Araştırma Makalesi
Research Article

Gönderim / Received: 17/04/2025
Kabul / Accepted: 26/09/2025

Hukuk Fakültesi Dergisi
Ankara Hacı Bayram Veli University
Faculty of Law Review

ISSN: 2651-4141 e-ISSN: 2667-4068
Cilt / Volume 29 Ekim / October 2025 Sayı / No. 4

DİJİTAL ÜRÜN YAŞAM DÖNGÜSÜNDE SİBER GÜVENLİK: SİBER DAYANIKLILIK YASASI EKSENLİ AB DÜZENLEYİCİ ÇERÇEVESİ

CYBERSECURITY IN DIGITAL PRODUCT LIFECYCLE: THE CYBER RESILIENCE ACT CENTERED EU REGULATORY FRAMEWORK

Esma Muheyne DOĞAN*

ÖZET

Dijital ürünlerin yaşam döngüsünde siber güvenliğin sağlanması, günümüz teknoloji ekosisteminin en kritik konularından biri haline gelmiştir. Avrupa Birliği'nin (AB) dijital dönüşüm sürecinde ortaya çıkan siber güvenlik risklerine karşı geliştirdiği Siber Dayanıklılık Yasası (Cyber Resilience Act, CRA), kapsamlı ve çok katmanlı bir düzenleyici çerçevenin merkezi bileşeni olarak öne çıkmaktadır. Bu çalışma, CRA'nın dijital bileşenli ürünlerin tüm yaşam döngüsü boyunca siber güvenliğini sağlama hedefini detaylı biçimde analiz etmektedir. Çalışmanın ikinci bölümünde, CRA'nın Yapay Zekâ Yasası (AI Act) ile kesişim noktasındaki yapay zekâ sistemlerinin güvenli gelişimini sağlama amacı ve Ürün Sorumluluğu Direktifi'nin (PLD) bu iki düzenlemeyi tamamlayarak dijital çağın gerekliliklerine uygun modernize edilmiş bir sorumluluk rejimi sunması incelenmektedir. Çalışma ayrıca, bu düzenleyici çerçevenin üreticiler ve paydaşlar için getirdiği yükümlülükleri ve zorlukları ele almaktadır. Sonuç olarak, CRA eksenli AB düzenleyici çerçevesinin yalnızca güvenlik standartları getirmekle kalmayıp, dijital ürün ekosisteminde

* **Av.,** İstanbul Barosu/İSTANBUL, **E-Posta:** av.esmadogan@gmail.com, **ORCID:** 0009-0008-0612-8036, **DOI:** 10.34246/ahbvuhfd.1678639.

• **Atıf Şekli/Cite As:** Doğan, Esma Muheyne, "Dijital Ürün Yaşam Döngüsünde Siber Güvenlik: Siber Dayanıklılık Yasası Eksenli AB Düzenleyici Çerçevesi", HBV-HFD, 2025, C. 29, S. 4, s. 1729-1760.

• **İntihal /Plagiarism**: Bu makale intihal programında taranmış ve en az iki hakem incelemesinden geçmiştir./*This article has been scanned via a plagiarism software and reviewed by at least two referees.*

"güvenlik kültürü" oluşturarak uzun vadeli ve sürdürülebilir bir siber dayanıklılık stratejisi sunduğu ortaya konmaktadır.

Anahtar Kelimeler: *Siber dayanıklılık, Ürün sorumluluğu, Yapay zekâ, Dijital dönüşüm, Siber güvenlik*

ABSTRACT

Ensuring cybersecurity throughout the lifecycle of digital products has emerged as one of the most critical issues in today's technological ecosystem. The Cyber Resilience Act (CRA), adopted by the European Union in response to cybersecurity risks arising from digital transformation, stands out as the central component of a comprehensive and multi-layered regulatory framework. This study analyzes in detail the CRA's objective of ensuring cybersecurity of products with digital components throughout their entire lifecycle. The second part of the research examines the intersection of the CRA with the Artificial Intelligence Act (AI Act) in ensuring the secure development of AI systems, and how the Product Liability Directive (PLD) complements these two regulations by providing a modernized liability regime suitable for the digital age. The study also addresses the obligations and challenges this regulatory framework brings for manufacturers and stakeholders. In conclusion, the research demonstrates that the CRA centered EU regulatory framework not only establishes security standards but also offers a long-term and sustainable cyber resilience strategy by fostering a "security culture" within the digital product ecosystem.

Keywords: *Cyber resilience, Product liability, Artificial intelligence, Digital transformation, Cybersecurity.*

EXTENDED ABSTRACT

This study examines the European Union's regulatory framework for digital security, focusing on the Cyber Resilience Act (CRA) and its interaction with the AI Act and the Product Liability Directive (PLD). The digital transformation has fundamentally changed the nature of products and services, rendering traditional legal frameworks inadequate. This transformation process gained unexpected momentum during the COVID-19 pandemic, forcing institutions into rapid digital adaptation while creating new targets for cyber attackers. According to the 2024 report of the German Federal Office for Information Security, cyber attacks have both increased in number and become more professional through the "Cybercrime-as-a-Service" model.

The EU's digital security strategy aims to ensure cyber security throughout the entire lifecycle of products, from design to end-use. The CRA, which came into force on December 10, 2024, the AI Act, and the new PLD form a regulatory framework that constitutes a coordinated response to these challenges. The main research question of this study is to explain how the CRA establishes a comprehensive cyber security framework throughout the lifecycle of products with digital components and how it interacts with other regulations.

The study finds that the CRA represents a significant shift from voluntary approaches to mandatory mechanisms in addressing cybersecurity concerns. Its most notable innovation is transforming "security by design" from an engineering method to a legal obligation. The CRA adopts a risk-based classification system, categorizing digital products as standard products, Class I and Class II important products, and critical products. This classification determines the level of security assessment required, with higher-risk products subject to more stringent third-party evaluations.

The CRA establishes comprehensive vulnerability reporting requirements with strict timelines: 24-hour early warning notification, 72-hour detailed notification, and 14-day final report for serious security incidents. Non-compliance can result in penalties of up to €15 million or 2.5% of global annual turnover, whichever is higher. However, the study identifies certain limitations in the CRA, such as the exclusion of "silent patching" and the ambiguous definition of "actively exploited vulnerabilities," which potentially leaves security risk assessment to manufacturers' discretion.

The research demonstrates significant interaction between the CRA and AI Act, particularly regarding high-risk AI systems. Products classified as high-risk AI systems must comply with the CRA's cybersecurity requirements, with risk assessments considering AI-specific vulnerabilities such as data poisoning and adversarial attacks. Article 12 of the CRA provides that digital products classified as high-risk AI systems (except critical digital products) that meet the cybersecurity requirements of Article 15 of the AI Act will also be considered compliant with the CRA.

Regarding product liability, the research shows that the PLD complements the CRA by modernizing the liability regime for digital products. One of the most important innovations of the Directive is the regulation regarding the legal status of software, explicitly including it within the scope of the product definition regardless of its supply and usage method. The directive also

specifically addresses liability for AI systems, holding developers responsible for damages caused by unexpected behaviors.

A critical finding is that the "development risks defense" becomes practically difficult to invoke under the new framework. This defense, which allows manufacturers to avoid liability if they could not have discovered the defect given the state of scientific knowledge, is challenged by the CRA's extensive requirements for continuous monitoring and rapid response to vulnerabilities. The CRA and PLD create a dual protection mechanism that both incentivizes preventive measures and provides effective remedies for potential violations.

The research concludes that while the CRA-centered regulatory framework offers a comprehensive approach to digital security throughout the product lifecycle, it poses significant implementation challenges. Manufacturers face substantial compliance burdens, particularly regarding stringent security assessment requirements and tight timelines for vulnerability management. Despite these challenges, the potential benefits of strengthened digital security and increased consumer confidence justify the necessity of this regulatory framework. For future development, it is important to focus on how the balance between innovation and cybersecurity is maintained, particularly for SMEs, and whether these regulations effectively shape global standards for digital product security.

GİRİŞ

COVID-19 pandemisiyle hızlanan dijital dönüşüm[1] ve uzaktan çalışma sistemlerinin yaygınlaşması, siber saldırılarda önemli bir artışa neden olmuştur[2]. Yapay zekâ, büyük veri, blockchain ve bulut bilişim gibi gelişmekte olan teknolojiler, işletmeler için siber güvenlik risklerini artırırken[3], bu dönüşüm süreci geleneksel hukuki çerçeveleri de yetersiz hale getirmektedir.

Bu artan siber saldırı trendini destekler nitelikte, Alman Federal Bilgi Güvenliği Ofisi'nin (*Bundesamt für Sicherheit in der Informationstechnik)* 2024 raporunda belirtildiği üzere, siber saldırılar hem sayıca artmış hem de

[1] COVID-19 and Digitalisation, (https://www.eurofound.europa.eu/en/covid-19-and-digitalisation, Erişim Tarihi: 22.08.2025)

[2] Lallie/Shepherd/Nurse/Erola/Epiphaniou/Maple/Bellekens, s.15; Pranggono/Arabo, s.1.

[3] Saeed/Altamimi/Alkayyal/Alshehri/Alabbad, s.16

"Hizmet Olarak Siber Suç"[4] modeliyle profesyonelleşmiştir[5]. Google'ın Şubat 2025 tarihli "*Google Threat Intelligence*" raporuna göre siber güvenlik, artık teknik bir mesele olmaktan çıkarak hayati bir ulusal güvenlik tehdidi haline gelmiştir[6].

Özellikle dikkat çekici olan nokta, sağlık sektöründeki durumun ciddiyetidir. Google raporunda hastanelere yönelik siber saldırılardaki artışa dikkat çekilmekte, bu saldırıların sadece veri güvenliğini tehdit etmekle kalmayıp doğrudan insan hayatını da risk altına aldığı vurgulanmaktadır[7]. Hastaneye yapılan siber saldırılar sonrasında hasta ölüm oranında önemli artışlar tespit edilmiş, bu durumun kritik tıbbi sistemlerin devre dışı kalmasından kaynaklandığı belirlenmiştir[8].

