik alanındaki düzenlemeleri iki temel eksen üzerinde şekillenmektedir: bilgi sistemleri yönetimi ve sermaye piyasası şeffaflığı çerçevesinde kamuyu aydınlatma. Bu iki eksenli yapı, sermaye piyasasında faaliyet gösteren kuruluşlar için farklı amaçlara hizmet eden iki ayrı bildirim kanalı oluşturmaktadır.

SPK'nın siber güvenliğe ilişkin temel düzenlemesi, 13 Mart 2025 tarihinde yayımlanan VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği'dir.[97] Bu Tebliğ, sermaye piyasası kurumları, borsalar, halka açık ortaklıklar ve kripto varlık hizmet sağlayıcıları dahil geniş bir kapsama sahiptir.[98]

Tebliğ'in 24. maddesi, siber olay müdahale ve bildirim yükümlülüklerini düzenlemektedir. Maddenin birinci fıkrası, gerçekleşen bilgi güvenliği ihlalinin veya tespit edilen güvenlik açığının mümkün olan en kısa sürede kayda alınmasını ve gerekli işlemlerin yapılmasını öngörmektedir.[99] Maddenin dördüncü fıkrasına göre yaşanan bir olayın kritik operasyonları kesintiye uğratacak veya veri sızıntısıyla sonuçlanacak potansiyelde belirlenmesi durumunda derhal Kurul, müşteriler ve ilgili diğer kurumlar bilgilendirilir.[100] Derhal ifadesi, olay tespit edilir edilmez bildirim yapılması gerektiğini

96 6362 sayılı Sermaye Piyasası Kanunu, RG: 30.12.2012-28513.

97 Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10), RG: 13.03.2025-32840.

98 SPK VII-128.10 Tebliği, m. 2.

99 SPK VII-128.10 Tebliği, m. 24(1).

100 SPK VII-128.10 Tebliği, m. 24(4).

göstermekte ve bu açıdan SGB düzenlemeleriyle uyumlu bir yaklaşım sergilemektedir.

SPK'nın ikinci bildirim kanalı ise sermaye piyasası şeffaflığı çerçevesinde kamuyu aydınlatma rejimi üzerinden işlemektedir. II-15.1 sayılı Özel Durumlar Tebliği, halka açık ortaklıkların içsel bilgileri kamuya açıklama yükümlülüğünü düzenlemektedir.[101] Tebliğ'in 5. maddesi uyarınca, içsel bilgiler ortaya çıktığında veya öğrenildiğinde açıklanması gerekmektedir.[102] Siber güvenlik olayları, sermaye piyasası araçlarının değerini, fiyatını veya yatırımcıların yatırım kararlarını etkileyebilecek öneme sahipse içsel bilgi niteliği taşıyabilmektedir.

Örneğin bir bankanın veya halka açık şirketin kritik sistemlerini etkileyen bir fidye yazılımı saldırısı, operasyonel faaliyetlerde kesintiye yol açıyorsa ve bu durum finansal sonuçları önemli ölçüde etkileyebilecekse, Kamuyu Aydınlatma Platformu (KAP) üzerinden açıklanması gerekmektedir. Tebliğ'in 6. maddesi, içsel bilgilerin kamuya açıklanmasının ertelenmesini belirli koşullarda mümkün kılmakta, ancak bu erteleme yatırımcıların yanıltılmasına yol açmaması ve bilgilerin gizli tutulmasını sağlayabilecek olması kaydıyla uygulanabilmektedir.

Bu durum, sermaye piyasasında faaliyet gösteren kuruluşlar için çoklu bildirim yükümlülüğü getirmektedir: SGB'ye gecikmeksizin bildirim, SPK'ya VII-128.10 kapsamında derhal bildirim ve halka açık ortaklıklar için KAP üzerinden kamuya açıklama. Her bir kanalın farklı amaçları, muhatabı ve sonuçları bulunmaktadır. Bilgi sistemleri odaklı bildirimler teknik müdahale ve düzenleme amaçlı iken, KAP bildirimleri yatırımcıların bilgilendirilmesi ve piyasa şeffaflığı amacına hizmet etmektedir.

3. BTK ve Şebeke Güvenliği

Bilgi Teknolojileri ve İletişim Kurumu, 5809 sayılı Elektronik Haberleşme Kanunu çerçevesinde elektronik haberleşme sektöründe düzenleyici ve denetleyici yetkiye sahiptir. BTK'nın siber güvenlik

---

101 SPK Özel Durumlar Tebliği (II-15.1), RG: 23.01.2014-28891.

102 SPK II-15.1 Tebliği, m. 5(1).

alanındaki temel düzenlemesi, Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği'dir.

Yönetmelik'in 38. maddesi, ihlallerin bildirilmesi yükümlülüğünü açıkça düzenlemektedir. Madde uyarınca, işletmeci abonelerinin yüzde beşinden fazlasını etkileyen şebeke ve bilgi güvenliği ihlallerini ve iş sürekliliğini kesintiye uğratan olayları en kısa sürede Kuruma bildirir.[103] Söz konusu bildirim asgari olarak; olayın gerçekleşme zamanını, niteliğini, etkisini, süresini ve alınan önlemleri içerir. Bu hüküm, elektronik haberleşme işletmecileri için net bir eşik ve bildirim yükümlülüğü getirmektedir.

Bu çerçevede, elektronik haberleşme işletmecileri bakımından şebeke ve bilgi güvenliği ihlallerinin BTK'ya bildirimi ile kişisel veri ihlallerinin KVKK Kurumuna bildirimi, farklı normatif temellere dayanmakla birlikte, ihlalin etki alanının belirlenmesi, olayın niteliği ve süreci hakkında detaylı bilgi sunulması ve belirli süreler içinde raporlama yapılması bakımından paralel iki bildirim rejimi oluşturmaktadır. Örneğin, bir elektronik haberleşme işletmecisinin sistemlerinde meydana gelen bir siber olay hem hizmetin kesintiye uğramasına hem de abone kişisel verilerinin sızmasına yol açıyorsa, işletmeci açısından aynı olay için hem BTK'ya Yönetmelik md. 38 kapsamında, hem de KVKK md. 12/5 ve Kurul'un 2019/10 sayılı kararı çerçevesinde Kurula veri ihlali bildirimi yapılması gündeme gelecektir.

4. Ödeme Sistemleri ve TCMB

Türkiye Cumhuriyet Merkez Bankası (TCMB), 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun çerçevesinde ödeme sistemleri ve elektronik para kuruluşlarının gözetim ve denetimine ilişkin yetkilere sahiptir.[104] 6493 sayılı Kanun özel bir sektörel ihlal bildirimi yükümlülüğü getirmiştir. TCMB tarafından talep edilen bilgi

---

[103] Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği, m. 38(1).

[104] 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun, RG: 27.06.2013-28690.

ve belgelerin geçerliliğini etkileyecek herhangi bir değişiklik olması halinde, sistem işleticileri, ödeme kuruluşları ve elektronik para kuruluşları TCMB'yi derhal bilgilendirmekle yükümlüdür. Bu hükmün derhal ifadesi, SGB'nin gecikmeksizin ve SPK'nın derhal kavramlarıyla benzer bir anlam taşımaktadır.

Ayrıca, 2021 tarihli Tebliğ, ödeme ve elektronik para kuruluşlarına siber olay bildirim yükümlülüğü getirmektedir.[105] Tebliğ uyarınca kuruluşlar, siber olayları olay yönetimi kapsamında ele almak ve TCMB'ye gerekli bildirimleri yapmakla yükümlüdür. Özellikle hassas müşteri verilerinin veya kişisel verilerin sızmasına ya da ifşasına yol açan siber olaylar söz konusu olduğunda, kuruluşlar hem müşterilerini hem de Kişisel Verileri Koruma Kurulunu mümkün olan en kısa süre içerisinde bilgilendirmekle yükümlüdür.

Bir ödeme kuruluşunun siber saldırı nedeniyle hizmet kesintisi yaşadığını varsayalım. Bu durumda kuruluş, TCMB'ye derhal bilgilendirme yükümlülüğü çerçevesinde performans raporlaması gerçekleştirirken, aynı zamanda SGB'ye gecikmeksizin bildirim yapmakta, kullanıcı verileri etkilenmişse KVKK'ya en geç 72 saat içinde raporlama sunmakta ve hizmeti sunduğu bankanın iştiraki ise BDDK'ya operasyonel risk bildirimi yapabilmektedir. Her bildirim farklı bir risk boyutunu ele almaktadır: TCMB ödeme sistemlerinin kesintisiz işleyişi ve finansal istikrar, BDDK bankacılık sistemi sağlamlığı, KVKK kişisel veri güvenliği, SGB teknik altyapı sürekliliği ve ulusal güvenlik perspektifinden değerlendirme yapmaktadır.

5. Enerji Sektöründe EPDK'nın Olgunluk Modeli

Enerji Piyasası Düzenleme Kurumu, 6446 sayılı Elektrik Piyasası Kanunu ve 4628 sayılı Enerji Piyasası Düzenleme Kurumunun Teşkilat ve Görevleri Hakkında Kanun çerçevesinde enerji sektöründe

[105] Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ, RG: 01.12.2021-31676.

düzenleyici ve denetleyici yetkiye sahiptir.[106] EPDK'nın siber güvenlik alanındaki temel düzenlemesi, 6 Haziran 2023 tarihli Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği'dir.[107] Bu Yönetmelik, elektrik ve doğal gaz iletim ve dağıtım lisansı sahipleri ile belirli üretim tesislerini kapsamaktadır.

Yönetmelik'in ayırt edici özelliği, olgunluk seviyesine dayalı farklılaştırılmış bir yükümlülük sistemi getirmesidir. Enerji kuruluşları, siber güvenlik olgunluk seviyelerine göre sınıflandırılmakta ve her seviye için farklı gereklilikler öngörülmektedir. Bu yaklaşım, diğer sektörel düzenleyicilerin tek tip yükümlülük sistemlerinden ayrılmaktadır. Olgunluk seviyesi yüksek olan kuruluşlardan daha kapsamlı siber güvenlik tedbirleri beklenirken, olgunluk seviyesi düşük olan kuruluşlar için temel yükümlülükler tanımlanmaktadır.

Yönetmelik kapsamında enerji kuruluşları, yetkinlik modeline uyumlarını gösteren öz denetim raporlarını, ilerleme raporlarını ve sektörel denetim raporlarını düzenli olarak EPDK'ya bildirmekle yükümlüdür. Bu raporların iletim süreleri ve içerikleri, kuruluşun yetkinlik seviyesine ve denetim aşamasına göre farklılık göstermektedir. EPDK, bildirimleri değerlendirerek ve gerekli gördüğü durumlarda yerinde denetim gerçekleştirebilmektedir.

EPDK'nın yaklaşımı, endüstriyel kontrol sistemlerinin güvenliğine özel vurgu yapmaktadır. Enerji altyapılarının operasyonel teknoloji bileşenleri, geleneksel bilgi teknolojisi sistemlerinden farklı güvenlik gereksinimleri ve tehdit profilleri içermektedir. SCADA, DCS ve PLC gibi endüstriyel kontrol sistemleri, fiziksel süreçleri yöneten kritik altyapılardır ve bu sistemlere yönelik siber saldırılar doğrudan operasyonel kesintilere ve fiziksel zararlara yol açabilir. Yönetmelik, bu

---

[106] 6446 sayılı Elektrik Piyasası Kanunu, RG: 30.03.2013-28603; 4628 sayılı Enerji Piyasası Düzenleme Kurumunun Teşkilat ve Görevleri Hakkında Kanunu RG: 03.03.2011-24335 (Mükerrer).