Bu kritik durumu daha da karmaşık hale getiren unsur, sağlık sektöründeki IoT (*Internet of Things, nesnelerin interneti*) cihazlarının yarattığı güvenlik açıklarıdır. Bu cihazların çoğunun güncel olmayan işletim sistemleri kullanması ve zayıf güvenlik önlemlerine sahip olması, onları siber saldırganlara karşı oldukça savunmasız hale getirmektedir[9]. Sağlık sektöründeki IoT hedefli saldırılarda %60'lık artış yaşanması[10], bu cihazların acil güvenlik önlemleri gerektirdiğini göstermektedir.

Sağlık sektöründeki bu yaşamsal risklerin yanı sıra, saldırıların ekonomik boyutu da oldukça çarpıcıdır. FBI verilerine göre son on yılda e-posta dolandırıcılığından kaynaklanan toplam kayıp 55 milyar dolara ulaşmıştır[11].

---

[4] *Hizmet olarak siber suç (Cybercrime-as-a-Service), siber suçluların saldırı faaliyetlerini modüler hizmetler halinde bölerek dark web üzerinden pazarladıkları bir iş modelidir. Bu model sayesinde teknik bilgisi sınırlı kişiler bile karmaşık siber saldırılar düzenleyebilir, çünkü her aşama ayrı bir uzman tarafından hizmet olarak sunulmaktadır. Sonuç olarak siber suç, daha organize, erişilebilir ve karlı bir iş haline dönüşmüştür.* Bkz: Huang/Siegel/Madnick, s.1:13.

[5] 2024 State of IT Security in Germany Report, (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2024.html?nn=1021082., Erişim Tarihi: 22.08.2025)

[6] Cybercrime: A Multifaceted National Security Threat, (https://services.google.com/fh/files/misc/cybercrime-multifaceted-national-security-threat.pdf, Erişim Tarihi: 22.08.2025)

[7] Google, dn.5.

[8] McGlave/Neprash/Nikpay, s. 24.

[9] ElSayed/Abdelgawad/Elsayed, s. 8.

[10] ElSayed/Abdelgawad/Elsayed, s. 8.

[11] Google, dn.5.

Ekonomik zararların ötesinde, durumu daha da kritik hale getiren unsur devlet destekli siber faaliyetlerdir[12]. Bu devlet destekli siber faaliyetler "sessiz savaşlar" olarak nitelendirilebilir; zira hem saldırganlar hem de mağdurlar kasıtlı olarak açıklama yapmaktan kaçınmakta, saldırılar maskelenmekte ve sofistike operasyonlar çoğunlukla tespit edilememektedir[13]. Bu durum göz önünde bulundurulduğunda, siber güvenliğin artık sadece kurumların bilişim departmanlarının sorumluluğu olmadığı açıktır. Günümüzde siber güvenlik, ülkelerin ekonomik rekabet gücü ve ulusal savunma açısından kritik bir zorunluluk haline gelmiştir[14].

Bu kapsamlı tehdit manzarası karşısında, güvenlik sorunlarının çözümü için dünya çapında çeşitli hukuki yaklaşımlar geliştirilmektedir[15]. AB, bu değişime yanıt olarak, dijital çağın gereksinimlerini karşılayan kapsamlı düzenlemeler yapmıştır.

AB'nin dijital güvenlik stratejisi, ürünlerin tasarımdan üretim, piyasaya sürülme ve kullanım sürecine kadar uzanan tüm yaşam döngüsünde siber güvenliği sağlamayı amaçlamaktadır. Bu stratejinin temel bileşenleri olarak Siber Dayanıklılık Yasası (*Cyber Resilience Act*, CRA ve Yasa[16]), Yapay Zekâ Yasası (*AI Act*) ve yeni Ürün Sorumluluğu Direktifi (*Product Liability Directive*, PLD veya Direktif) birbiriyle etkileşim halinde düzenleyici bir çerçeve oluşturmaktadır.

CRA, dijital bileşenli ürünlerin tasarım aşamasından kullanım

---

[12] Google, dn.5.

[13] Koch/Golling, s.3-4.

[14] Google, dn.5, Li/Liu, s.8184.

[15] The UK Product Security and Telecommunications Infrastructure (Product Security) Regime, (https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime, Erişim Tarihi: 22.08.2025); Microsoft Digital Defense Report 2024, (https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024. Erişim Tarihi: 22.08.2025)

[16] *AB düzenlemeleri Türkçe akademik çalışmalara konu olduğunda "Regulation" başlıklı düzenlemeler, hukuki statüleri gereği "tüzük" olarak çevrilmektedir.* Bkz: Çekin, s.166, Güçlütürk, s.207-222. *Ancak Papakonstantinou ve De Hert'in "act-ification" kavramı çerçevesinde ortaya koyduğu üzere AB yasa koyucusunun dijital teknoloji mevzuatında "act" terminolojisini kullanması bilinçli bir tercihtir ve bu durum uluslarüstü düzeyde doğrudan uygulanabilir bir hukuki çerçeve oluşturmak amacıyla geliştirilen yeni bir yasama paradigmasının göstergesidir. Bu bağlamda, AB'nin bu stratejik terminoloji tercihini yansıtmak amacıyla, bu makalede "act" kelimesi İngilizce aslına uygun olarak "yasa" şeklinde çevrilmiştir*. Bkz: Papakonstantinou/De Hert 2022, s.48-60

ömrünün sonuna kadar siber güvenliğini temin etmeyi; AI Act, yapay zekâ sistemlerinin güvenli gelişimini ürün yaşam döngüsünün her aşamasında sağlamayı; PLD ise dijital çağda ürün sorumluluğu rejimini yaşam döngüsü perspektifinden modernize etmeyi amaçlamaktadır. Bu düzenlemeler birlikte, dijital ürünlerin üretimden son kullanım aşaması boyunca güvenliği ve sorumluluğuna ilişkin bütüncül bir çerçeve oluşturmaktadır. Bu bütüncül çerçevenin daha iyi anlaşılması için özellikle CRA'nın detaylı incelenmesi gerekmektedir. Bu çalışma, AB'nin dijital ürün yaşam döngüsü güvenlik ekosisteminin merkezinde yer alan CRA'yı detaylı olarak incelemeyi ve bu düzenlemenin ürünlerin gelişim, üretim, dağıtım ve kullanım aşamalarında AI Act ve PLD ile kesişen noktalarını analiz etmeyi amaçlamaktadır. Çalışmanın temel sorusu, CRA'nın dijital bileşenli ürünlerin yaşam döngüsü genelinde nasıl kapsamlı bir siber güvenlik çerçevesi oluşturduğu ve diğer düzenlemelerle nasıl etkileşimde bulunduğudur.

Bu temel soruyu yanıtlamak için sistematik bir yaklaşım izlenecektir. Öncelikle AB'nin dijital güvenlik ekosistemini ürün yaşam döngüsü perspektifinden ele alan yeni düzenleyici çerçeveye genel bir bakış sunulacaktır. CRA'nın her aşamadaki temel amaçları, kapsamı ve uygulama gereklilikleri detaylandırılacak; ardından CRA'nın AI Act ile kesişim noktaları ve PLD ile tamamlayıcı ilişkisi ele alınacaktır. Sonraki bölümde, bu üç yasal düzenlemenin dijital ürün yaşam döngüsü sorumluluğunu nasıl şekillendirdiği analiz edilecek ve üreticilerin ürün geliştirme süreçlerinde bu düzenlemelere uyum sağlamasının pratik etkileri değerlendirilecektir. Çalışma, CRA'nın AB'nin dijital ürün yaşam döngüsü güvenlik stratejisindeki merkezi rolünün kapsamlı bir değerlendirmesi ile sonlandırılacaktır.

Çalışmada savunulan temel görüş, CRA dijital bileşenli ürünlerin yaşam döngüsü boyunca siber güvenliği sağlamada önemli bir adım olmakla birlikte, uygulamada ciddi zorluklara sebep olabileceğidir. Özellikle yasanın kapsamlı yükümlülükleri ve sıkı zaman çizelgeleri, üreticiler için önemli uyum zorlukları yaratacaktır. Ancak bu zorlukların, dijital güvenlik ekosisteminin sağlamlaştırılması ve tüketici güveninin artırılması yönündeki potansiyel faydaları göz önüne alındığında, yasanın gerekliliği ve değeri ortaya çıkmaktadır.

I. AB'NİN YENİ DÜZENLEYİCİ ÇERÇEVESİNE GENEL BAKIŞ

AB, siber güvenlik alanında kapsamlı bir yasal çerçeve geliştirmeye

yönelik çalışmalarına son yıllarda hız vermiştir. Bu çerçevenin en güncel ve kapsamlı parçası olan CRA, AB'nin dijital tek pazarının güvenliğini sağlamaya yönelik önemli bir adım olarak karşımıza çıkmaktadır[17].

A. AB'nin Siber Güvenlik Düzenlemeleri ve CRA'nın Gelişimi

AB'nin siber güvenlik alanındaki düzenlemeleri, değişen teknolojik koşullar ve artan siber tehditler karşısında evrimleşerek bugünkü kapsamlı çerçeveye ulaşmıştır. Bu evrim süreci, gönüllü yaklaşımlardan zorunlu mekanizmalara[18] doğru bir geçişi yansıtmaktadır[19].

1. Siber Dayanıklılık Yaklaşımı ve Önceki Düzenlemeler

Artan siber tehditlerin karmaşıklığı ve dijital ürünlerdeki güvenlik açıkları, organizasyonları ve özellikle AB'yi kapsamlı bir siber güvenlik yaklaşımı geliştirmeye yöneltmiştir[20]. Bu bağlamda siber dayanıklılık, geleneksel *"tahmin et ve koru*" metodolojisinin ötesine geçerek, salt teknik bir güvenlik meselesi olmaktan çıkıp, sistemlerin saldırılara karşı koyabilme, normal işleyişini sürdürebilme ve gerektiğinde hızla toparlanabilme yeteneğini kapsayan bütünsel bir yaklaşımı ifade etmektedir[21]. Bu yaklaşım, organizasyonların dijital sistemlerin mutlak güvenliğinin imkansız olduğunu kabul ederek, teknolojinin sağladığı verimlilik avantajlarından vazgeçmeden, metaforik olarak "*zehirli meyve diyetiyle beslenmeyi*" öğrenmeyi gerektirir[22].

AB'nin siber güvenlik alanındaki düzenleyici gelişimi, sorunların tespiti ve bunlara yönelik kademeli çözüm arayışını yansıtmaktadır. İlk

---

[17] Chiara, "Towards a right to cybersecurity in EU law? The challenges ahead", s.6-7, Fahey, s.1077, Kamara, s.2-3, Shaffique, s.7-8.

[18] *Gönüllü yaklaşımlar, büyük şirketler ve kritik altyapı sağlayıcıları ile resmi ve gayri resmi iletişim kanalları kurarak bilgi paylaşımını teşvik eden ancak katılımı zorunlu kılmayan sistemlerdir; zorunlu mekanizmalar ise güçlü otoritelerin kurallara uymayı seçmeyenlere yaptırım uygulayarak ürünleri denetleme, geri çekme, piyasadan yasaklama ve para cezası verme yetkilerine sahip olduğu sistemlerdir.* Bkz: Ludvigsen, s. 4-8.

[19] *AB'nin zorunlu mekanizmalarla düzenleme tercihi, tek pazarın bütünlüğünü sağlama amacından kaynaklanmaktadır.* Bkz: Fahey, s.1075.

[20] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=join:JOIN_2013_071. Erişim Tarihi: 22.08.2025)

[21] Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN%3A2020%3A18%3AFIN. Erişim Tarihi: 22.08.2025)

[22] Dupont, s. 2. *(yazarın çevirisi)*

aşamada, özel sektörün siber tehditlere karşı hazırlıksız olması ve koordineli bir yanıt mekanizmasının eksikliği, 2016 yılında NIS Direktifi'nin (*Directive on Security of Network and Information Systems*) kabulüne yol açmıştır[23]. Bu direktif, özel sektörün hazırlık düzeyini artırmaya ve koordineli müdahale mekanizmaları oluşturmaya odaklanmış,[24] ancak zamanla bu yaklaşımın yetersiz kaldığı görülmüştür. Bu yetersizlikler Kasım 2022'de kabul edilen NIS II Direktifiyle değiştirilerek AB'nin siber dayanıklılığının güçlendirilmesi hedeflenmiştir[25]. NIS II Direktifi, kritik altyapı kurumlarını hedef alan siber tehditlere karşı kapsamlı koruma sağlamaktadır[26]. Bu düzenleme, hastaneler, bankalar ve enerji şirketleri gibi toplum için hayati önem taşıyan kuruluşların internete bağlı sistemlerini ve dijital altyapılarını korumak amacıyla AB üyesi ülkelerin uyması gereken ortak güvenlik standartlarını belirlemektedir. NIS II'yi tamamlayıcı[27] nitelikte olan CRA ise AB pazarındaki akıllı cihazların ve yazılımların güvenlik kriterlerini düzenleyerek, AB'nin hem kurumsal hem de ürün seviyesinde siber tehditlerden korunmasını sağlamaktadır.

AB'nin siber güvenlik düzenlemeleri alanındaki diğer önemli bir adım ise 2019'da kabul edilen Siber Güvenlik Yasası'dır (*Cyber Security Act*). Bu yasa ile gönüllü sertifikasyon programları ve kritik altyapının korunmasına yönelik kılavuz ilkeler getirilmiştir[28]. Fakat bu gönüllü yaklaşımın dijital

[23] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), Gerekçe 35, (http://data.europa.eu/eli/dir/2016/1148/oj/eng, Erişim Tarihi: 22.08.2025).

[24] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2013:1:FIN. 5. Erişim Tarihi: 22.08.2025)

[25] Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive)- FAQs | Shaping Europe's Digital Future, (https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs. Erişim Tarihi: 22.08.2025)

[26] 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 (NIS II Directive), Madde 2, Madde21, (https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng Erişim Tarihi: 22.08.2025).

[27] NIS II Directive, Gerekçe 22, Madde 4.

[28] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Gerekçe 54, Madde 52(4), (https://data.europa.eu/eli/reg/2019/881/oj/eng, Erişim Tarihi: 22.08.2025)

ürünlerin güvenliğini sağlamada yetersiz kalması, daha kapsamlı ve zorunlu bir düzenleme ihtiyacını ortaya çıkarmıştır[29].

2. CRA'nın Amacı ve Temel Yenilikleri

10 Aralık 2024'te yürürlüğe giren CRA, yatay düzenleyici çerçeve yaklaşımıyla, mevcut mevzuattaki dağınık ve yetersiz düzenlemeleri harmonize eden, dijital bileşenli ürünlerin güvenliğine ilişkin kapsamlı ve zorunlu gereklilikler getiren bir düzenleme olarak şekillendirilmiştir[30]. CRA, AB'nin dijital güvenlik alanında karşılaştığı iki temel soruna çözüm getirmeyi amaçlamaktadır: Dijital bileşenli ürünlerin düşük siber güvenlik seviyesi ve kullanıcıların bu ürünlerin güvenlik özellikleri hakkında yeterli bilgiye sahip olmaması[31].

CRA'nın en önemli yeniliklerinden birisi "tasarım aşamasında güvenlik"[32] ilkesini bir mühendislik yönteminden yasal bir zorunluluğa dönüştürmesidir. Bu kapsamda üreticiler, ürünlerinin tasarım aşamasından başlayarak tüm yaşam döngüsü boyunca siber güvenlik risklerini tespit etmek ve bunlara karşı önlem almak zorundadır[33]. Gerekçe 56'da belirtildiği üzere, üreticiler güvenlik güncellemelerini otomatik olarak sağlamak zorunda olacak ve kullanıcılar bu güncellemeleri kolayca yönetebilecektir. Ayrıca Gerekçe 77'ye göre üreticiler, ürünlerindeki bileşenleri belgeleyerek tedarik zinciri şeffaflığını artıracak ve güvenlik açıklarını daha iyi takip edebilecektir.

Düzenlemenin etkin bir şekilde uygulanabilmesi için geniş bir paydaş katılımı öngörülmüştür[34]. Bu paydaşlar arasında donanım ve yazılım

---

[29] Study on the Need of Cybersecurity Requirements for ICT Products, (https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products. Erişim Tarihi: 22.08.2025).

[30] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 13 March 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act), Madde1, Gerekçe 3-4, (https://data.europa.eu/eli/reg/2024/2847/oj/eng. Erişim Tarihi: 22.08.2025)

[31] Cyber Resilience Act, Gerekçe 1.

[32] *Yazılım mühendisliği disiplininde bilgi sistemlerinin güvenlik gereksinimlerini yazılım geliştirme yaşam döngüsünün başlangıç aşamalarından itibaren sistematik olarak entegre eden proaktif bir metodolojik yaklaşımdır. Bu yaklaşım, güvenlik sorunları ortaya çıktıktan sonra çözüm aramak yerine, güvenlik önlemlerini sistem tasarımının temel bir parçası haline getirir*. Bkz: Del-Real/De Busser/Van den Berg, s.15.

[33] Bygrave, s. 27-43.

[34] Cyber Resilience Act,Madde 9.

üreticileri, ithalatçılar ve dağıtıcılar, ticaret birlikleri, tüketici örgütleri, dijital ürün kullanıcıları ve vatandaşlar, araştırmacılar ve akademisyenler, onaylanmış kuruluşlar ve akreditasyon kuruluşları ile siber güvenlik sektörü profesyonelleri yer almaktadır. Özellikle KOBİ'ler için getirilen kolaylaştırıcı düzenlemeler dikkat çekicidir. Gerekçe 93'te belirtildiği gibi mikro ve küçük işletmeler için basitleştirilmiş teknik dokümantasyon formları sağlanacak, böylece idari yükler hafifletilecektir.

CRA, geniş bir dijital ürün yelpazesi için zorunlu gereklilikler getiren ilk[35] AB mevzuatı olarak, siber güvenliğin ürün tasarımına entegre edilmesini ve sürekli izlenmesini sağlayan kapsamlı bir çerçeve sunmaktadır[36]. Yasanın nihai hedefi, kritik altyapıların ve toplumun işleyişi için vazgeçilmez olan güvenli bir internet ortamı sağlamak ve böylece dijital tek pazarın güvenli ve verimli işleyişini desteklemektir[37].

B. CRA'nın Kapsamı ve Getirdiği Yükümlülükler

CRA, kapsamlı bir yaklaşımla, dijital ürünlerin güvenliğinden sorumlu tüm aktörlere belirli yükümlülükler getirmekte ve bu ürünleri risk bazlı bir yaklaşımla sınıflandırmaktadır. Bu bölümde, yasanın kapsamı ve getirdiği bazı yükümlülükler incelenecektir.

1. Kapsam İçindeki Ürünler ve Sınıflandırma

CRA, dijital ürünlerin siber güvenliğini sağlamak amacıyla üç temel yaklaşım üzerine inşa edilmiştir[38]. İlk yaklaşım olan yatay düzenleme ile dijital bileşenli ürünlerin siber güvenliğine ilişkin dağınık mevzuat yapısını tek bir çerçevede birleştirerek hem hukuki öngörülebilirliği artırmayı hem de pazar bölünmesini önlemeyi hedeflemektedir[39].

Bu noktada Yasa kapsamına giren ürünler, bir cihaza veya ağa doğrudan

[35] Cyber Resilience Act Enters into Force to Make Europe's Cyberspace Safer and More Secure, (https://digital-strategy.ec.europa.eu/en/news/cyber-resilience-act-enters-force-make-europes-cyberspace-safer-and-more-secure. Erişim Tarihi: 22.08.2025)

[36] Kamara, s. 2.

[37] Cyber Resilience Act, Gerekçe 2.

[38] Chiara, s. 3-10.

[39] Cyber Resilience Act,Gerekçe 4; Commission Staff Working Document: Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020, (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52022SC0282. Erişim Tarihi: 22.08.2025)

veya dolaylı olarak mantıksal veya fiziksel veri bağlantısı içeren tüm dijital elementli ürünlerdir[40]. Dijital bileşenli ürün, "*yazılım veya donanım ürünü ve uzaktan veri işleme çözümleri, ayrıca ayrı olarak piyasaya sürülen yazılım veya donanım bileşenleri*" olarak tanımlanmıştır[41]. Bu kapsamda, donanım bileşenleri (örneğin anakartlar, mikroişlemciler), ağ cihazları (yönlendiriciler, modemler, anahtarlar), işletim sistemleri, video düzenleme araçları, akıllı ev ürünleri (akıllı kapı kilitleri, bebek izleme sistemleri, alarm sistemleri), bağlı oyuncaklar ve kişisel giyilebilir sağlık teknolojileri gibi ürünler yasa kapsamındadır[42]. Kapsam dışında bırakılan bazı ürünler tıbbi cihazlar, motorlu taşıtlar, gemiler ile denizcilik ekipmanları şeklindedir[43]. Ayrıca bulut bilişiminin de kapsam dışı olduğu, yazılım hizmet modeli (SaaS), platform hizmet modeli (PaaS) ve altyapı hizmet modelinin (IaaS) NIS II direktifinin uygulandığı kapsamda olduğu netleştirilmiştir[44].