[107] Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği, RG: 06.06.2023-32213.

farklılığı dikkate alarak operasyonel teknoloji güvenliğine özgü hükümler içermektedir.[108]

6. Sivil Havacılık Genel Müdürlüğü

Sivil Havacılık Genel Müdürlüğü (SHGM), 5431 sayılı Sivil Havacılık Genel Müdürlüğü Teşkilat ve Görevleri Hakkında Kanun çerçevesinde sivil havacılık sektöründe düzenleyici ve denetleyici yetkiye sahiptir.[109] SHGM'nin siber güvenlik alanındaki temel düzenlemesi, 1 Nisan 2023 tarihinde yürürlüğe giren Sivil Havacılık İşletmelerine Yönelik Siber Güvenlik Talimatı (SHT-SİBER)'dir.[110]

SHT-SİBER, havaalanları, havayolları, hava trafik yönetimi ve yer hizmetleri sağlayıcıları dahil tüm sivil havacılık işletmelerini kapsamaktadır.[111] Talimat, işletmelerin siber güvenlik politika ve prosedürleri oluşturmasını, risk analizi yapmasını, erişim yönetimi sistemleri kurmasını ve siber olay müdahale mekanizmaları geliştirmesini zorunlu kılmaktadır.

Bildirim yükümlülükleri açısından SHT-SİBER, siber olayların tespit edilmesi durumunda SHGM'ye raporlanmasını öngörmektedir. Talimat'ın 64. maddesi zorunlu bildirimlere ilişkin çerçeveyi belirlemekte, işletmenin belirtilen durumlarda SHGM'yi ivedilikle bilgilendirmesi gerektiğini hükme bağlamaktadır. Kritik havacılık sistemlerini etkileyen olaylar için bildirim süreleri katılaştırılmakta ve olay sonrası detaylı analiz raporları talep edilmektedir. SHGM, bildirimleri değerlendirerek gerekli durumlarda acil güvenlik direktifleri yayımlayabilmektedir.

7. Sağlık Sektörü

Sağlık sektörü, siber güvenlik bildirim yükümlülükleri açısından özellikle karmaşık bir yapı arz etmektedir. Sağlık kuruluşlarının siber

---

108 EPDK Yönetmeliği, m. 1.

109 5431 sayılı Sivil Havacılık Genel Müdürlüğü Teşkilat ve Görevleri Hakkında Kanun, RG: 18.11.2005-25997.

110 Sivil Havacılık İşletmelerine Yönelik Siber Güvenlik Talimatı (SHT-SİBER), 01.04.2023 yürürlük.

111 SHT-SİBER, m. 2.

güvenlik olayları, aynı anda hasta güvenliği riski, kişisel veri ihlali ve kritik altyapı kesintisi boyutlarını içermektedir. Sağlık verileri en hassas kişisel veri kategorisini oluşturduğundan, bu çok boyutlu risk profili sağlık sektöründe paralel bildirim yükümlülüklerinin en yoğun şekilde kesiştiği alanlardan birini oluşturmaktadır.

Türkiye İlaç ve Tıbbi Cihaz Kurumu (TİTCK), 8 Aralık 2021 tarihli Tıbbi Cihaz Yönetmeliği çerçevesinde tıbbi cihazların güvenliği açısından siber güvenlik boyutunu düzenlemektedir.[112] Yönetmelik'in 3. maddesinin (zz) bendi, saha güvenliği düzeltici faaliyetini piyasada bulundurulan bir cihazla ilgili ciddi olumsuz olay riskini önlemek ya da azaltmak amacıyla teknik veya tıbbi nedenlerle imalatçı tarafından yürütülen düzeltici faaliyet olarak tanımlamaktadır.[113] Yazılım içeren veya ağa bağlı tıbbi cihazlarda siber güvenlik zafiyetleri, bu tanım kapsamında ciddi olumsuz olay riski oluşturduğunda bildirim zorunluluğu doğurmaktadır.

Yönetmelik'in 85 ila 89. maddeleri, tıbbi cihaz güvenliği için özel bir gözetim sistemi olan vijilans sistemini düzenlemektedir.[114] Vijilans kapsamında, piyasada bulundurulan cihazların imalatçıları ciddi olumsuz olayları ve saha güvenliği düzeltici faaliyetlerini elektronik sistem vasıtasıyla TİTCK'ya raporlamakla yükümlüdür. İmalatçılar, ciddi olumsuz olayların kaydedilmesi ve raporlanması için bir sisteme sahip olmak zorundadır.[115]

Bildirim süreleri, olayın ciddiyetine göre farklılaştırılmıştır. Ciddi kamu sağlığı tehdidi söz konusu olduğunda imalatçının tehditten haberdar olmasından itibaren 2 gün içinde derhal bildirim yapılması gerekmektedir.[116] Ölüm veya kişinin sağlık durumunda beklenmeyen ciddi bozulma durumunda imalatçının olaydan haberdar olmasından itibaren 10 gün içinde bildirim yapılmalıdır.[117] Diğer ciddi olumsuz

112 Tıbbi Cihaz Yönetmeliği, RG: 02.06.2021 / 31499 (Mükerrer).
113 Tıbbi Cihaz Yönetmeliği, m. 3(zz).
114 Tıbbi Cihaz Yönetmeliği, m. 85-89.
115 Tıbbi Cihaz Yönetmeliği, m. 85(1).
116 Tıbbi Cihaz Yönetmeliği, m. 85(4).
117 Tıbbi Cihaz Yönetmeliği, m. 85(5).

olaylar için ise 15 gün içinde bildirim yapılması gerekmektedir.[118] Bu süre aralığı, diğer düzenleyici kurumların belirsiz veya sabit sürelerinden farklı olarak, risk temelli bir esneklik sunmaktadır.

Yönetmelik'in 87. maddesinin sekizinci fıkrası, saha güvenliği düzeltici faaliyeti hakkındaki bilgilerin bir saha güvenliği bildirimi yoluyla söz konusu cihazın kullanıcılarının dikkatine gecikmeksizin sunulmasını zorunlu kılmaktadır.[119] Bu hüküm, hasta güvenliği perspektifinden siber güvenlik zafiyetlerini değerlendirmektedir. Bir kalp pili, insülin pompası veya ameliyat robotu yazılımındaki zafiyet, doğrudan hasta sağlığını tehdit edebileceğinden acil bildirim gerektirmektedir.

Sağlık kuruluşlarının kişisel veri koruma yükümlülükleri, 21 Haziran 2019 tarihli Kişisel Sağlık Verileri Hakkında Yönetmelik ile özel olarak düzenlenmiştir.[120] Yönetmelik'in 18. maddesi, kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde veri sorumlusu tarafından Kişisel Verileri Koruma Kurulu'na yapılacak bildirimin Kurulun bu hususa ilişkin düzenleyici işlemleri esas alınarak gerçekleştirileceğini hükme bağlamaktadır.[121]

Sağlık sektöründeki bir siber olay, tipik olarak çoklu bildirim kanallarını tetiklemektedir. Eğer saldırı tıbbi cihazları etkilemişse TİTCK'ya vijilans sistemi üzerinden ciddi kamu sağlığı tehdidi durumunda derhal, ölüm veya ciddi bozulma halinde 10 gün içinde, diğer durumlarda 15 gün içinde ciddi olumsuz olay bildirimi yapılması gerekmektedir. Hasta verileri sızmışsa, Kişisel Sağlık Verileri Hakkında Yönetmelik hükümleri çerçevesinde Kişisel Verileri Koruma Kurulu'na en geç 72 saat içinde özel nitelikli kişisel veri ihlali bildirimi yapılmalıdır.[122]

Sağlık sektöründe koordinasyon eksikliğinin sonuçları özellikle ciddidir. Bir siber olay sırasında sağlık kuruluşunun önceliği hasta

---

118 Tıbbi Cihaz Yönetmeliği, m. 85(3).

119 Tıbbi Cihaz Yönetmeliği, m. 87(8).

120 Kişisel Sağlık Verileri Hakkında Yönetmelik, RG: 21.06.2019 / 30808.

121 Kişisel Sağlık Verileri Hakkında Yönetmelik, m. 18(2).

122 KVKK, m. 12(5); Kişisel Verileri Koruma Kurulu Kararı, 2019/10.

güvenliğini sağlamak ve hizmet sürekliliğini restore etmektir. Örneğin bir ilçe devlet hastanesinin hem TİTCK'ya vijilans sistemi üzerinden tıbbi cihaz güvenliği bildirimi, hem Kişisel Verileri Koruma Kurulu'na veri ihlali formu, hem Siber Güvenlik Başkanlığı'na siber olay raporu sunması gerekmektedir. Bu durum, teorik çerçevede tartışılan koordinasyonsuz çokluk maliyetlerinin sektörel bir örneğini teşkil etmektedir.

C. Kişisel Veri İhlali Bildirimi ve KVKK'nın Kesişen Rolü

Kişisel Verileri Koruma Kurulu'nun veri ihlali bildirim yükümlülüğü, paralel yükümlülükler sisteminin kritik bir bileşenidir. KVKK'nın bildirim rejimi, tüm sektörleri kesen yatay bir nitelik taşımakta ve siber güvenlik olaylarının önemli bir kısmını kapsamaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12. maddesinin beşinci fıkrası uyarınca, veri sorumluları kişisel verilerin hukuka aykırı olarak işlenmesi veya erişilmesi durumunda ilgili kişilere ve Kurul'a bildirimde bulunmakla yükümlüdür.[123]

En kısa sürede ifadesinin ne anlama geldiği, 24 Ocak 2019 tarihli ve 2019/10 sayılı KVK Kurulu kararıyla açıklığa kavuşturulmuştur. Karara göre, veri sorumlusunun durumu öğrendiği andan itibaren gecikmeksizin ve Kurul düzenlemeleri çerçevesinde uygulamada en geç 72 saat içinde Kurul'a ihlal bildirimde bulunması gerekmektedir. İhlalden etkilenen kişilerin belirlenmesini müteakip, ilgili kişilere de makul süre içinde bildirim yapılması zorunludur.

Siber güvenlik olayları sıklıkla kişisel veri ihlallerine yol açtığından, KVKK bildirimi paralel yükümlülükler zincirinin önemli bir halkasını oluşturmaktadır. Bir siber saldırı sonucu kişisel veri içeren müşteri verileri sızdığında, kuruluş hem SGB'ye gecikmeksizin hem ilgili sektörel düzenleyiciye (BDDK, SPK gibi), hem de KVKK'ya 72 saat içinde bildirimde bulunmak zorundadır. Her bir bildirim farklı format ve içerik gereklilikleri taşımaktadır. Bu çoklu bildirim yükümlülüklerinin oluşturduğu ağır yük ve potansiyel yaptırım tehdidi,

---

123 6698 sayılı Kişisel Verilerin Korunması Kanunu, RG: 07.04.2016-29677; 6698 sayılı KVKK, m.12/5 ve KVK Kurulu'nun 24.01.2019 tarihli 2019/10 sayılı kararı.

veri sorumlularını bildirimden kaçınmaya ve olayı gizlemeye itebilmektedir; bu durum literatürde bildirim fobisi (*notification-phobia*) olarak adlandırılmakta ve genel siber güvenlik ortamı açısından önemli bir tehdit oluşturmaktadır.[124]

Her kişisel veri ihlali aynı zamanda bir siber olay niteliği taşıma potansiyeli barındırdığından, Kabahatler Kanunu'nun 15. maddesi uyarınca içtima hükümleri ve yetki çatışması değerlendirilmelidir. Ancak içtima sisteminin karmaşıklığı ve uygulamadaki belirsizlikler göz önüne alındığında, her iki mevzuatın da işlerlik kazanması için koordineli bir yaklaşım gerekmektedir.

D. Çakışma ve Belirsizlik Noktaları

Mevcut sektörel bildirim rejimlerinin birlikte işlemesi, uygulamada önemli çakışma ve belirsizlik noktaları oluşturmaktadır. Bu sorunlar, teorik çerçevede tartışılan koordinasyon eksikliğinin somut tezahürleridir ve üç temel kategoride toplanabilir.

İlk olarak, aynı olayın farklı kurumlar tarafından farklı şekilde nitelendirilmesi sorunu bulunmaktadır. Bir siber olay, BTK açısından şebeke güvenliği ihlali, KVKK açısından kişisel veri ihlali, BDDK açısından operasyonel risk olayı, SPK açısından içsel bilgi ve SGB açısından kritik siber olay olarak nitelendirilebilmektedir. Her bir nitelendirme farklı bildirim yükümlülükleri, farklı süreler ve farklı yaptırımlar doğurmaktadır.

Bu durumu somutlaştırmak için tipik bir örnek üzerinden değerlendirme yapmak faydalı olacaktır. Bir bankanın müşteri verilerinin sızdığı bir siber saldırı durumunda, aynı olay BDDK'ya siber olay yönetim prosedürü çerçevesinde raporlama, TCMB'ye (ödeme sistemleri etkilenmişse) derhal bilgilendirme, KVKK'ya Kurul düzenlemeleri uyarınca uygulamada en geç 72 saat içinde, SPK'ya (halka açık bankaysa) KAP üzerinden kamuyu aydınlatma, SPK Sektörel

---

[124] Mehmet Bedii Kaya, "Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law", *Annales de La Faculté de Droit d'Istanbul* 70 (31 Aralık 2021), 195-241.

SOME'sine düzenli raporlama ve SGB'ye gecikmeksizin bildirim yapılması gerekmektedir. Kuruluş, saldırıyı bertaraf etmeye çalışırken aynı zamanda dört veya beş farklı kuruma farklı format ve içerikte bildirimler hazırlamak zorunda kalmaktadır.

Kurum	Bildirim Süresi	Hukuki Dayanak
SGB	Gecikmeksizin	7545 sayılı Kanun m.7(1)(b)
BDDK	Prosedür çerçevesinde raporlama	Bilgi Sistemleri Yönetmeliği m.18
SPK	Derhal	VII-128.10 Tebliği m.24(4)
BTK	En kısa sürede	Şebeke ve Bilgi Güvenliği Yönetmeliği m.38
KVKK	En geç 72 saat	KVKK m.12(5), 2019/10 sayılı Kurul Kararı
TCMB	Derhal	6493 sayılı Kanun m.23 31676 sayılı Tebliğ m.7
TİTCK	Derhal / 10 gün / 15 gün	Tıbbi Cihaz Yönetmeliği m.85-88
SHGM	İvedilikle	SHT-Siber Talimatı m.13(2)

İkinci olarak, kuruluşlar, siber olayın kritik aşamasında tüm kaynaklarını olay müdahalesine seferber etmek isterken, aynı zamanda farklı kurumlara zaman baskısı altında bildirim yapmak zorunda kalmaktadır. Bu durum, özellikle kaynakları sınırlı küçük ve orta ölçekli işletmeler için orantısız bir yük oluşturmaktadır. Örneğin bir fintech girişiminin hem BDDK'ya, hem KVKK'ya, hem SPK'ya, hem de SGB'ye bildirim yapması gerekmekte, ancak bu kurumların hiçbirinin KOBİ ölçekli bir bildirim formatı bulunmamaktadır.

Üçüncü olarak, format ve kanal farklılıkları bulunmaktadır. BTK şebeke operatörleri için raporlama ve geri bildirim mekanizması, BDDK bankalara özgü siber olay yönetim prosedürü, SPK'nın KAP sistemi ve SOME raporlama formatları, KVKK'nın veri ihlali bildirim formu ve SGB'nin oluşturacağı merkezi bildirim platformu farklı veri alanları, teknik detay seviyeleri ve raporlama mantıkları içermektedir. Bir kuruluşun aynı olayı farklı formatlara uyarlayarak birden fazla kanala girme zorunluluğu, mükerrer raporlama yükü oluşturmaktadır. Bu yük, özellikle sınırlı kaynaklara sahip küçük ve orta ölçekli işletmeler için orantısız maliyetler doğurmaktadır.

Son olarak, siber olay ile zafiyet ayrımı belirsizlik kaynağıdır. SGB hem siber olayları hem de zafiyetleri kapsarken, diğer kurumlar ağırlıklı olarak gerçekleşmiş olaylara odaklanmaktadır. Bir kuruluşun tespit ettiği ancak henüz istismar edilmemiş kritik bir zafiyet, SGB'ye bildirilmeli midir? Eğer bu zafiyet üçüncü taraf bir yazılımda tespit edilmişse ve birden fazla sektörü etkiliyorsa, hangi sektörel düzenleyiciye bildirilmelidir? Zafiyet bildirimi sonrasında düzenleyici kurumların koordinasyonu nasıl sağlanacaktır? Bu sorular mevzuatta açık karşılık bulamamaktadır.

Tüm bu çakışma ve belirsizlik noktaları, Türkiye'de siber olay bildiriminin bugün itibarıyla çoklu paralel raporlama rejimine tabi olduğunu göstermektedir. Aynı olay, farklı hukuki niteliklerle, farklı sürelerde, farklı formatlarda, farklı kurumlara bildirilmek zorundadır. Bu durum, büyük kurumlar için operasyonel yük, KOBİ'ler için ise uyumdan vazgeçme riski doğurmaktadır.

Bu paralel yapı kalıcı bir durum değildir. SGB'nin ikincil düzenlemelerle kuracağı eşgüdümlü bildirim çerçevesi, teorik çerçevede tartışılan meta-regülasyon modelini hayata geçirebilir. Başkanlık, tek giriş noktası oluşturarak operatörlerin bildirim yükünü azaltabilir, sektörel kurumlarla otomatik bilgi paylaşımı protokolleri kurarak uzmanlık kaybını önleyebilir ve risk temelli kademeli bildirim standartları belirleyerek süre çatışmalarını çözebilir. Bu dönüşüm, Bölüm IV'te önerilen eşgüdümlü yönetişim modelinin temelini oluşturacaktır.

IV. Eşgüdümlü Bildirim Çerçevesi Önerisi

A. Meta-Regülasyon Perspektifinden Model Tasarımı

Paralel bildirim rejimlerinin ortaya çıkardığı koordinasyon sorununa çözüm, meta-regülasyon yaklaşımıyla kurulmalıdır.[125] Meta-

[125] Sektörel düzenleyici kurumlar da dahil olmak üzere bağımsız idari otoritelerin anayasal statüye kavuşmasının önemi ve bu statünün koordinasyon mekanizmalarıyla ilişkisi için bkz. Akgün, "Bağımsız İdari Otoritelerin Anayasal Statüsünün Belirlenmesi İhtiyacı: Teorik ve Pratik Gerekçeler".

regülasyon, düzenleyiciyi düzenleyen bir üst koordinasyon katmanı olarak çalışır; farklı otoritelerin faaliyetlerini uyumlandırır, tutarlılığı sağlar ve ortak standartlar etrafında bilgi akışını kolaylaştırır.[126] Bu çerçevede Siber Güvenlik Başkanlığı'nın rolü, doğrudan tüm bildirimleri tek başına yönetmekten çok, düzenleyici alanlar arasında etkileşimi yöneten ve ortak dili kuran bir meta-regülatör olarak yeniden tanımlanmalıdır. Düzenleyici otorite, bir orkestra şefi gibi farklı aktörlerin uzmanlığını muhafaza ederken senkronizasyonu sağlar; sürecin her adımını tek elde toplamadan çerçeveyi kurar ve işler hale getirir. ENISA'nın ulusal CSIRT'ler arasında ağ kuran, ortak tatbikatları ve bilgi paylaşım altyapısını işleten rolü, bu modelin pratik karşılığıdır.[127]

Tek giriş-çok çıkış mimarisi, bu meta-regülasyonun somut mekanizmasıdır. Tek giriş, tüm sektörler için ortak bir bildirim kapısının varlığını ifade eder. Başkanlık tarafından işletilen standart bir bildirim formu ve ortak veri sözlüğü üzerinden yapılan tekil başvuru, aynı anda yetkileri ve ilgi alanları farklı kurumlara dağıtılacak şekilde kurgulanır. Çok çıkış ise bu tek başvurunun akıllı yönlendirme ile ilgili düzenleyici kurumlara, sektörel SOME'lere ve gerektiğinde adli veya idari mercilere eşzamanlı iletilmesini ifade eder. Böylece epistemik merkezsizlik korunur; her kurum kendi risk perspektifini, yöntembilimini ve sektörel uzmanlığını sürdürürken mükerrer raporlama ve bilgi parçalanması en aza indirilir.

Mimarinin teknik altyapısı üç bileşenden oluşur. Birincisi, operatörlerin erişeceği merkezi bildirim portalıdır. Portal, kullanıcı dostu arayüz sunmalı, rehberli bildirim süreçleri içermeli ve hem acil bildirimler hem de detaylı raporlar için farklı formlar sağlamalıdır. İkincisi, olay sınıflandırma ve yönlendirme motorudur. Motor, bildirimin içeriğini analiz ederek hangi sektörel düzenleyicilerin bilgilendirilmesi gerektiğini otomatik olarak belirler ve ilgili kurumlara

---

[126] Koliba vd., *Governance Networks in Public Administration and Public Policy*, 179.

[127] Adams vd., "The Governance of Cybersecurity : A Comparative Quick Scan of Approaches in Canada, Estonia, Germany, the Netherlands and the UK", 98-99.

uygun formatta veri iletir. Üçüncüsü, kurumlar arası veri paylaşım altyapısıdır. Bu altyapı, sektörel düzenleyicilerin kendi sistemlerine entegre olabilecek API'ler sağlar ve gerçek zamanlı veri senkronizasyonu mümkün kılar.

Yönlendirme algoritması çok boyutlu bir matriks üzerinde çalışır. Olayın sektörü, etki alanı, kritiklik seviyesi ve yasal yükümlülük tetikleyicileri algoritmanın temel parametreleridir. Örneğin bir bankanın ödeme sistemlerini etkileyen ransomware saldırısında, sistem otomatik olarak BDDK'yı operasyonel risk açısından, TCMB'yi ödeme sistemleri açısından, KVKK'yı müşteri verileri etkilenmişse kişisel veri ihlali açısından ve SPK'yı halka açık banka ise piyasa bilgilendirmesi açısından haberdar eder. Her kurum kendi bakış açısından ihtiyaç duyduğu veri setine erişirken, operatör yalnızca bir kez bildirim yapmış olur.