Yasa, dijital ürünleri güvenlik risklerine göre farklı sınıflara ayırarak risk temelli bir yaklaşım benimsemiştir. Ürünler, temel uygunluk değerlendirmesi gerektiren standart ürünler, iki sınıfa ayrılan önemli ürünler (Sınıf I'de tarayıcılar ve şifre yöneticileri, Sınıf II'de güvenlik duvarları ve saldırı tespit sistemleri) ve kritik altyapı bağımlılığı olan kritik ürünler olmak üzere üç kategoride sınıflandırılmaktadır[45]. Önemli ve kritik kategorideki ürünler, yaratabilecekleri yüksek güvenlik riskleri nedeniyle üçüncü taraf denetimi gibi daha kapsamlı uygunluk değerlendirmelerine tabi tutulurken normal ürünler için üreticinin kendi kontrolü yeterli görülmüştür[46]. Bu sınıflandırma gereğince bir ürünün yarattığı risk ne kadar yüksekse, o kadar sıkı güvenlik denetiminden geçmesi gerekmektedir.

CRA'nın üçüncü temel yaklaşımı olan ürün güvenliği ilkesi, ürünlerin piyasaya sürülmeden önce temel güvenlik gerekliliklerini karşılamasını zorunlu

[40] Cyber Resilience Act,Madde 2 (1).

[41] Cyber Resilience Act,Madde 3 (1) (*yazarın çevirisi*).

[42] *Bütün bu ürünler Yasa'nın Ek III (Annex III, Important Products with Digital Elements) başlığı altında sayılmıştır*. Bkz: Cyber Resilience Act Ek III.

[43] Cyber Resilience Act, Madde 2 (2), (3).

[44] Cyber Resilience Act,Gerekçe 12.

[45] Cyber Resilience Act,Gerekçe 44-45, *Ayrıca EkIII ve Ek IV'te hangi ürünlerin hangi sınıfa girdiği açıklanmıştır.*

[46] Cyber Resilience Act,Madde 32.

kılmaktadır. Bu yaklaşım, "Yeni Yasal Çerçeve"[47] ilkeleri doğrultusunda ex-ante bir denetim mekanizması öngörmekte ve ürünlerin piyasaya sürülmeden önce temel gereklilikleri karşılamasını şart koşmaktadır[48].

2. Güvenlik Açığı Raporlama Yükümlülükleri

CRA, dijital ürün üreticilerine kapsamlı bir güvenlik açığı raporlama çerçevesi getirmektedir. Yasa, dijital bileşenli ürün üreticileri için kapsamlı bir siber güvenlik raporlama çerçevesi oluşturarak, güvenlik açıklarının bildirilmesine yönelik zorunlu ve gönüllü raporlama yapılmasını düzenlemiştir.

OLAY TÜRÜ	ZORUNLU/ GÖNÜLLÜ	KRİTER	ÖRNEK
Aktif Sömürülen Güvenlik Açığı	**ZORUNLU**	Dijital unsurda aktif istismar	Saldırganların şu anda kullandığı açık, zararlı yazılımın istismar ettiği zafiyet
Ciddi Olay: Veri/İşlev İhlali	**ZORUNLU**	Hassas veri kaybı veya kritik işlev durması	Veri çalınması, ransomware, sistem çökmesi
Ciddi Olay: Kötü Amaçlı Kod	**ZORUNLU**	Zararlı yazılım tespit edilmesi	Trojan yüklenmesi, malware bulaşması
Pasif Güvenlik Açığı	**GÖNÜLLÜ**	Henüz sömürülmeyen açık	Yazılım testinde bulunan açık, güvenlik denetiminde keşfedilen zafiyet
Başarısız Saldırı *(near miss)*	**GÖNÜLLÜ**	Önlenen ciddi olay	Otomatik sistem tarafından durdurulan saldırı
Risk Artıran Tehdit	**GÖNÜLLÜ**	Güvenlik profilini etkileyen durum	Yeni saldırı tekniği, sektörel tehdit

Tablo 1: CRA m.14 ve m.15 doğrultusunda yapılması gereken raporlamalar[49]

Zorunlu raporlama süreci, sıkı zaman çizelgeleri ve adımları içeren bir yapıya sahiptir. CRA m.14 gereğince ilk olarak, güvenlik açığı öğrenildikten sonra 24 saat içinde bir erken uyarı bildirimi yapılmalıdır. Bu

[47] *AB iç pazarındaki malların dolaşımını ve ürün yerleştirme koşullarını iyileştirmeyi, piyasa gözetimini ve uygunluk değerlendirmelerinin kalitesini artırmayı amaçlayan, aynı zamanda CE işaretini netleştiren ve ürün mevzuatı için genel bir çerçeve oluşturan bir düzenlemedir, Bkz:*New Legislative Framework - European Commission,(https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en. Erişim Tarihi: 22.08.2025)

[48] Chiara, s. 7.

[49] *Tablo, Yasa kapsamındaki zorunlu- gönüllü raporlama ayrımını göstermesi amacıyla yazar tarafından hazırlanmıştır.*

bildirim, ürünün hangi üye devletlerde mevcut olduğunu ve güvenlik açığının temel özelliklerini içerir. Sonrasında, 72 saat içinde daha detaylı bir bildirim gönderilir; bu bildirimde ürün hakkında genel bilgiler, ihlalin niteliği, alınan veya alınabilecek düzeltici önlemler yer alır. Raporlamanın son aşaması, düzeltici bir önlem mevcutsa 14 gün içinde sunulacak nihai rapordur. Bu rapor, güvenlik açığının detaylı bir tanımını, varsa kötü niyetli aktörler hakkında bilgileri ve güvenlik güncellemelerinin detaylarını içerir. Ciddi güvenlik olayları, hassas verilerin korunmasını olumsuz etkileyen veya kötü amaçlı kod girişine neden olabilecek durumlar olarak tanımlanır.

CRA, kullanıcıların bilgilendirilmesine de özel önem vermektedir. Aynı madde gereğince üreticiler, yalnızca teknik mercilere değil, güvenlik açığından etkilenen kullanıcılara da bildirimde bulunmakla yükümlüdürler. Eğer üretici zamanında bilgilendirme yapmazsa, Bilgisayar Güvenliği Olay Müdahale Ekibi (*Computer Security Incident Response Teams*, CSIRT) doğrudan kullanıcıları bilgilendirebilir. Tüm bildirimler, AB genelinde standart hale getirilmiş tek bir raporlama platformu üzerinden yapılır ve üreticinin ana merkezinin bulunduğu üye devletin Bilgisayar Güvenliği Olay Müdahale Ekibine iletilir.

3. Yaptırımlar ve Gönüllü Raporlama

CRA, raporlama yükümlülüklerine uyulmaması durumunda caydırıcı yaptırımlar öngörmektedir. Üretici zorunlu raporlama yapmadığı takdirde 15 milyon Euro'ya varan idari para cezası ile şirketin bir önceki mali yıldaki toplam küresel cirosunun yüzde 2,5'u kadar olan ceza tutarından hangisi daha yüksekse o tutarla cezalandırılacaktır[50].

CRA'nın raporlama yükümlülüklerindeki kavramsal belirsizlikler, düzenlemenin etkinliği açısından önemli sorunlar yaratma potansiyeli taşımaktadır[51]. Bu belirsizliğin temeli, bir güvenlik açığı aktif olarak istismar edildiğinde zorunlu raporlama gerektirirken henüz sömürülmemişse bunun gönüllü raporlama gerektirdiği ve bu durumun tespitine yönelik güvenilir kanıtın kimin tarafından sunulacağının belli olmamasıdır. Bu konuya ilişkin madde, "aktif olarak istismar edilen güvenlik açıklarını" yani yalnızca kötü niyetli aktörlerin fiilen kullandığı, buna ilişkin "güvenilir kanıtların" mevcut

[50] Cyber Resilience Act, Madde 64(2).

[51] Ruohonen/Timmers, s. 5.

olduğu açıkları hedeflemektedir[52]. Yasanın aktif istismar edilen açıklar hakkındaki bu hükmü, gerekçede de belirtildiği üzere iyi niyetli güvenlik testleri, araştırmalar ve sistem güvenliğini artırmaya yönelik müdahaleleri bildirim yükümlülüğünden muaf tutmayı amaçlamaktadır[53]. Bu yaklaşım bir taraftan üretici veya iyiniyetli aktörlerin yaptığı güvenlik testlerini korurken diğer taraftan henüz istismar edilmemiş güvenlik açıklarının "sessizce" düzeltilebilmesine olanak sağlamaktadır. Literatürde "sessiz yama" olarak adlandırılan bu uygulama, üreticilerin keşfettikleri güvenlik açıklarını bilgileri başkalarıyla paylaşmaksızın düzeltmeleri anlamına gelir[54].

Henüz istismar edilmemiş açıkların erken tespit ve düzeltilmesi güvenlik açısından olumlu olmakla beraber bu bilgilerin daha geniş güvenlik topluluğu ile paylaşılmaması, siber sistemlerin iç içe geçmiş yapısı nedeniyle güvenlik açığının bağlantılı başka bir sistemde açık olmaya devam etmesine yol açabilecektir[55]. Ayrıca, üreticilerin ekonomik veya itibar kaygıları ile açıkları henüz istismar olmadığı gerekçesi ile raporlamaktan kaçınmaları, genel tehdit farkındalığının azalması riskini beraberinde getirecektir[56].