Ortak veri sözlüğü, bu mimarinin dili ve omurgasıdır. Kurumlar arası kavram birliğini sağlayan tanımlar seti, bildirimlerde aynı terimlerin aynı anlama gelmesini güvenceye alır ve karşılaştırılabilirliği mümkün kılar. Sözlük üç katmandan oluşur. İlk katman, tüm bildirimlerde zorunlu olan minimum ortak veri setidir: olay tespit zamanı, bildirim zamanı, olayın kısa özeti, etkilenen sistem veya hizmet tanımı, etkilenen kullanıcı veya müşteri sayısı tahmini, olayın devam durumu ve bildirimi yapan kuruluşun kimlik bilgileri.

İkinci katman, sektörel özelleşmiş veri setleridir. Her sektörel düzenleyici, kendi risk perspektifinden ihtiyaç duyduğu ek veri alanlarını tanımlar. BDDK için finansal etki tahmini ve likidite riskleri; BTK için etkilenen altyapı kapasitesi ve servis kesinti süresi; KVKK için etkilenen veri kategorileri ve alınan koruyucu önlemler sektöre özgü bilgileri içerir. Bu özelleşmiş setler, ortak terminoloji sözlüğünü kullanır ve standart formatlara uyar.

Üçüncü katman, kavramsal tanımları netleştiren terminoloji sözlüğüdür. Siber olay, bilgi varlıklarının gizlilik, bütünlük veya erişilebilirliğini yahut hizmet sürekliliğini etkileyen her türlü vakayı kapsayan şemsiye bir terimdir. Sızıntı, yetkisiz ifşa veya sızdırma yoluyla ortaya çıkan ve ağırlıkla gizlilik boyutunu ihlal eden alt türdür.

Kişisel veri ihlali ise sızıntının özel bir hali olarak konumlanır; ancak kişisel veriye ilişkin rejim kendi meşru menfaatini koruduğundan, sözlükte yer alan tanımlarla KVKK terminolojisi arasında açık eşleştirme sağlanır.

Risk temelli kademeli bildirim, bu modelin çalışma usulüdür. Belirsizliği yönetmek ve farklı düzeyde müdahaleyi mümkün kılmak için sistem üç aşamada işler. İlk bildirim, olayın tespit edilmesinden itibaren sektörel risk profiline ve olayın kritikliğine göre belirlenecek makul süre içinde yapılır. Bu aşamada minimum bilgi seti yeterlidir: olayın başlangıç zamanı, tipi, etkilenen sistemler, olayın devam durumu ve ilk müdahale. Bu bildirim, düzenleyici kurumların durumun farkında olmasını ve gerekirse acil koordinasyon başlatmasını sağlar.

Detaylı bildirim, ilk bildirimi takiben sektörel düzenleyicilerin belirlediği ve olayın karmaşıklığı ile orantılı süre zarfında sunulur. Bu aşamada olayın kapsamı, etkilenen kullanıcı sayısı, veri ihlali durumu, alınan teknik ve organizasyonel önlemler ile kök neden analizinin ilk bulguları raporlanır. Bu süre, kurumların olayı analiz etmesi için yeterli esnekliği sağlarken düzenleyicilerin zamanında müdahale etmesine imkân tanır. Finansal sektörde sistemik risk taşıyan olaylar için daha kısa süreler öngörülürken, karmaşık tedarik zinciri saldırılarında makul gerekçelerle daha uzun süreler tanınabilir.

Nihai rapor, olayın çözümlenmesinden itibaren sektörel standartlara ve olayın niteliğine göre belirlenecek süre içinde tamamlanır. Rapor, tam kök neden analizi, alınan kalıcı önlemler, çıkarılan dersler ve benzer olayların önlenmesi için yapılan değişiklikleri içerir. Bu rapor, düzenleyici kurumların sektörel öğrenme sağlaması ve gerekirse düzenleme değişiklikleri yapması için kritik öneme sahiptir.

Başkanlığın bu mimariyi kurma yetkisi, 7545 sayılı Kanun'un 7. maddesinden kaynaklanır.[128] Bilişim sistemleri üzerinden faaliyet gösteren, veri toplayan ve işleyen kişi ve kuruluşların zafiyet veya siber olayları gecikmeksizin bildirme ödevi,[129] ortak usul ve esaslarla tek giriş-çok çıkış modeline uyarlanır. Başkanlık, maddenin üçüncü fıkrasının

[128] 7545 sayılı Kanun, m. 7.

[129] 7545 sayılı Kanun, m. 7(1)(b).

tanıdığı ikincil düzenleme yetkisiyle[130] tek formu, yönlendirme mantığını ve standartları belirler. Sektör otoritelerinin uzmanlığı korunurken, Başkanlık üst düzey koordinasyonu sağlayan gerçek bir meta-regülatör haline gelir.

İkincil düzenlemenin tasarımında dört ilke gözetilmelidir. Birincisi, sektörel düzenleyici kurumların mevcut yetkileri korunmalı; SGB düzenlemesi bu yetkileri ortadan kaldırmak yerine koordine etmelidir. İkincisi, protokol sistemi kurulurken sektörel kurumların aktif katılımı sağlanmalı; tek taraflı dayatma yerine müzakereli bir süreç izlenmelidir. Üçüncüsü, geçiş süreci için yeterli süre tanınmalı ve pilot uygulamalarla sistem test edilmelidir. Dördüncüsü, özellikle KOBİ'ler için orantılılık ilkesi gözetilmeli ve uyum maliyetleri minimize edilmelidir.

Önerilen model, sektörel çeşitliliği ortadan kaldırmayı değil, koordine etmeyi amaçlar. Dengeli modelde, sektörel kurumlar kendi alanlarında ek bilgi ve belge talep etme, sektörel risk değerlendirmesi yapma, özel denetim ve inceleme başlatma, sektöre özgü rehber ve standartlar yayımlama ile kendi mevzuatı çerçevesinde yaptırım uygulama yetkilerini korur. SGB'nin üst düzey koordinasyon yetkileri ise ortak standartlar ve minimum gereklilikler belirleme, kurumlar arası bilgi akışını düzenleme, çapraz sektörel riskleri tespit ve koordine etme, ulusal düzeyde siber tehdit istihbaratını paylaşma ile kurumlar arası çalışma grupları ve ortak tatbikatlar organize etmeyi kapsar.

Kamu menfaatinin belirli bir paydaş kitlesine yoğunlaştığı hallerde çıkış kanalı menfaat temelinde ayrıştırılır. Yatırımcı menfaatine ilişkin gelişmelerde Kamuyu Aydınlatma Platformu'nun işlevi korunur. Tek girişte yapılan bildirim, sermaye piyasası mevzuatındaki açıklama yükümlülükleriyle uyumlu olacak şekilde KAP'a yönlendirilir veya özdeş kabul edilir. Kişisel veri ihlalleri, KVKK rejiminin koruduğu menfaatler gözetilerek Başkanlık-KVKK eşgüdümünde ele alınır. Tek formun KVKK bakımından geçerliliği mutabakatla tesis edilir ya da hızlı bir eşleştirme mekanizması işletilir.

---

[130] 7545 sayılı Kanun, m. 7(3).

Yükümlülüklere uyulmaması halinde idari yaptırımların farklı rejimler boyunca art arda uygulanması, içtima ve yetki çatışması bakımından değerlendirilmelidir.[131] Bir siber güvenlik olayı bildirim yükümlülüğünün ihlali tespit edildiğinde, SGB öncelikle diğer ilgili kurumları bilgilendirir. Kurumlar arasında koordinasyon toplantısı yapılarak hangi kurumun hangi açıdan yaptırım uygulayacağı belirlenir. AAynı fiil farklı hukuki niteliklere sahipse, her kurum kendi alanına giren ihlaller bakımından yaptırım uygulayabilir; ancak aynı fiil nedeniyle birden fazla idari para cezasının kümülatif biçimde uygulanması, 5326 sayılı Kabahatler Kanunu'nun genel kanun niteliği ve m. 15'te yer alan içtima hükümleri ile Anayasa'daki *ne bis in idem* ve orantılılık ilkeleri çerçevesinde sınırlandırılmak zorundadır. Yaptırım kararları arasında çelişki olmaması için, her kurum diğer kurumların tespitlerini dikkate alır ve gerekçeli kararlarında buna atıfta bulunur.

Bu öneri, tek kapıdan giren bilginin doğru kurumlara eşzamanlı ve amaçla uyumlu şekilde ulaşmasını, herkesin aynı kavram setiyle konuşmasını ve düzenleyici çoğulluğun koordinasyon içinde işlemesini hedefler. Model, operatörlerin mükerrer raporlama yükünü ortadan kaldırırken her düzenleyici kurumun kendi perspektifinden risk değerlendirmesi yapmasını mümkün kılar.

B. Karşılaştırmalı Analiz Işığında Türkiye Modeli

Avrupa Birliği'nde NIS2'nin üye devletlere bıraktığı aktarma esnekliği, pratikte 27 farklı uygulamaya evrilerek çok uluslu teşebbüsler için dağınık ve maliyetli bir bildirim panoraması oluşturmuştur. Komisyon bu parçalanmayı gidermek üzere 17 Ekim 2024 tarihli 2024/2690 sayılı Uygulama Tüzüğü ile dijital altyapı ve belirli platform sağlayıcıları bakımından hem risk yönetimi tedbirlerinin teknik-metodolojik gereklerini hem de hangi hallerde olayın önemli sayılacağını yeknesak biçimde tanımlamak zorunda kalmıştır.[132]

---

131 7545 sayılı Kanun, m. 16(10).

132 Commission Implementing Regulation (EU) 2024/2690, olayın önemli sayılacağı haller ve risk yönetimi gerekleri ile eşiklerin standardizasyonu; örn. finansal kayıp, kesinti ve kullanıcı etkisi kriterleri ile yatay-sektör özel hükümler.

Tüzük, ISO/IEC 27001 ve Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute - ETSI) EN 319 401 gibi standartlara yaslanan ortak bir çerçeve kurarken, olay kritikliğini ölçülebilir eşiklere bağlamaktadır. Örneğin doğrudan finansal kaybın 500 bin avroyu veya yıllık cironun yüzde beşini aşması, otuz dakikayı geçen tam kesinti, bir saatten uzun sınırlı erişilebilirlik ya da Birlikteki kullanıcıların en az yüzde beşi veya bir milyonunun etkilenmesi gibi kriterler, bulut, veri merkezi, içerik dağıtım ağı, alan adı sistemi ve çevrimiçi pazar yeri sağlayıcıları için ayrıntılı olarak sayılmaktadır. Bu yaklaşım, olay sınıflandırmasını yoruma açık genel kavramlardan çekip veriyle doğrulanabilir somut eşiklere taşımakta ve üye devletlerdeki raporlama kararlarını uyumlu hale getirmektedir.

Türkiye açısından, III. bölümde haritalandırılan çok katmanlı yapıda her kurumun farklı eşikler kullanması sorunu, SGB ikincil düzenlemelerinde AB benzeri nicel kriterlerle çözülebilmektedir. IV. A'da önerilen ortak veri sözlüğü, bu eşikleri standartlaştırarak hem kurumlardaki değerlendirmeyi nesnelleştirebilecek hem de tek giriş-çok çıkış mimarisinde veri tekrarını azaltabilecektir. AB'nin 27 ülkeyi uyumlaştırma çabası Türkiye'de baştan tek bir koordineli sistemle aşılabilmektedir.

NIS2'de olay zaman çizelgesi üç aşamalı bir akış olarak sabitlenmiştir; farkına varılmasından itibaren en geç yirmi dört saat içinde erken uyarı, yetmiş iki saat içinde olay bildirimi ve bir ay içinde nihai rapor sunulmaktadır. Erken uyarı sonrasında CSIRT'in mümkün olduğunca yirmi dört saat içinde ilk geri bildirim sağlaması, teknik yönlendirme ve azaltım tavsiyesini hızlandıran bir temas noktası oluşturmaktadır.[133] Türkiye'de SGB'nin belirleyeceği birinci bildirim penceresini yirmi dört saatle hizalamak, III. bölümde görülen farklı süre pencerelerini koordine edebilmektedir. KVKK'nın 72 saati, SPK'nın derhal kuralı ve BTK'nın en kısa sürede ifadesi bu koordinasyon kapsamında uyumlaştırılabilmektedir. IV. A'da önerilen risk temelli

[133] NIS2 m. 23 uyarınca erken uyarı 24 saat, olay bildirimi 72 saat ve nihai rapor 1 ay; CSIRT'in mümkün olduğunca 24 saat içinde geri bildirimine ilişkin hüküm.

kademeli bildirim, NIS2'nin üç aşamalı yapısını doğrudan benimseyerek uluslararası uyumluluğu sağlayabilmektedir.

Finans alanında DORA, NIS2'ye göre daha ileri bir bütünleşme örneğini temsil etmektedir ve NIS2 karşısında *lex specialis* konumundadır. DORA'nın 17 Ocak 2025'te uygulanmaya başlamasıyla finansal kuruluşların büyük bilgi teknolojileri olaylarını bildirmesinde Birlik çapında ortak bir usul dili oluşmuştur; Komisyonun 2025/302 sayılı Uygulama Tüzüğü, majör bilgi teknolojileri olayı ve önemli siber tehdit bildirimlerinde kullanılacak standart formları ve prosedürleri belirlemiştir.[134] DORA'nın bu konsolidasyon gücü ödeme hizmetleri sektöründe somut biçimde görülmektedir. Ödeme Hizmetleri Direktifi 2'nin (Payment Services Directive 2 - PSD2) 96. maddesi ödeme hizmeti sağlayıcılarına büyük operasyonel veya güvenlik olaylarını yetkili otoriteye bildirme yükümlülüğü getirmiştir. DORA'nın 7. maddesi PSD2'yi değiştirerek, kredi kurumları, ödeme kurumları, hesap bilgisi hizmeti sağlayıcıları ve elektronik para kurumları bakımından PSD2 madde 96'nın 1 ila 5. fıkralarının uygulanmayacağını ve bunun yerine DORA'nın olay bildirim mekanizmasının geçerli olacağını hükme bağlamıştır.[135] Bu düzenleme, idari yükü azaltmak ve mükerrer bildirim gerekliliklerinden kaçınmak amacıyla tek ve tam uyumlu bir olay bildirim mekanizması oluşturmuştur.

Bu çerçevede, Komisyon'un 18 Kasım 2025 tarihli Digital Omnibus Tüzük taslağı, çalışmada teşhis edilen parçalı bildirim mimarisinin Birlik düzeyinde de sistemik bir sorun olarak görüldüğünü teyit eden bir gelişme olarak okunmalıdır.[136] Taslak, GDPR, NIS2,

---

134 DORA temel çerçevesi ve uygulamaya başlama tarihi; majör BT olayı bildirimine ilişkin standart form ve prosedürleri belirleyen Komisyon Uygulama Tüzüğü 2025/302; NIS2-DORA ilişkisinde lex specialis kılavuzu.

135 DORA m. 7 ile PSD2 m. 96'ya eklenen 7. fıkra; DORA dibace 54'te operasyonel veya güvenlik ödeme ile ilgili olayların ICT niteliği taşıyıp taşımadığına bakılmaksızın DORA kapsamında raporlanması.

136 Avrupa Komisyonu, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative

DORA, eIDAS ve CER kapsamındaki siber olay ve veri ihlali bildirimlerini, ENISA tarafından işletilecek tek bir giriş noktasında birleştirmeyi; böylece aynı olay bakımından farklı metinlere göre ayrı ayrı bildirim yapılmasından kaynaklanan idari yükü azaltmayı amaçlamaktadır. Aynı zamanda GDPR'daki veri ihlali bildirim süresinin yetmiş iki saatten doksan altı saate çıkarılması ve denetim otoritesine bildirim yükümlülüğünün yalnızca yüksek risk içeren ihlallerle sınırlandırılması öngörülmektedir. EDPB'nin ortak bir ihlal bildirim şablonu ve yüksek risk sayılacak durumlara ilişkin yeknesak bir liste hazırlamakla görevlendirilmesi, hem veri koruması hem siber güvenlik ekseninde ortak veri sözlüğü ve standardize edilmiş raporlama mantığının tesisi yönünde atılmış tipik bir meta-regülasyon adımıdır. Böylece AB, NIS2, DORA ve GDPR'ın paralel ve kısmen çakışan bildirim rejimlerinin yarattığı "notification fatigue" sorununa, senkronize ve tek kapılı bir mimariyle yanıt vermeye çalışmaktadır.

III. bölümde görüldüğü üzere, Türkiye'de BDDK-SPK-TCMB üçgeninde en yoğun koordinasyon problemi yaşanmaktadır. Aynı finansal kuruluş aynı siber olayı hem BDDK'ya operasyonel risk bildirimi, hem TCMB'ye ödeme sistemleri bildirimi, hem SPK'ya piyasa bilgilendirmesi olarak raporlamak zorunda kalmaktadır. IV. A'da önerilen model, DORA mantığıyla sektörel özelleşmiş veri setleri içeren tek bir formu öngörmektedir. PSD2'nin DORA'ya devri, ödeme sistemleri bakımından TCMB bildirimi ile SGB bildirimi arasında benzer bir konsolidasyon için emsal teşkil etmektedir. Her kurum kendi alanında ek bilgi talep etme ve yaptırım uygulama yetkilerini korurken, temel bildirim tek kapıdan yapılabilmektedir.

Sermaye piyasası şeffaflığı açısından 596/2014 sayılı Piyasa Dolandırıcılığı Tüzüğü'nün (Market Abuse Regulation - MAR) 17. maddesi de önemli bir kesişim noktası oluşturmaktadır. MAR, ihraççıların kendilerini doğrudan ilgilendiren içsel bilgileri mümkün olan en kısa sürede kamuya açıklama yükümlülüğünü

framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final, 19.11.2025.

düzenlemektedir.[137] Siber güvenlik olayları, operasyonel faaliyetleri, mali durumu veya itibarı önemli ölçüde etkileyen nitelikte olduğunda MAR madde 17 kapsamında içsel bilgi niteliği kazanabilmekte ve derhal açıklanması gerekmektedir.[138] Türkiye'de SPK'nın II-15.1 sayılı Özel Durumlar Tebliği, MAR madde 17'nin işlevsel karşılığını oluşturmaktadır ve halka açık ortaklıkların içsel bilgileri KAP üzerinden derhal açıklamasını öngörmektedir.[139]

III. bölümde haritalanan üç ayrı bildirim kanalının farklı format ve muhataplara hitap etmesi, operasyonel yük oluşturmaktadır. SGB, SPK ve KAP bildirimleri farklı amaçlara hizmet etmektedir. Ancak bu çoklu yapının tamamıyla rasyonalizasyona tabi tutulması mümkün değildir: SGB ve SPK bildirimleri düzenleyici otoritelere yönelik idari gözetim amaçlı iken, KAP bildirimleri doğrudan yatırımcı koruması ve piyasa güvenini sağlama amacına hizmet etmektedir.[140] Bu nedenle

---

137 Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC), OJ L 173, 12.6.2014, art. 17.

138 İçsel bilgi tanımı için bkz. MAR, art. 7. İçsel bilgi, "kamuya açıklanmamış, spesifik nitelikte olan, doğrudan veya dolaylı olarak bir veya birden fazla ihraççı veya bir veya birden fazla finansal araca ilişkin bulunan ve kamuya açıklanması halinde söz konusu finansal araçların veya bunlarla ilgili türev finansal araçların fiyatı üzerinde önemli bir etkisi olması muhtemel olan bilgi" şeklinde tanımlanmaktadır.

139 Sermaye Piyasasında Özel Durumların Kamuya Açıklanmasına İlişkin Tebliğ (II-15.1), 23.01.2014 tarihli ve 28891 sayılı Resmi Gazete'de yayımlanmıştır. Tebliğ'in 2. maddesi "özel durum açıklaması" olarak "ortaklığın yatırım kararlarını etkileyebilecek nitelikteki finansal durumu, faaliyetleri ve bunlara ilişkin öngörü, beklenti ve tahminlerinde meydana gelen değişikliklere ve ortaklıkla ilgili olarak sermaye piyasasında oluşan fiyatın etkilenmesine neden olabilecek her türlü olay ve gelişmelere ilişkin açıklama" tanımını vermektedir.

140 MAR'ın preamble (preambule) bölümünde yatırımcı güveni ve piyasa bütünlüğü vurgusu için bkz. MAR, Recital 1-3. KAP'ın kuruluş amacı için bkz. 6362 sayılı Sermaye Piyasası Kanunu, m. 15.

KAP'ın ayrı bir bildirim mekanizması olarak korunması, farklı menfaat sahiplerinin bilgi ihtiyaçlarını karşılama açısından gerekli olabilecektir.

Ürün odaklı güvenlikte CRA, üreticinin yaşam döngüsü boyunca risk yönetimini ve koordineli zafiyet açıklamasını merkeze almaktadır. 2024/2847 sayılı Tüzük, aktif olarak istismar edilen zafiyetlerin ve ürün güvenliğini etkileyen ciddi olayların ENISA tarafından işletilecek tekil raporlama platformu üzerinden bildirilmesini ve ulusal CSIRT ile eş zamanlı bildirim yapılmasını öngörmektedir.[141] Türkiye'de 7545 sayılı Siber Güvenlik Kanunu kapsamında da ürün güvenliğine ilişkin düzenlemeler bulunmaktadır. Kanun madde 5/h uyarınca Siber Güvenlik Başkanlığı, kamu kurum ve kuruluşları ile kritik altyapıların bilişim sistemlerinde kullanılacak ve siber güvenliğe etkisi olan yazılım, donanım, ürün ve hizmetlere dair kriterleri belirleme yetkisine sahiptir. Aynı Kanun madde 7 uyarınca siber güvenlik ürün, sistem, yazılım, donanım ve hizmetleri üreten şirketlerin faaliyet öncesi Başkanlıktan onay alması, sertifikasyon ve belgelendirmeye tabi olması öngörülmektedir. Kanun madde 8/c gereği kamu kurumları ve kritik altyapılarda kullanılacak siber güvenlik ürün, sistem ve hizmetleri yalnızca Başkanlık tarafından yetkilendirilmiş ve belgelendirilmiş siber güvenlik uzmanlarından, üreticilerden veya şirketlerden tedarik edilmelidir. Kanun madde 8/b bilişim sistemleri üzerinden hizmet sunanları, tespit ettikleri zafiyet veya siber olayları gecikmeksizin Başkanlığa bildirmekle yükümlü kılmaktadır. III. bölümde görüldüğü üzere zafiyet bildirimine ilişkin usul ve esaslar henüz bütünleşik bir zemine kavuşmamıştır. IV. A'da önerilen zafiyet koordinasyon platformunun ENISA'nın tekil platformu ve CVE (Common Vulnerabilities and Exposures - Ortak Zafiyetler ve Açıklıklar) gibi küresel ekosistemle birlikte çalışabilir şekilde tasarlanması, CRA'nın ürün güvenliği yaklaşımını Türkiye'ye taşıyabilmektedir. CRA'nın aktif istismar için 24 saat, zafiyet bildirimi için 72 saat, nihai rapor için 14 gün şeması, SGB düzenlemesinde zafiyet hattı için uyarlanabilmektedir.