---

[52] Cyber Resilience Act, Madde 3(42): "*aktif olarak istismar edilen güvenlik açığı, kötü niyetli bir aktörün sistem sahibinin izni olmaksızın sistemi istismar ettiğine dair güvenilir kanıtların bulunduğu güvenlik açığı anlamına gelir*." (*Yazarın çevirisi*)

[53] "*Aktif olarak istismar edilen güvenlik açıkları, bir üreticinin kullanıcılarını veya diğer gerçek ya da tüzel kişileri etkileyen bir güvenlik ihlalinin, kötü niyetli bir aktörün üreticinin piyasaya sürdüğü dijital unsurlu ürünlerdeki bir kusuru kullanması sonucu ortaya çıktığını belirlediği durumları ifade eder. Bu tür güvenlik açıklarına örnek olarak, bir ürünün kimlik doğrulama ve yetkilendirme fonksiyonlarındaki zayıflıklar gösterilebilir. İyi niyetli test, araştırma, düzeltme veya sistem sahibi ile kullanıcılarının güvenliğini artırmak amacıyla açıklama yapma maksadıyla keşfedilen ve kötü niyetli amaç taşımayan güvenlik açıkları zorunlu bildirim kapsamına alınmamalıdır."* Bkz: Cyber Resilience Act, Gerekçe 68. (*Yazarın çevirisi*)

[54] *Sessiz yama, bir yazılım veya cihaz üreticisinin, ürünlerindeki güvenlik açıklarını kimseye haber vermeden, bir yama numarası (CVE ID) atamadan ve açıklama yapmadan gizlice düzeltmesidir. Bu uygulama, başlangıçta sorunun çözüldüğü izlenimini verse de aslında IT uzmanlarını ve kullanıcıları riskler konusunda bilgisiz bırakır. Bu durum, siber suçluların gizli yamayı inceleyerek açığı keşfetmesine ve diğer sistemlere saldırmasına olanak tanır. Dolayısıyla, sessiz yamalar, siber güvenliğin geliştirilmesi çabalarını engeller ve uzun vadede herkes için daha büyük bir tehlike yaratır.* Ayrıntılı bilgi için Bkz: The risks of silent patching and why it must end, (https://www.techtarget.com/iotagenda/post/The-risks-of-silent-patching-and-why-it-must-end, Erişim tarihi: 22.08.2025), The resounding negative effects of silent patches, (https://www.scworld.com/perspective/the-resounding-negative-effects-of-silent-patches,Erişim tarihi: 22.08.2025), Tang/Kim/Ezzini/Song/Tian/Klein/Bissyande, s.1.

[55] The risks of silent patching and why it must end, (https://www.techtarget.com/iotagenda/post/The-risks-of-silent-patching-and-why-it-must-end, Erişim tarihi: 22.08.2025)

[56] Ruohonen/Timmers, s. 6.

Yine, aktif istismar edilen güvenlik açıklarına ilişkin güvenilir kanıtların üretici tarafından sunulduğu senaryoda, üretici, bu açıkların aktif olarak istismar edilmediğini ileri sürerek sessiz yama seçeneğini tercih edebilecektir. Ancak zorunlu raporlama yükümlülüklerine uyulmamasının karşılığı ağır yaptırımlar, üreticiler açısından doğru raporlama yapma konusunda önemli bir caydırıcılık unsuru oluşturmaktadır. Özellikle m. 60'ta düzenlenen ve pazar gözetim otoritelerinin uyumluluk kontrolü için "tarama" *(sweep)* işlemleri yapma yetkisi bu caydırıcılığı güçlendirmektedir. Kamu otoritelerinin kendi tehdit istihbaratı platformları, güvenlik bilgi ve olay yönetimi sistemleri ile benzer teknik araçlara sahip olması da aktif istismara yönelik güvenilir kanıtların üreticiler harici sunulabilecek olması, üreticilerin sübjektif değerlendirmelerinin sonradan sorgulanabilmesini mümkün kılacaktır[57]. Bu durum, bir güvenlik açığını raporlamamayı tercih eden üreticilerin daha sonra uyumsuz oldukları gerekçesi ile m.64 gereğince yaptırımlarla karşılaşma riskini artıracaktır.

Yukarda belirtildiği üzere, CRA zorunlu raporlamanın yanı sıra gönüllü raporlama mekanizmaları da sunmaktadır. Bu doğrultuda yasa m.15, henüz zorunlu bildirim gerektirmeyen güvenlik açıkları, potansiyel tehditler ve yakın tehlike oluşturan güvenlik vakaları hakkında gönüllü olarak rapor verilmesini düzenlemiştir. Üreticiler itibar ve finansal kaygılarla güvenlik açıklarını olduğundan daha az önemli gösterme eğiliminde olabilecekleri göz önünde bulundurulduğunda, bu esnekliğin siber güvenlik raporlama sisteminin etkinliğini ciddi biçimde zayıflatma riski taşıdığı düşünülebilir.

II. AI ACT VE CRA: DİJİTAL GÜVENLİK DÜZENLEMELERİNİN ETKİLEŞİMİ

AI Act ve CRA arasındaki ilişki, AB'nin dijital teknolojilere yönelik bütüncül yaklaşımını gösterir şekilde kapsam ve uygulama açısından iç içedir[58]. Her iki düzenleme beş temel noktada birleşmektedir: iç pazarda dijital teknolojilerin güvenliğini ve güvenilirliğini sağlama amacı, risk bazlı bir yaklaşımla şirketlere getirilen uyum yükümlülükleri, kişisel verilerin korunmasına verilen özel önem, dijital teknolojilere olan tüketici güvenini artırma hedefi ve KOBİ'lerin uyum maliyetlerine gösterilen hassasiyet[59].

[57] Ruohonen/Timmers, s. 6.

[58] *Yeni Yasal Çerçeve, bu bütüncül yaklaşımı açık bir şekilde göstermektedir.* Bkz: dn. 35

[59] Bagni, s. 213.

A. Yüksek Riskli Yapay Zekâ Sistemlerinde Siber Güvenlik Gereklilikleri

CRA'nın 51'inci Gerekçesine göre AI Act m.6 uyarınca yüksek riskli yapay zekâ sistemleri olarak sınıflandırılan ve CRA kapsamına giren dijital bileşenli ürünler, CRA'da belirtilen temel siber güvenlik gerekliliklerine uymalıdır. Aynı doğrultudaki yaklaşım AI Act'in 77'nci gerekçesinde de vurgulanmaktadır. AI Act'in CRA'dan önce yürürlüğe girdiği göz önünde bulundurulduğunda, gerekçe metninde "*dijital bileşenleri olan ürünler için yatay siber güvenlik gereksinimlerine ilişkin Avrupa Parlamentosu ve Konseyi tüzüğü*" ifadesiyle gelecekteki CRA düzenlemesi öngörülmüş ve iki düzenleme arasındaki uyumluluğun hukuki çerçevesi çizilmiştir. Bu çerçeveye göre eğer bir yüksek riskli yapay zekâ sistemi CRA kapsamındaki temel gereklilikleri karşılıyorsa ve bunu AB uygunluk beyannamesi ile belgelendirmişse, AI Act'in siber güvenlik şartlarını da yerine getirmiş kabul edilir. Ancak bu değerlendirme sürecinde yapay zekaya özgü güvenlik tehditleri mutlaka göz önünde bulundurulmalıdır; yetkisiz müdahaleler sonucu sistemin kullanımının değiştirilmesi, veri zehirlenmesi ve düşmanca saldırılar gibi yapay zekaya özel güvenlik açıkları ile temel haklara yönelik risklerin dikkate alınması gerekmektedir[60]. Bu yaklaşım ile hem genel siber güvenlik standartları korunurken hem de yapay zekâ sistemlerinin kendine özgü risklerinin etkin biçimde değerlendirilmesi sağlanmaktadır.

B. Düzenlemeler Arasındaki Uyumluluk Mekanizmaları

CRA m.12 gereğince, yüksek riskli yapay zekâ sistemleri olarak sınıflandırılan dijital ürünlerin (kritik dijital ürünler hariç), AI Act m.15'te belirtilen siber güvenlik gerekliliklerini karşılamaları durumunda, CRA ile de uyumlu kabul edileceğini belirtmektedir.

Bu uyum mekanizması bağlamında değerlendirildiğinde, AI Act ve CRA arasındaki etkileşimin incelenmesi, AB'nin dijital teknolojilere yönelik koordineli adımlarını ortaya koymaktadır[61]. Bu çerçevede yapay zekâ sistemlerine getirilen düzenlemeler, teknolojik inovasyonu yavaşlatma riskini barındırdığı için eleştirilse de[62] uzun vadede daha güvenilir ve sürdürülebilir

[60] AI Act, Gerekçe 77.

[61] Burri/Zihlmann, s.20, Mueck/On/Du Boispean, s.98-100., Bolgouras/Zarras/Leka/Stylianou/Farao/Xenakis, (*Yazarlar bu etkileşimi daha geniş bir düzenleyici çerçevede incelemişlerdir.*), s.5.

[62] Bradford, s.393, Castro/McLaughlin, s.12, McAfee, "EU proposals to regulate AI are only

bir dijital ekosistem oluşturulması için gerekli görüldüğü için AB yasa koyucusu tarafından düzenlenmesinden kaçınılmamıştır[63].

III. ÜRÜN SORUMLULUĞU DİREKTİFİ (PLD): DİJİTAL ÇAĞDA YENİLENEN SORUMLULUK REJİMİ

1985'ten bu yana AB'nin ürün sorumluluğu rejiminin temelini oluşturan PLD, dijital çağın getirdiği yeni zorluklar karşısında yetersiz kalmıştır. Özellikle hatalı yazılım güncellemeleri, kusurlu algoritmalar ve dijital hizmetlerdeki sorumluluk belirsizliği gibi konularda önemli yasal boşluklar ortaya çıkmıştır[64]. Bu eksiklikleri gidermek amacıyla 23 Ekim 2024'te yayımlanan yeni direktif, yapay zekâ sistemleri, döngüsel ekonomi iş modelleri ve küresel tedarik zincirlerindeki gelişmeler ışığında ürün kavramının kapsamını yeniden tanımlamakta ve mevcut yasal belirsizlikleri gidermeyi hedeflemektedir[65].