---

[141] CRA, 2024/2847 sayılı Tüzük m. 14 ve 16; üreticinin aktif istismar edilen zafiyet ve ciddi olay bildirimleri için ENISA'nın kuracağı tekil platforma raporlama yükümlülüğü.

Yatay veri korumasında Genel Veri Koruma Tüzüğü'nün (General Data Protection Regulation - GDPR) 33. maddesi, denetim otoritesine yapılacak kişisel veri ihlali bildirimi için en geç yetmiş iki saatlik bir pencere getirmektedir. NIS2 Direktifi'nin 2. maddesinin 12. fıkrası, bu Direktif'in GDPR ve e-Gizlilik Direktifi'ne halel getirmeksizin uygulanacağını açıkça hükme bağlamıştır. Direktif'in 35. maddesi kişisel veri ihlaliyle kesişimde yetkili otorite işbirliğini düzenlerken, dibaceler bu ilişkiyi daha da netleştirerek GDPR anlamında kişisel veri ihlali olan durumların NIS2 kapsamında bildirilmeyeceğini, ancak kişisel veriyi etkileyen fakat GDPR anlamında veri ihlali teşkil etmeyen siber olayların NIS2 kapsamında raporlanacağını belirtmektedir.[142] Bu ayrım, iki rejim arasında çifte raporlamayı önleyen açık bir koordinasyon mekanizması kurmaktadır.

III. bölümde görüldüğü üzere, Türkiye'de SGB ile KVKK arasında benzer bir açık koordinasyon hükmü bulunmamaktadır. Kurul'un 2019/10 sayılı kararıyla içtihatlaşan yetmiş iki saat kuralının SGB'nin yirmi dört saatlik erken uyarı şemasıyla eşleştirilmesi belirsizlik getirmektedir. IV. A'da önerilen modelin SGB ikincil düzenlemesinde NIS2-GDPR koordinasyonuna paralel bir madde içermesi kritiktir. Kişisel veri ihlali teşkil eden siber olaylar KVKK'ya bildirilip, bu bildirimin SGB'ye de iletilmesi yeterli kabul edilebilmektedir. Diğer taraftan, kişisel veri ihlali teşkil etmeyen ancak siber güvenlik boyutu olan olaylar SGB'ye bildirilmektedir. Ancak hangi durumların sadece KVKK'ya, hangi durumların sadece SGB'ye, hangi durumların ise her ikisine birden bildirileceği açık hükümlere bağlanmalıdır.

Elektronik haberleşmede NIS2'nin yürürlüğe girmesiyle Avrupa Elektronik Haberleşme Kodu'nun (*European Electronic Communications Code - EECC*) 40 ve 41. maddelerindeki ulusal güvenlik ve olay bildirimi rejiminin yürürlükten kalkması, bu alandaki raporlamayı NIS2 şemsiyesi altına toplamıştır. Türkiye'de BTK'nın şebeke ve bilgi

---

[142] GDPR m. 33'te 72 saatlik veri ihlali bildirimi; NIS2 Direktifi m. 2(12) GDPR ve e-Privacy Direktifi'ne halel getirmeme, m. 35 kişisel veri ihlaliyle kesişimde yetkili otorite işbirliği ve dibaceler'de "without prejudice" vurgusu ile iki rejim arasındaki koordinasyon mekanizması; NIS2 m. 31(3) ulusal siber güvenlik otoritelerinin GDPR denetim otoriteleriyle iş birliği.

güvenliği bildirim sisteminin SGB portalıyla veri eşleştirmesi kurması buradaki iş yükünü azaltabilecektir.

AB'de NIS2'nin iş birliği mimarisi, ulusal CSIRT ağı ile AB Siber Kriz İrtibat Ağı (*EU Cyber Crisis Liaison Organisation Network - EU-CyCLONe*) arasında kurulan operasyonel katmanı öne çıkarmaktadır. Erken uyarıyı takiben mümkün olduğunca yirmi dört saat içinde verilecek geri bildirim ve yönlendirme, ulusal teknik kapasite ile Birlik düzeyindeki operasyonel eş güdüm arasında hızlı bir arayüz ortaya çıkarmaktadır.[143] Türkiye'de USOM'un SGB bünyesine devri, bu operasyonel katmanın ulusal ayağını güçlendiren bir fırsattır. IV. A'da önerilen CSIRT yapısının EU-CyCLONe benzeri bir ulusal kriz bağ dokusu kurması, sektörel SOME'lerin kapatılması anlamına gelmeden tek giriş-çok çıkış akışını hızlandırma potansiyeli bulunmaktadır.

Dağınıklığı azaltan asıl fark, AB'de standardizasyonun ayrıntı düzeyidir. NIS2 Direktifi'ni uygulayan 2024/2690 sayılı Komisyon Uygulama Tüzüğü ile birlikte, olayların ne zaman "önemli" sayılacağı açık ölçütlerle belirlenmiştir: etkilenen kullanıcı sayısı, kesinti süresi, veri gizliliğine etkisi, finansal kayıp tutarı ve tekrarlayan olayların birikimli etkisi gibi somut kriterler bulunmaktadır. Finans sektöründe de DORA Tüzüğü ve ilgili uygulama düzenlemeleri, bildirim formlarının alanlarını ve süreç adımlarını tek tip hale getirmiştir. Türkiye'de SGB'nin çıkaracağı usul ve esaslarda bu düzeyde ayrıntılı kriterler belirlediğinde, III. bölümde haritalanan çok katmanlı yapıdaki her kurum, IV. A'da önerilen tek olay anlatısından kendi görev alanına giren bilgileri seçip alabilecektir. SGB, BTK, BDDK gibi kurumlar bu sayede koordineli çalışabilecektir.

Türkiye'ye özgü modelin Avrupa deneyiminden çıkaracağı ikinci ders, *lex specialis* kuralının açık yazımıdır. NIS2 ile DORA arasındaki ilişki, finansın risk yönetimi ve raporlama alanlarında DORA'yı öncelikli kılmıştır; PSD2 ile DORA arasındaki ilişki ise ödeme hizmetleri olay bildirimini DORA'ya konsolide etmiştir. Aynı mantıkla SGB'nin ikincil düzenlemeleriyle finans için BDDK-TCMB-SPK eksenini, sermaye

[143] EU-CyCLONe'nin rolü ve NIS2 m. 23(5) kapsamında erken uyarı geri bildirimi.

piyasası şeffaflığı için KAP disiplinini ve kişisel veri ihlallerinde Kurul'un yetmiş iki saat penceresini açıkça gösteren bir eşleştirme maddesi, sınır çizgilerini tartışmasız hale getirebilmektedir. KOBİ'ler için sadeleştirilmiş alanlar ve rehberli akış tasarımı ise IV. A'da önerilen orantılılık ilkesini somutlaştırabilecektir.

Ürün güvenliğinde CRA'nın tekil bildirim platformu ile olay güvenliğinde NIS2'nin ulusal CSIRT merkezli hattının farklı amaçlara hizmet ettiğini unutmamak gerekmektedir. Birinci hat üretici-araştırmacı-pazar güvenliği ekseninde ürün zafiyetlerinin hızlı kapanmasına, ikinci hat ise hizmet sürekliliği ve kamu yararı perspektifinden operasyonel müdahalenin senkronize edilmesine odaklanmaktadır. IV. A'da önerilen ikiz hat kurgusu, AB'de ayrışmış iki hattın birlikte çalışmasını yerli bağlama taşımaktadır.

Son olarak, modelin kurumlar arası işlemesini sağlayacak yumuşak eş güdüm katmanı, AB'de ENISA'nın oynadığı rolün yerli karşılığı olan SGB'ye denk düşecektir. NIS2'nin iş birliği yapıları ve EU-CyCLONe ile CSIRT ağı arasındaki veri paylaşım mimarisi, senaryo temelli tatbikatlar ve ortak sözlüklerle güçlendirilmektedir. Aynı şekilde, SGB'nin de ulusal düzeyde ortak terminoloji sözlüğü ve sektörlere özgü ek alanları içeren form şemasını ilan etmesi, ENISA'nın standardizasyon yaklaşımıyla aynı dili kurabilecektir.

Bu karşılaştırma, AB'nin önce esneklikten kaynaklanan farklılaşmayı yaşayıp sonra ayrıntı düzeyi yüksek standardizasyonla parçalanmayı giderdiğini, finans ve ürün güvenliği gibi alanlarda *lex specialis* ve tekil platform çözümleriyle akışı sadeleştirdiğini ve iş birliği mimarisini operasyonel geri bildirim odaklı kurduğunu ortaya koymaktadır. Türkiye'de 7545 sayılı Kanun'un verdiği ikincil düzenleme yetkisi, aynı hedeflere daha başlangıçta ulaşmak için elverişli bir yöntemdir. SGB'nin bu makalede önerilen tek giriş-çok çıkış mimarisini, zaman çizelgesini, eşiğe dayalı sınıflandırmayı, form-prosedür standardizasyonunu ve sektörel uzmanlığı koruyan ama rapor yükünü tekilleştiren bir eş güdüm rejimini oluşturması mümkün görünmektedir.

V. Sonuç

Çalışmanın ortaya koyduğu tablo, Türkiye'de siber olay bildirimine ilişkin hukuki mimarinin tek merkezli bir rejime indirgenmediğini göstermektedir. 7545 sayılı Kanun sonrasında dahi sektörel düzenlemeler kendi amaç ve araçlarıyla birlikte işlemeye devam etmektedir. Bu çoğul yapı, bildirimin tek bir hukuki kategoriye sığmadığını ortaya koymaktadır. Her düzenleyici alan olayın niteliğini kendi risk epistemolojisi içinde yeniden tanımlamakta, dolayısıyla aynı vakıa farklı süre, format ve muhataplara yönelen çoklu yükümlülükleri tetikleyebilmektedir.

Teorik çerçevede incelenen risk toplumu ve merkezsiz regülasyon perspektifi, bu yapının kaçınılmazlığını açıklamaktadır. Siber risklerin çok boyutlu doğası, farklı epistemik toplulukların devreye girmesini gerektirmektedir. BDDK finansal istikrar perspektifinden, BTK teknik altyapı sürekliliği açısından, SPK piyasa şeffaflığı bağlamında, KVKK kişisel veri güvenliği çerçevesinde aynı olayı değerlendirmektedir. Her bir perspektif farklı bir uzmanlık alanını, farklı bir risk metodolojisini ve farklı bir düzenleme mantığını içermektedir. Dolayısıyla paralel yükümlülüklerin varlığı, riskin kendisinin çok boyutlu yapısının kurumsal düzeyde bir yansımasıdır.

Metin boyunca izi sürülen süre rejimleri ve eşikler bu çok katmanlılığın pratik karşılığını açıkça göstermektedir. Gecikmeksizin, derhal, en kısa sürede ve 72 saat gibi zaman ifadeleri yeknesak bir yoruma kavuşmamıştır. Sektörel mevzuatta yer yer açık eşikler bulunurken, yer yer belirsizlikler devam etmektedir. Bu durum, aynı olayın farklı kanallarda farklı hız ve ayrıntı düzeyleriyle raporlanmasını gündeme getirmektedir. Bankacılık, sermaye piyasası, elektronik haberleşme, ödeme hizmetleri, kişisel veriler, tıbbi cihaz ve havacılık gibi alanlar bakımından bildirim yükümlülüklerinin dayanakları, muhatapları ve veri setleri değişmektedir. Bu değişkenlik olay yönetiminin hukuki boyutuna sadece nicel bir yük değil, niteliksel bir karmaşıklık da eklemektedir.

Bu bulgular, çok merkezli düzenleme mantığının iki yüzünü görünür kılmaktadır. Bir yandan sektörel uzmanlık, riskin bağlamsal

niteliğini yakalayabilen denetim ve gözetim mekanizmaları üretmektedir. Diğer yandan mükerrer raporlama, idari maliyet ve koordinasyonsuzluk ihtimali özellikle olay anında karar alma süreçlerini zorlaştırmaktadır. Büyük ölçekli aktörler bakımından operasyonel planlama ve kaynak tahsisi sorunları ortaya çıkmakta, küçük ve orta ölçekli kurumlar bakımından ise fiili uyum kapasitesini aşan yükler söz konusu olabilmektedir. Çalışmanın sektörel kesitleri bu ikili dinamiğin ölçülebilir olduğunu göstermektedir.

Karşılaştırmalı çerçeve, tartışmayı teknik uyum arayışının ötesine taşıyarak yönetişimsel bir öğrenme imkânına işaret etmektedir. Avrupa'daki standartlaşmış zaman çizelgeleri ve bildirim şablonları, etkinliğin tek başına kurumsal merkezileşmeden değil, bilgi akışının yeknesaklığından beslendiğini düşündürmektedir. Bu gözlem, Türkiye'de ortaya çıkan çoğul rejimin normatif bir dağınıklık olarak değil, koordinasyon kapasitesi inşa edildiğinde değer üretebilecek bir düzenleme alanı olarak okunabileceğini göstermektedir. NIS2'nin getirdiği üç aşamalı zaman çerçevesi, DORA'nın finansal sektör için öngördüğü konsolide yaklaşım ve CRA'nın ürün güvenliği alanında kurduğu tekil platform modeli, Türkiye'nin ikincil düzenlemeler yoluyla benzer standartları kurması için somut örnekler sunmaktadır.

Çalışmanın önerdiği eşgüdümlü bildirim çerçevesi, meta-regülasyon yaklaşımından hareketle koordinasyonsuz çokluk sorununa çözüm aramaktadır. Önerilen model, operatörlerin SGB tarafından işletilen merkezi bir portal üzerinden tek bir bildirim yapmasını öngörmektedir. Bu tekil bildirim, akıllı yönlendirme mekanizması aracılığıyla olayın niteliğine göre ilgili sektörel düzenleyicilere otomatik olarak iletilmektedir. Örneğin bir bankanın ödeme sistemlerini etkileyen siber olay, sistemin analiziyle BDDK'ya operasyonel risk boyutuyla, TCMB'ye ödeme sistemleri perspektifinden ve halka açık bankaysa SPK'ya operasyonel etki açısından eşzamanlı ulaşmaktadır. Böylece kuruluş aynı bilgiyi tekrar tekrar farklı formatlarda girmek zorunda kalmamakta, her düzenleyici kurum ise kendi perspektifinden ihtiyaç duyduğu veri setine erişebilmektedir.

Ancak bu koordineli mimari, tüm bildirimlerin tek kanala indirgenmesi anlamına gelmemektedir. Kişisel veri ihlalleri ve sermaye

piyasası şeffaflığı alanlarında farklı menfaatlerin korunması nedeniyle ayrı bildirim hatlarının varlığı rasyoneldir. KVKK'nın koruduğu temel hak ve özgürlükler, operasyonel risk yönetiminden farklı bir meşruiyet temeline dayanmaktadır. NIS2-GDPR ilişkisinde görüldüğü üzere, kişisel veri ihlali bildirimi ayrı bir rejim olarak işlemekte ve siber güvenlik bildirimiyle koordinasyon mekanizmalarıyla bağlantılandırılmaktadır. Benzer şekilde KAP üzerinden yapılan kamuyu aydınlatma, doğrudan yatırımcı koruması ve piyasa güvenini sağlama amacına hizmet etmekte, düzenleyici gözetimden farklı bir işlev görmektedir. Dolayısıyla önerilen model, operasyonel risk ve teknik altyapı odaklı bildirimleri konsolide ederken, temel hak temelli ve piyasa şeffaflığı odaklı bildirimlerin ayrı kanallarını muhafaza etmektedir.

Modelin işleyişi ortak veri sözlüğü ve risk temelli kademeli bildirim sistemine dayanmaktadır. Ortak veri sözlüğü, farklı kurumların aynı kavramları aynı şekilde anlamasını sağlamakta ve karşılaştırılabilirliği mümkün kılmaktadır. Risk temelli kademeli bildirim ise olayın tespit edilmesinden itibaren üç aşamalı bir süreç öngörmektedir. İlk bildirim olayın farkına varılmasıyla birlikte minimum bilgi setiyle yapılmakta, detaylı bildirim makul süre içinde kök neden analizi ve etki değerlendirmesiyle sunulmakta, nihai rapor ise olayın çözümlenmesinden sonra alınan kalıcı önlemleri ve çıkarılan dersleri içermektedir. Bu yapı, hem operatörlerin uyum yükünü hafifletecek hem de düzenleyici kurumların kendi perspektiflerinden risk değerlendirmesi yapmasına imkân tanıyacaktır.

Siber Güvenlik Başkanlığı'nın meta-regülatör rolü bu bağlamda kritik önem taşımaktadır. Başkanlık, doğrudan tüm bildirimleri tek başına yöneten bir otorite olmaktan ziyade, sektörel kurumların bildirim mekanizmalarını koordine eden, ortak standartlar geliştiren ve bilgi akışını kolaylaştıran bir üst düzey koordinasyon işlevi görmelidir. Meta-regülasyon yaklaşımında düzenleyici otorite, orkestra şefi gibi farklı düzenleme aktörlerinin koordinasyonunu sağlar, bilgi akışını kolaylaştırır ve ortak standartları teşvik eder ancak tüm düzenleme sürecini tek başına kontrol etmez. Bu perspektif, sektörel uzmanlığı

köreltmeden koordinasyon maliyetlerini minimize etmeyi mümkün kılmaktadır.

Çalışmanın kaleme alındığı dönemde Avrupa Birliği'nde Komisyon'un Digital Omnibus Tüzük taslağıyla GDPR, NIS2 ve DORA başta olmak üzere temel dijital mevzuatta yer alan bildirim yükümlülüklerini tek bir giriş noktasında toplama ve yüksek risk odaklı, yeknesak şablonlara bağlama yönünde adım atması, burada önerilen eşgüdümlü bildirim çerçevesinin yalnızca ulusal bağlama özgü pragmatik bir çözüm değil, aynı zamanda karşılaştırmalı hukuk düzleminde ortaya çıkan genel yönetişim trendiyle uyumlu olduğunu göstermektedir.[144] AB'nin parçalı rejimleri sonradan rasyonalize etmeye dönük bu çabası karşısında, Türkiye'de 7545 sayılı Kanun'un tanıdığı ikincil düzenleme yetkisi, çok merkezli siber güvenlik yönetişimini baştan itibaren koordine edilmiş bir çoğulluk zemininde inşa etme bakımından önemli bir fırsat penceresi sunmaktadır.

Sonuç itibarıyla çalışma, siber olay bildirimine ilişkin hukuki çerçevenin geçişsel bir evrede bulunduğunu ortaya koymaktadır. Sektörel özerklik ile ulusal eşgüdüm arasındaki ilişki belirleyici mesele haline gelmiştir. Hukuki öngörülebilirlik, düzenleyici tutarlılık ile idari esneklik arasındaki dengenin bundan sonraki dönemde rejimin başarısını tayin edeceği açıktır. Mevcut mimari tekil bir merkezden yönetilen yekpare bir sistem değildir. Ancak kavramsal dilin ve veri sözlüğünün yakınsaması ölçüsünde işlevsel hale gelebilecek çok katmanlı bir yönetişim alanı potansiyeli taşımaktadır. 7545 sayılı Kanun'un tanıdığı ikincil düzenleme yetkisi, bu potansiyelin gerçekleştirilmesi için elverişli bir araçtır. İkincil düzenlemelerin tasarımında AB deneyiminden alınacak dersler, koordineli çoğulculuk perspektifi ve orantılılık ilkesi gözetildiğinde, Türkiye etkin bir siber güvenlik olay bildirim rejimi kurabilecektir.

144 Digital Omnibus Teklifi, COM(2025) 837 final, md. 10

Hakem Değerlendirmesi: Dış bağımsız.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

Peer-review: Externally peer-reviewed.

Conflict of Interest: The author has no conflict of interest to declare.

Grant Support: The author declared that this study has received no financial support.

Peer-Review: Externes Peer-Review-Verfahren.

Interessenkonflikt: Der/die Autorinnen unterliegt/unterliegen keinem Interessenkonflikt.

Finanzielle Unterstützung: Der/die Autorinnen erklärt/en, dass diese Studie keine finanzielle Unterstützung erhalten hat.

EXTENDED SUMMARY

This study examines the complex landscape of cybersecurity incident notification obligations in Turkey, analyzing the theoretical foundations, practical implications, and optimal design of multi-layered reporting architectures through the lens of risk governance, decentered regulation, and meta-regulatory frameworks.

Turkey's cybersecurity notification regime has entered a new phase with the enactment of the Cybersecurity Law (Law No. 7545), establishing the Cybersecurity Presidency (SGB) as a central coordinating authority. However, this new framework does not replace existing sectoral notification mechanisms maintained by regulatory bodies including the Information and Communication Technologies Authority (BTK), the Banking Regulation and Supervision Agency (BDDK), the Capital Markets Board (SPK), the Energy Market Regulatory Authority (EPDK), and others. This creates a situation where the same cybersecurity incident may trigger multiple, parallel reporting obligations to different authorities, each with distinct timelines, formats, and thresholds. The research question centers on how this polycentric notification architecture can be optimized to balance regulatory effectiveness with compliance burden.

The analysis draws on three interconnected theoretical perspectives. Risk society theory explains why cyber risks inherently defy singular regulatory categorization. Modern cyber risks exhibit characteristics that transcend traditional boundaries: they are spatially and temporally unbounded, often invisible without technical expertise, potentially irreversible in impact, exceed conventional liability frameworks, and challenge democratic decision-making processes. This multi-dimensional nature means that a single incident simultaneously constitutes an operational continuity issue, a data protection breach, a financial stability risk, and potentially market-sensitive information. Decentered regulation theory demonstrates that regulation emerges not from a single hierarchical authority but from complex interactions among multiple actors, knowledge flows, and power relationships. Different regulatory communities operate with distinct rationalities: BDDK approaches cyber incidents through financial stability metrics; BTK focuses on network infrastructure resilience; SPK evaluates market transparency implications; KVKK safeguards fundamental rights related to personal data. Meta-regulation and coordinated pluralism concepts provide the normative framework for

addressing coordination challenges without sacrificing the benefits of polycentricity, establishing common standards and information-sharing protocols while preserving sectoral autonomy.