A. Yazılımların Hukuki Statüsü ve Ürün Kapsamı

Direktifin getirdiği en önemli yeniliklerden biri, yazılımların hukuki statüsüne ilişkin düzenlemedir[66]. Bu bağlamda Direktif, yazılım teknolojilerini (işletim sistemleri, donanım yazılımları, bilgisayar programları, uygulamalar ve yapay zekâ sistemleri dahil olmak üzere) ürün kapsamında açıkça

---

going to hinder innovation", 2021, (https://www.ft.com/content/a5970b6c-e731-45a7-b75b-721e90e32e1c, Erişim tarihi: 22.08.2025), Timis, "How to regulate AI without stifling innovation", (https://www.weforum.org/stories/2023/06/how-to-regulate-ai-without-stifling-innovation, Erişim tarihi: 22.08.2025), *Düzenlemelerin inovasyonu yavaşlatmayabileceği yönünde görüşler de bulunmaktadır. Doğru tasarlanmış düzenlemelerin AI inovasyonunu destekleyebileceği yönünde* Bkz: Tartaro/Smith/Shaw, s.4-5, Bradford, s.450-453. *Çok katı düzenlemelerin inovasyonu engelleyebileceği, hiç düzenleme yapılmaması sonucu yetersiz denetimin de halkın güvenini sarsacağı ve yapay zekanın kötüye kullanılmasına yol açabileceği yönündeki görüş için* Bkz: Bolgouras/Zarras/Leka/Stylianou/Farao/Xenakis, s.16.

[63] Tartaro/Smith/Shaw, s.4-5., Commission Staff Working Document Impact Assessment Accompanying the Proposal for a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts EU (2021), (https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence, Erişim Tarihi: 22.08.2025)

[64] Q&As on the Revision of the Product Liability Directive, (https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5791, Erişim Tarihi: 22.08.2025)

[65] Directive (EU) 2024/2853 of the European Parliament and of the Council of 13 March 2024 on liability for defective products (Product Liability Directive), Gerekçe 3, (https://data.europa.eu/eli/dir/2024/2853/oj/eng, Erişim Tarihi: 22.08.2025)

[66] Product Liability Directive,Gerekçe 13.

tanımlamaktadır. Söz konusu yazılımlar, münferit bir ürün olarak piyasaya sürülebildiği gibi mevcut ürünlere entegre edilerek de kullanılabilmekte ve işleyişleri esnasında potansiyel risk teşkil edebilmektedir.

Direktif, hukuki belirlilik ilkesi çerçevesinde, yazılımların kusursuz sorumluluk kapsamında bir ürün olarak değerlendirilmesi konusunda açık bir düzenleme getirmektedir[67]. Buna göre yazılım, ister yerel bir cihazda depolanmış olsun, ister iletişim ağı veya bulut teknolojileri üzerinden erişilsin, isterse yazılım-hizmet (*software-as-a-service*) modeli aracılığıyla tedarik edilsin, tedarik ve kullanım şeklinden bağımsız olarak ürün kapsamında değerlendirilir[68]. Bununla birlikte, "bilgi" kavramı ürün tanımının dışında tutulmuş, ürün sorumluluğu normları dijital dosyaların içeriği olan bilgilere (medya dosyaları, e-kitaplar) ve yazılımların salt kaynak kodlarına kadar genişletilmemiştir[69]. Keza ticari amaçla dağıtılmayan açık kaynak yazılımları da ürün tanımının kapsamı dışında bırakılmıştır[70]. Açık kaynak yazılımlarının geliştiricilerinin bu projelerde çoğunlukla gönüllü olarak ve ücretsiz çalıştığı göz önünde bulundurulduğunda, sorumluluk kapsamı dışında bırakılmaları bu değerli çalışmaları engellememek adına önemlidir[71].

B. Yapay Zekâ Sistemlerinde Üretici Sorumluluğu

Direktifin yapay zekâ sistemlerini ürün olarak kabulünün yanı sıra, AI Act ile uyumlu bir şekilde, yapay zekâ sistem tedarikçileri de dahil olmak üzere, yazılım geliştiricileri ve üreticileri "imalatçı" statüsünde değerlendirilmektedir[72]. Üretici kavramının imalatçıyı da kapsayacak şekilde genişletilmesinin nedeni, pek çok ürünün artık AB dışında üretilmesi olarak gösterilmiştir[73]. Bu çerçevede yapay zekâ sistemlerinin özelliklerini dikkate alarak, sistemin öğrenme kabiliyeti veya piyasaya sürüldükten sonra yeni özellikler kazanma yeteneğinin ürün güvenliği değerlendirmesinde dikkate alınması gerektiği ve üreticinin beklenmeyen davranışlardan kaynaklanan

[67] Product Liability Directive, Madde 4, Madde 8.

[68] Product Liability Directive, Gerekçe 13.

[69] *Direktif henüz teklif halindeyken "bilgi" nin kapsam dışında tutulması, Wagner tarafından ABAD'ın "Krone" içtihatıyla aynı doğrultuda olduğu şeklinde yorumlanmıştır*. Bkz: Wagner, s. 13.

[70] Product Liability Directive, Gerekçe 14-15.

[71] Schütte, s.88.

[72] Product Liability Directive, Gerekçe 13.

[73] Schütte, s.89.

zararlardan sorumlu olacağını öngörülmektedir[74]. Bu düzenleme, yapay zekâ sistemlerinden kaynaklanabilecek zararların tazmin rejimini belirginleştirmekte ve zarar gören gerçek kişilerin[75] haklarının korunmasına yönelik önemli bir adım teşkil etmektedir.

C. İspat Yükünün Hafifletilmesi

Yapay zekâyı kapsayan önemli yeniliklerden bir diğeri ürün sorumluluğuna ilişkin davalarda getirilen ispat kolaylığıdır[76]. Bu düzenleme, davaya konu ürünü üreten üreticinin karşı tarafa kıyasla daha fazla bilgiye sahip olduğu gerekçesine dayanmakta ve belirli koşullarda uygulanmaktadır[77]. Bu çerçevede, teknik veya bilimsel karmaşıklık nedeniyle davacının ürünün kusurluluğunu veya kusurluluk ile zarar arasındaki illiyet bağını ispatlamasının aşırı derecede güç olduğu ve davacının kusurluluk veya illiyet bağının muhtemel olduğunu ortaya koyduğu durumlarda, m.9 uyarınca davalı tarafından delillerin ifşasına rağmen mahkemeler kusurluluğu veya illiyet bağını karine olarak kabul edebilecektir[78].

Bu durumda, ispat zorluğunun kusurluluğun kanıtlanmasına ilişkin olduğu hallerde davacının ürünün kusurlu olmasının muhtemel olduğunu ortaya koyması yeterlidir. İspat zorluğunun nedensellik bağını kanıtlamaya ilişkin olduğu hallerde ise ürünün kusurluluğunun zararın olası nedeni olduğunu göstermesi yeterli sayılır. Davacının bu zorlukları göstermek için argüman sunması yeterli olup, bunların ispatı gerekmemektedir. Örneğin yapay zekâ sistemleriyle ilgili bir davada, davacının sistemin kendine özgü özelliklerini veya bu özelliklerin nedensel bağı kurmayı nasıl zorlaştırdığını açıklaması gerekmez. Bu değerlendirmede ürünün karmaşık yapısı (örneğin yenilikçi bir tıbbi cihaz), kullanılan teknolojinin karmaşıklığı (örneğin makine öğrenmesi), analiz edilmesi gereken bilgi ve verilerin karmaşıklığı ve nedensel bağlantının karmaşık yapısı (örneğin bir ilaç veya gıda ürünü ile bir sağlık durumunun başlangıcı arasındaki bağlantı) gibi faktörler dikkate alınacaktır. Bununla birlikte davalı, aşırı zorlukların varlığı da dahil olmak üzere iddianın tüm unsurlarına itiraz etme hakkına sahiptir.

---

[74] Product Liability Directive, Gerekçe 32.

[75] Product Liability Directive, Madde 5.

[76] European Law Institute, s. 9-10.

[77] *İspat kolaylığı yazarlar tarafından "adalete erişimin kolaylaştırılması" başlığıyla açıklanmıştır*. Bkz: Li/Schütte, s.18.

[78] Product Liability Directive, Gerekçe 48; Arat/ Akıncı, s. 396-400.

D. Siber Güvenlik ve Sürekli Sorumluluk Anlayışı

CRA ile de yakın ilişki içinde olan Direktif, siber güvenlik konusunda önemli düzenlemeler getirmektedir. Buna göre bir ürünün siber güvenlik açığı nedeniyle kusurlu olduğu kabul edilebilecek[79] ve üreticiler, gelişen siber güvenlik risklerine karşı ürünlerinin güvenlik açıklarını gidermek için gerekli yazılım güncellemelerini sağlamadıkları takdirde sorumluluktan kurtulamayacaklardır[80]. Bu düzenleme, üreticilerin ürünün yaşam döngüsü boyunca siber güvenliğini sağlama yükümlülüğünü vurgulamaktadır.

Dijital çağın getirdiği yeni ihtiyaçlar ve manevi varlıklarımızın artan önemi doğrultusunda, Direktif ile dijital verilerin kaybı veya bozulması durumunda tazminat hakkı tanınmış ve tıbbi olarak kanıtlanabilen psikolojik zararlar kişisel yaralanma kapsamına dahil edilmiştir[81]. Karma kullanımlı malların yaygınlaşması nedeniyle hem özel hem profesyonel amaçla kullanılan varlıklara gelen zararlar tazminat kapsamına alınırken,[82] salt profesyonel amaçlı zararlar kapsam dışı bırakılmıştır[83]. Bu husus, özel amaçlı- profesyonel amaçlı kullanım ayrımının halen korunmasının, direktifin amacının "zayıf tüketiciyi korumak" değil, "üreticiyi daha güvenli ürünler üretmeye teşvik etmek" yönünde değiştiğinden dolayı gerekli olmadığı yönünde eleştirilmektedir[84]. Üreticiyi daha güvenli ürünler üretmeye teşvik edilmesi, ispat yükünün hafifletilmesi ile değerlendirildiğinde, genel olarak tüketiciler ve zarar gören gerçek kişiler için olumlu bir adım olmakla birlikte, bu düzenlemenin üreticiler üzerindeki muhtemel etkileri henüz netlik kazanmamıştır.

Zararın tespiti çerçevesinde ise yasal kesinlik ihtiyacı gözetilerek, tazminat hesaplama yetkisi üye devletlere verilmiş ve manevi zararların tazmini ulusal yasalara bırakılmıştır. Saf ekonomik kayıp ve gizlilik ihlalleri gibi durumlar ise tek başına tazminat nedeni sayılmamıştır[85].

---

[79] Product Liability Directive, Gerekçe 32.

[80] Product Liability Directive, Gerekçe 51.

[81] Product Liability Directive, Gerekçe 20-21; Wagner, s. 21-25; European Law Institute, s. 8.