The study maps detailed notification requirements across sectors. The Cybersecurity Law mandates "without delay" notification to SGB for detected vulnerabilities or cyber incidents. BDDK requires immediate reporting through cyber incident management procedures. SPK demands "immediate" notification under its Information Systems Management Communiqué and public disclosure through the Public Disclosure Platform for material events. BTK stipulates reporting breaches affecting more than 5% of subscribers "as soon as possible." KVKK establishes a 72-hour deadline for personal data breach notifications. TCMB requires "immediate" notification for payment system incidents. EPDK employs a maturity-level-based differentiated obligation system. This multiplicity creates three categories of problems: definitional inconsistencies where the same incident receives different classifications, temporal conflicts between vague terms and specific deadlines, and format diversity requiring duplicate data entry across separate reporting systems.

The European Union's approach offers instructive solutions. The NIS2 Directive establishes a standardized three-stage timeline: early warning within 24 hours, incident notification within 72 hours, and final report within one month. Commission Implementing Regulation 2024/2690 provides quantifiable thresholds for determining incident significance, including financial loss exceeding €500,000 or 5% of annual revenue, service interruptions lasting more than 30 minutes, and impact affecting at least 5% or one million EU users. The Digital Operational Resilience Act demonstrates sector-specific consolidation, explicitly amending the Payment Services Directive 2 to channel all ICT incident reporting through DORA's framework, thereby eliminating duplicate reporting. The Cyber Resilience Act establishes a single reporting platform operated by ENISA for product vulnerabilities, showing how specialized domains can benefit from unified channels.

The study proposes an integrated notification framework based on meta-regulatory principles, operating through a single-entry-multiple-exit architecture. Operators would submit a unified report through SGB's centralized portal using a common data dictionary. Intelligent routing mechanisms would automatically distribute relevant information to appropriate

sectoral authorities based on incident classification. The framework incorporates three essential components: a common data dictionary standardizing terminology while accommodating sector-specific data fields, a minimum common dataset including incident detection time and affected systems, and sector-specific modules allowing each authority to request additional information relevant to its regulatory perspective. Risk-based tiered reporting implements a three-stage process with initial notification for situational awareness, detailed notification with comprehensive analysis, and final reports documenting remedial actions and lessons learned. The SGB's role evolves from parallel regulator to meta-regulator, coordinating sectoral mechanisms rather than directly managing all notifications. Certain notification channels remain separate due to distinct protected interests: KVKK's fundamental rights protection and KAP's investor protection functions serve different legitimacy bases than operational risk supervision, warranting independent mechanisms with coordination protocols.

The study demonstrates that Turkey's multi-layered cybersecurity notification regime reflects not regulatory dysfunction but the inherent multi-dimensionality of cyber risk. Parallel obligations arise from different epistemological communities evaluating the same incident through distinct analytical frameworks. The Cybersecurity Law's secondary regulation authority provides the legal foundation for implementing coordinated notification architecture through common data dictionaries, standardized timelines aligned with international best practices, quantifiable thresholds for incident classification, and automated information-sharing protocols, achieving effective cyber risk governance without sacrificing sectoral expertise.

KAYNAKÇA

ADAMS, S. vd. "The Governance of Cybersecurity : A Comparative Quick Scan of Approaches in Canada, Estonia, Germany, the Netherlands and the UK". *Tilburg University / WODC, Lahey*.

AKGÜN, Mustafa. "Bağımsız İdari Otoritelerin Anayasal Statüsünün Belirlenmesi İhtiyacı: Teorik ve Pratik Gerekçeler". *Amme İdaresi Dergisi* 57/2 (2024), 29-60.

AKTAN, Coşkun Can - Yay, Serdar. "REGÜLASYON İKTİSADINA GİRİŞ". *Ekonomi Bilimleri Dergisi* 8/1 (31 Aralık 2016), 59-72.

AYRES, Ian - Braithwaite, John. *Responsive Regulation: Transcending the Deregulation Debate*. Oxford University Press, 1992. https://doi.org/10.1093/oso/9780195070705.001.0001

BALDWIN, Robert vd. *LSE Research Online Documents on Economics*. "Risk Management and Business Regulation". *LSE Research Online Documents on Economics*. https://ideas.repec.org//p/ehl/lserod/35975.html

BALDWIN, Robert vd. (ed.). *The Oxford handbook of regulation*. Oxford, U. K: Oxford University Press, 1st pbk. ed., 2012.

BALDWIN, Robert vd. *Understanding Regulation: Theory, Strategy, and Practice*. New York: Oxford University Press, 2nd ed., 2012.

BECK, Ulrich vd. *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*. Stanford University Press, 1994.

BECK, Ulrich. *Risk Society: Towards a New Modernity*. London: Sage, Repr., 2009.

BECK, Ulrich. *World at Risk*. Polity, 2009.

BLACK, Julia. "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes". *Regulation & Governance* 2/2 (2008), 137-164. https://doi.org/10.1111/j.1748-5991.2008.00034.x

BLACK, Julia. "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World".

Current Legal Problems 54/1 (01 Ocak 2001), 103-146. https://doi.org/10.1093/clp/54.1.103

BLACK, Julia. "Regulatory Conversations". *Journal of Law and Society* 29/1 (2002), 163-196. https://doi.org/10.1111/1467-6478.00215

BLACK, Julia. "The Emergence of Risk-Based Regulation and the New Public Risk Management in the United Kingdom". *Public Law*, 510-546.

BLACK, Julia - Baldwin, Robert. "Really Responsive Risk-Based Regulation". *Law & Policy* 32/2 (15 Mart 2010), 181-213. https://doi.org/10.1111/j.1467-9930.2010.00318.x

BURNUKARA, Simay. *2001 krizi sonrası Türk bankacılık sisteminde BDDK'nın rolü ve fonksiyonu*. İstanbul Ticaret Üniversitesi, 2012. https://acikerisim.ticaret.edu.tr/items/72bcbae1-3f64-47ce-85f5-2f1a47c72515

CARTER, David P. - Mahallati, Nadia. "Coordinating Intermediaries: The Prospects and Limitations of Professional Associations in Decentralized Regulation". *Regulation & Governance* 13/1 (2019), 51-69. https://doi.org/10.1111/rego.12167

COEN, David - Thatcher, Mark. "Network Governance and Multi-Level Delegation: European Networks of Regulatory Agencies". *Journal of Public Policy* 28/1 (Nisan 2008), 49-71. https://doi.org/10.1017/S0143814X08000779

COGLIANESE, Cary - Lazer, David. "Management-Based Regulation: Prescribing Private Management to Achieve Public Goals". *Law & Society Review* 37/4 (Aralık 2003), 691-730. https://doi.org/10.1046/j.0023-9216.2003.03703001.x

COGLIANESE, Cary - Mendelson, Evan. "Meta-Regulation and Self-Regulation". *The Oxford Handbook of Regulation*. ed. Robert Baldwin vd. 0. Oxford University Press, 2010. https://doi.org/10.1093/oxfordhb/9780199560219.003.0008

DEIBERT, Ronald J. - Rohozinski, Rafal. "Risking Security: Policies and Paradoxes of Cyberspace Security". *International Political Sociology*

4/1 (01 Mart 2010), 15-32. https://doi.org/10.1111/j.1749-5687.2009.00088.x

ECKERT, Sandra - Börzel, Tanja A. "Experimentalist Governance: An Introduction". *Regulation & Governance* 6/3 (2012), 371-377. https://doi.org/10.1111/j.1748-5991.2012.01163.x

GİDDENS, Anthony. "Risk and Responsibility". *The Modern Law Review* 62/1 (1999), 1-10.

GREENBERG, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday, 2019.

HANCHER, L. - Moran, M. "Organizing Regulatory Space". *A Reader on Regulation*. ed. Robert Baldwin vd. 0. Oxford University Press, 1998. https://doi.org/10.1093/acprof:oso/9780198765295.003.0005

HOOD, Christopher vd. *The Government of Risk: Understanding Risk Regulation Regimes*. OUP Oxford, 2001.

HUTTER, Bridget M. *The attractions of risk-based regulation: accounting for the emergence of risk ideas in regulation*. CARR London, 2005. https://web.actuaries.ie/sites/default/files/erm-resources/205_The_attractions_of_risk_based_regulation_accounting_for_the_emergence_of_risk_ideas_in_regulation.pdf

IŞIK, Alper. *İnternet Aktörleri ve Egemenliğin Değişen Boyutları*. İstanbul: On İki Levha Yayıncılık, 2. Basım, 2025.

JAMES, Oliver. "Regulation Inside Government: Public Interest Justifications and Regulatory Failures". *Public Administration* 78/2 (2000), 327-343. https://doi.org/10.1111/1467-9299.00208

KAYA, Mehmet Bedii. "Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law". *Annales de La Faculté de Droit d'Istanbul* 70 (31 Aralık 2021), 195-241. https://doi.org/10.26650/annales.2021.70.0007

KAYA, Mehmet Bedii. "Siber Güvenlik Hukuku". *Dijital Baskı*. mbkaya.com/hukuk/siber-guvenlik-hukuku.pdf

KOLİBA, Christopher J. vd. *Governance Networks in Public Administration and Public Policy*. New York: Routledge, 2. Basım, 2018. https://doi.org/10.4324/9781315268620

LUHMANN, Niklas. *Risk: A Sociological Theory*. çev. Rhodes Barrett. Abingdon, Oxon New York, NY: Routledge, Taylor & Francis Group, 2017.

MAGGETTİ, Martino. "De Facto Independence after Delegation: A Fuzzy-Set Analysis". *Regulation & Governance* 1/4 (2007), 271-294. https://doi.org/10.1111/j.1748-5991.2007.00023.x

OSTROM, Elinor. "Beyond Markets and States: Polycentric Governance of Complex Economic Systems". *The American Economic Review* 100/3 (2010), 641-672.

O'SULLİVAN, K.P.V. - Flannery, Darragh. "A Discussion on the Resilience of Command and Control Regulation within Regulatory Behavior Theories". *Journal of Governance and Regulation* 1/1 (2012), 15-24. https://doi.org/10.22495/jgr_v1_i1_p2

PAPADOPOULOS, Yannis. "How Does Knowledge Circulate in a Regulatory Network? Observing a European Platform of Regulatory Authorities Meeting". *Regulation & Governance* 12/4 (2018), 431-450. https://doi.org/10.1111/rego.12171

PARKER, Christine. *The Open Corporation: Effective Self-Regulation and Democracy*. Cambridge University Press, 2002.

POWER, Michael. *Organized Uncertainty: Designing a World of Risk Management*. Oxford University Press, 2007. https://doi.org/10.1093/oso/9780199253944.001.0001

RASBORG, Klaus. *Ulrich Beck: Theorising World Risk Society and Cosmopolitanism*. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-89201-2

SARI, Ömür Kadri. "TÜRK HUKUKUNDA DÜZENLEYİCİ VE DENETLEYİCİ KURUMLARIN TEMEL İLKELERİ". *Danıştay Dergisi* 152 (2020), 277-298.

YESILKAGIT, Kutsal. "Institutional compliance, European networks of regulation and the bureaucratic autonomy of national regulatory authorities". *Journal of European Public Policy* 18/7 (01 Ekim 2011), 962-979. https://doi.org/10.1080/13501763.2011.599965

YEUNG, Karen - Ranchordás, Sofia. *An Introduction to Law and Regulation: Text and Materials*. Cambridge, UK ; New York: Cambridge University Press, 2024.

Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. United State Government Accountability Office, 2018.