[82] Product Liability Directive, Gerekçe 25.

[83] Product Liability Directive, Gerekçe 22.

[84] Wagner, s. 22.

[85] Product Liability Directive, Gerekçe 24.

IV. CRA, AI ACT VE PLD ETKİLEŞİMİNDE DİJİTAL ÜRÜN SORUMLULUĞU

Bu düzenlemeler çerçevesinde dijital ürün sorumluluğu çerçevesindeki gereklilikler, özellikle yapay zekâ sistemleri ve siber dayanıklılık perspektifinden bakıldığında üreticilerin yükümlülüklerinin genişletildiğini göstermektedir.

A. Gelişim Riski Savunmasının Pratik Zorlukları

Dijital ürünler ve yapay zekâ sistemleri açısından önemli bir zorluk, PLD'nin m.11 'e' bendinde düzenlenen "gelişim riski" sorumluluktan muafiyet savunmasının, üreticinin ürünü piyasaya sürdüğü veya hizmete soktuğu sırada ya da kontrolü altında olduğu dönemde, bilimsel ve teknik bilginin nesnel durumunun kusuru tespit etmeye elverişli olmadığını kanıtlaması halinde kullanılabilecekken, bu savunmanın başarıyla ileri sürülmesinin pratikte oldukça zor olmasıdır[86].

Bu zorluğun temel nedenlerinden birincisi, CRA üreticilere kapsamlı yükümlülükler getirmektedir. Üreticiler ürünlerini bilinen güvenlik açıklarından arındırılmış şekilde piyasaya sürmeli (CRA Ek I), ürün yaşam döngüsü boyunca siber güvenliği korumalı (32. Gerekçe) ve yeni keşfedilen güvenlik açıklarına 24 saat içinde müdahale etmelidir (m.11). Avrupa Birliği Siber Güvenlik Ajansı (ENISA)'nın oluşturacağı güvenlik açığı veritabanı da üreticilerin güvenlik sorunlarını proaktif şekilde izlemesini zorunlu kılacak, bu da kusurun "tespit edilemez" olduğunu kanıtlamayı güçleştirecektir[87].

İkincisi, yapay zekâ sistemleri için özel zorluklar mevcuttur. Üreticiler sistemlerin kendi kendine öğrenme yeteneklerini ve potansiyel etkilerini sürekli izlemeli ve ürünlerin kullanım ve güncellemeler yoluyla gelişirken dahi güvenli kalmasını sağlamalıdır[88]. Bu sistemlerin öngörülemezliği ve öğrenme yetenekleri, bunların ürünün doğal karakteristik özellikleri olarak değerlendirilmesi nedeniyle "bilinmeyen risk" olarak nitelendirilmelerini zorlaştırmaktadır[89].

Üçüncüsü, PLD m.11(2) üreticinin kontrolü altındayken ortaya çıkan;

---

[86] Grau, s. 5-18, *Gelişim riski konusunda detaylı açıklama için* Bkz: Çekin, s.180-185.

[87] Grau,s. 18.

[88] Cyber Resilience Act, Madde 7(2)(c),11(1)(e), 11(2)(b), Madde 11(2)(c), Madde 7(2)(e).

[89] Grau, s. 11.

"*İlgili bir hizmet, yazılım güncellemeleri veya yükseltmeleri, güvenlik için gerekli yazılım güncellemelerinin eksikliği, ürünün önemli bir modifikasyonu nedeniyle oluşan kusurlar*" için bu savunmanın kullanılamayacağını açıkça düzenlemiştir[90].

Sonuç olarak, gelişen teknoloji çağı bilimsel ve teknik bilgilere ulaşmayı önemli ölçüde kolaylaştırmıştır. Bu durum, üreticilerin ilgili teknik ve bilimsel gelişmelerden haberdar olmadıklarına yönelik savunmalarını inandırıcı olmaktan çıkarmakta ve böyle bir mazeret sunmalarını giderek daha zor hale getirmektedir[91]. Dolayısıyla bu savunma teoride mümkün olmakla birlikte, yeni yasal çerçevenin getirdiği kapsamlı yükümlülükler ve sürekli sorumluluk anlayışı nedeniyle pratikte başarıyla uygulanması oldukça zor görünmektedir.

B. Tamamlayıcı Düzenlemeler ve Çift Yönlü Koruma Mekanizması

Dijital ürün sorumluluğu açısından CRA ve PLD, birbirini tamamlayıcı nitelikte düzenlemeler getirerek dijital ürünlerin siber güvenliğini sağlamada çift yönlü bir koruma mekanizması oluşturmaktadır. Bu tamamlayıcılık özellikle şu noktalarda belirgindir: CRA m.13 gereğince üreticilere getirilen risk değerlendirmesi yapma ve güvenlik açıklarını yönetme yükümlülüğü, PLD m.7'de düzenlenen kusur tanımıyla doğrudan bağlantılıdır; zira risk değerlendirmesinin yetersizliği veya güvenlik açıklarının giderilmemesi, ürünün kusurlu sayılmasına yol açmaktadır. Benzer şekilde, CRA'nın m.13(8) ve m.13(9) da düzenlenen güvenlik güncellemelerine ilişkin yükümlülükler, PLD m.11 de düzenlenen sorumluluk rejimiyle bütünleşmektedir; güncellemelerin sağlanmaması hem düzenleyici yaptırımlara hem de tazminat sorumluluğuna yol açmaktadır. Bu tamamlayıcılık, üreticileri güvenlik önlemleri almaya teşvik ederken (CRA m. 6), olası ihlallerde etkin bir telafi mekanizması sağlamaktadır (PLD m.6). Dolayısıyla CRA'nın önleyici tedbirleri ile PLD'nin telafi edici mekanizmaları, dijital ürünlerin güvenliği için kapsamlı ve etkin bir koruma sistemi oluşturmaktadır.

Üç düzenlemenin etkileşiminde oluşan dijital ürün sorumluluğu

[90] Product Liability Directive, Madde 11(2) *"[...] By way of derogation from paragraph 1, point (c), an economic operator shall not be exempted from liability where the defectiveness of a product is due to any of the following, provided that it is within the manufacturer's control:(a) a related service;(b)software, including software updates or upgrades;(c)a lack of software updates or upgrades necessary to maintain safety;(d)a substantial modification of the product"* (*Yazarın çevirisi*)

[91] Grau, s. 6.

rejiminde, gelişim riski savunmasının pratikte uygulanmasının zorluğu dikkat çekicidir. Bu durum, üreticilerin dijital ürünlerin güvenliğini sağlama konusundaki sorumluluklarını önemli ölçüde genişletmektedir. Bu genişlemenin inovasyon üzerinde engelleyici etki yaratma potansiyeli bulunsa da CRA ve PLD'nin oluşturduğu çift yönlü koruma mekanizmasının, dijital ürünlerin güvenliği için kapsamlı ve etkin bir sistem sunduğu değerlendirilmektedir. Bu mekanizma hem önleyici tedbirleri hem de telafi edici araçları içermesi bakımından dengeli bir yaklaşım sergilemektedir.

SONUÇ

Bu çalışma, AB'nin dijital güvenlik ekosisteminin merkezinde yer alan CRA'yı detaylı olarak incelemeyi ve bu düzenlemenin AI Act ve PLD ile etkileşimini analiz etmeyi amaçlamıştır. Bu doğrultuda, CRA'nın dijital bileşenli ürünlerin siber güvenliğini sağlama konusundaki merkezi rolü ve diğer düzenlemelerle oluşturduğu bütüncül çerçeve ortaya konulmuştur.

CRA'nın AI Act ve PLD ile etkileşimi, özellikle yapay zekâ bileşenli ürünlerin siber güvenliği ve bu ürünlerden kaynaklanan zararlardan sorumluluk konularında belirgin şekilde ortaya çıkmaktadır. CRA'nın bağlantılı ürünlerin siber güvenliğini temin etme hedefi, AI Act'in yapay zekâ sistemlerinin güvenli gelişimini sağlama amacıyla tamamlanmakta, PLD ise bu iki düzenlemeyi destekleyerek dijital çağda modernize edilmiş bir ürün sorumluluğu rejimi sunmaktadır.

Bu düzenleyici çerçevenin pratik etkileri değerlendirildiğinde, özellikle üreticiler açısından önemli zorluklar ortaya çıkmaktadır. CRA'nın getirdiği kapsamlı siber güvenlik gereklilikleri, üreticilerin ürün geliştirme ve pazara sunum süreçlerinde köklü değişiklikler yapmalarını gerektirmektedir[92]. Bir ürünün yaşam döngüsünün her aşamasında siber güvenliğin entegre edilmesi gerekliliği, mevcut süreçlerde önemli değişiklikler gerektirmekte, üreticilerin uyumluluk, inovasyon ve pazara sunum stratejilerine yaklaşımlarını yeniden düşünmelerini zorunlu kılmaktadır[93]. Özellikle KOBİ'ler, kaynak kısıtlamaları ve potansiyel olarak yüksek uyumluluk maliyetleri nedeniyle ek engellerle karşılaşmakta, bu da yeni hukuki ortamda rekabetçi ve uyumlu kalma yeteneklerini tehdit etmektedir[94]. Buna ek olarak, üreticiler sadece mevcut

[92] Schoo, s. 245.

[93] Parvanov, s. 13.

[94] Parvanov, s. 13.

riskleri ele almakla kalmayıp, aynı zamanda ürünlerini gelecekteki tehditlere karşı korumak için proaktif önlemler de almalıdır ki bu da halihazırda ağır olan uyumluluk yüküne katkıda bulunmaktadır[95].

Araştırmanın sonuçları, CRA merkezli bu üçlü düzenleyici çerçevenin, dijital dönüşümün getirdiği güvenlik ve sorumluluk sorunlarına kapsamlı bir yanıt sunma potansiyeli taşıdığını göstermektedir. Bu çerçeve, siber güvenlik risklerinin proaktif yönetimini teşvik ederken, olası ihlallere karşı etkin bir telafi mekanizması oluşturarak AB'nin dijital tek pazarında güven ve dayanıklılığı artırma potansiyeline sahiptir. Ancak, özellikle KOBİ'ler için uyum maliyetleri ve karmaşık gerekliliklerin yaratacağı zorluklar göz ardı edilmemelidir.

Gelecekte bu düzenlemelerin etkilerini değerlendirirken, inovasyon ve siber güvenlik arasındaki dengenin nasıl korunduğu, üreticilerin uyum maliyetlerinin nasıl yönetildiği ve en önemlisi, dijital ürünlerin güvenliğinde somut bir iyileşme sağlanıp sağlanmadığı sorularına odaklanılması önem taşımaktadır. AB'nin bu alanda öncü rol üstlenmesi takdire değer olmakla birlikte, düzenlemelerin küresel standartları nasıl şekillendireceği ve diğer bölgelerin benzer çerçeveleri benimseyip benimsemeyeceği de yakından izlenmelidir.

[95] Schoo, s. 249.

KAYNAKÇA

Arat, Ayşe/ Akıncı, Elif, "2022/0302 Sayılı Avrupa Birliği Yeni Ürün Sorumluluk Direktif Teklifinin Getirdikleri Üzerine Bir Değerlendirme", İstanbul Hukuk Mecmuası, 2024, C. 82, S. 2, s. 363-407.

Bagni, Filippo, "The Regulatory Sandbox and the Cybersecurity Challenge: From the Artificial Intelligence Act to the Cyber Resilience Act", Rivista Italiana Di Informatica e Diritto, 2023, Vol.5, No. 2, s.201-217.

Beardsley, Tod, "The resounding negative effects of silent patches", SC World, Vulnerability Management. (https://www.scworld.com/perspective/the-resounding-negative-effects-of-silent-patches, Erişim Tarihi: 22.08.2025)

Bolgouras, Vaios/ Zarras, Apostolis/ Leka, Christian/ Stylianou, Ioannis/ Farao, Aristeidis/ Xenakis, Christos, "Eu regulatory ecosystem for ethical AI", AI Ethics, 2025.

Bradford, Anu, "The False Choice Between Digital Regulation and Innovation", Northwestern University Law Review, 2024, C. 118, S. 2.

Burri, Mira/ Zihlmann, Zaira, "The EU Cyber Resilience Act – An Appraisal and Contextualization", Zeitschrift für Europarecht (EuZ), 2023, S. 2, s. B1-B45.

Bygrave, Lee A, "Cyber Resilience versus Cybersecurity as Legal Aspiration", 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon), 2022, s. 27-43.

Castro, Daniel/ McLaughlin, Michael, "Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence", Information Technology & Innovation Foundation, 2019. (https://www2.itif.org/2019-precautionary-principle.pdf, Erişim Tarihi: 22.08.2025).

Chiara, Pier Giorgio, "Towards a right to cybersecurity in EU law? The challenges ahead", Computer Law & Security Review, 2024, C. 53, s. 105961.

Chiara, Pier Giorgio, "Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?", European Journal of Risk Regulation, European Journal of Risk Regulation, 2025, s.1–16.

Commission Staff Working Document Impact Assessment Report: Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, 2022, (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52022SC0282., Erişim Tarihi: 22.08.2025)

Contreras, Ricardo Rodriguez, "COVID-19 and Digitalisation", (https://www.eurofound.europa.eu/en/covid-19-and-digitalisation#:~:text=According%20to%20the%20Organisation%20for,models%2C%20the%20promotion%20of%20online., Erişim Tarihi: 22.08.2025)

"Cyber Resilience Act Enters into Force to Make Europe's Cyberspace Safer and More Secure", Shaping Europe's Digital Future, (https://digital-strategy.ec.europa.eu/en/news/cyber-resilience-act-enters-force-make-europes-cyberspace-safer-and-more-secure, Erişim Tarihi: 22.08.2025)

Çekin, Mesut Serdar, «Güncel Gelişmeler Işığında AB ve Türk Hukukunda Dijital Ürünlere İlişkin Ürün Sorumluluğu ve Ürün Güvenliği Düzenlemeleri Üzerine Değerlendirme», Türk-Alman Üniversitesi Hukuk Fakültesi Dergisi, 2025, C. 7, S. 1, s. 156-202.

Del-Real, Cristina/ De Busser, Els/ van den Berg, Bibi, "Shielding software systems: A comparison of security by design and privacy by design based on a systematic literature review", Computer Law & Security Review, 2024, C. 52, s. 105933.

"Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive)- FAQs", Shaping Europe's Digital Future.(https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs, Erişim Tarihi: 22.08.2025)

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), Official Journal of the European Union L 194 (http://data.europa.eu/eli/dir/2016/1148/oj/eng, Erişim Tarihi: 22.08.2025)

Directive (EU) 2024/2853 of the European Parliament and of the Council of

13 March 2024 on liability for defective products (Product Liability Directive), Official Journal of the European Union L, (https://data.europa.eu/eli/dir/2024/2853/oj/eng, Erişim Tarihi: 22.08.2025)

dos Santos, Daniel, "The risks of silent patching and why it must end", TechTarget IoT Agenda, 29.12.2021. (https://www.techtarget.com/iotagenda/post/The-risks-of-silent-patching-and-why-it-must-end, Erişim Tarihi: 22.08.2025)

Dupont, Benoît, "The Cyber-Resilience of Financial Institutions: Significance and Applicability", Journal of Cybersecurity, 2019, Vol.5, No. 1, s.1-17.

ElSayed, Zag/ Abdelgawad, Ahmed/ Elsayed, Nelly, "Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions", arXiv preprint arXiv:2501.11250, 2025.

European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade", (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN%3A2020%3A18%3AFIN, Erişim Tarihi: 22.08.2025)

European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace", JOIN (2013) 1 final. (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2013:1:FIN, Erişim Tarihi: 22.08.2025)

European Commission, "Q&As on the Revision of the Product Liability Directive", (https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5791, Erişim Tarihi: 22.08.2025)

European Law Institute, "Guiding Principles for Updating the Product Liability Directive for the Digital Age". Innovation Paper Series, 2021. (https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Guiding_Principles_for_Updating_the_PLD_for_the_Digital_Age.pdf., Erişim Tarihi: 22.08.2025)

Fahey, Elaine, "The evolution of EU–US cybersecurity law and policy: on

drivers of convergence", Journal of European Integration, 2024, C. 46, S. 7, s. 1073-1088.

Federal Office for Information Security,"2024 State of IT Security in Germany Report", (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2024.html?nn=1021082., Erişim Tarihi: 22.08.2025)

Google Threat Intelligence Group, "Cybercrime: A Multifaceted National Security Threat", Google Cloud Blog, 2025. (https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat, Erişim Tarihi: 22.08.2025)

GOV.UK, "The UK Product Security and Telecommunications Infrastructure (Product Security) Regime", (https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime., Erişim Tarihi: 22.08.2025)

Grau, Guillem Izquierdo, "The Development Risks Defence in the Digital Age",European Journal of Risk Regulation, 2025, Vol.16, s.197–216.

Güçlütürk, Osman Gazi, "Avrupa Birliği Yapay Zeka Tüzük Tasarısı ve Siber Güvenlik", Gelişen Teknolojiler ve Hukuk IV: Siber Güvenlik içinde, (Ed. E. Eylem Aksoy Retornaz/ Osman Gazi Güçlütürk), On İki Levha Yayıncılık, İstanbul, 2023, s. 207-222.

Huang, Keman/ Siegel, Michael/ Madnick, Stuart, "Cybercrime-as-a-Service: Identifying Control Points to Disrupt", Cybersecurity Interdisciplinary Systems Laboratory (CISL) Working Paper, 2017, S. 2017-17, s. 1-30.

Kamara, Irene, "European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience". Innovation: The European Journal of Social Science Research, Vol.37, No.5, s.1441–1460.

Koch, Robert/ Golling, Mario, "Silent Battles: Towards Unmasking Hidden Cyber Attack", 2019 11th International Conference on Cyber Conflict (CyCon), 2019, s.1-20.

Lallie, Harjinder Singh/ Shepherd, Lynsay A./ Nurse, Jason R.C./ Erola, Arnau/ Epiphaniou, Gregory/ Maple, Carsten/ Bellekens, Xavier, "Cyber security in the age of COVID-19: A timeline and analysis of cybercrime and cyber-attacks during the pandemic". Computers & Security,2021, Vol. 102248.

Li, Yuchong/ Liu, Qinghui, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments", Energy Reports, 2021, C. 7, s. 8176-8186.

Li, Shu/ Schütte, Béatrice, "The proposal for a revised Product Liability Directive: The emperor's new clothes?", Maastricht Journal of European and Comparative Law, 2023, s. 1-24.

Ludvigsen, Kaspar Rosager, "Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law", arXiv preprint arXiv:2503.07250, 2025.

McAfee ,Andrew, "EU proposals to regulate AI are only going to hinder innovation", Financial Times, 2021. (https://www.ft.com/content/a5970b6c-e731-45a7-b75b-721e90e32e1c, Erişim Tarihi:22.08.2025)

McGlave, Claire/ Neprash, Hannah/ Nikpay, Sayeh, "Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients", SSRN Electronic Journal, 2023.

"Microsoft Digital Defense Report 2024", (https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024, Erişim Tarihi: 22.08.2025)

Mueck, Markus Dominik/ On, Amit Elazari Bar/ Du Boispean, Stephane, "Upcoming European Regulations on Artificial Intelligence and Cybersecurity", IEEE Communications Magazine, 2023, C. 61, S. 7, s. 98-102.

"New Legislative Framework", European Commission. (https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en, Erişim Tarihi: 22.08.2025)

Papakonstantinou, Vagelis/ De Hert, Paul, "The Regulation of Digital Technologies in the EU: The law-making phenomena of "act-ification", "GDPR mimesis" and "EU law brutality"", Technology and Regulation, 2022, s. 48-60.

Parvanov, Krasen Anatoliev, From Legislation to Practice- a Structured Guide for the EU's Cyber Resilience Act : Utilizing Design Science Research to Bridge Theory and Practice, Yayımlanmamış Yüksek Lisans Tezi, Skövde, 2024.

Pranggono, Bernardi/ Arabo,Abdullahi, "COVID-19 Pandemic Cybersecurity Issues". Internet Technology Letters,2021, Vol.4, No. 2, s.1-6.

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 13 March 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act), Official Journal of the European Union L. (https://data.europa.eu/eli/reg/2024/2847/oj/eng, Erişim Tarihi: 22.08.2025.

Ruohonen, Jukka/ Timmers, Paul, "Vulnerability Coordination Under the Cyber Resilience Act", (https://doi.org/10.48550/arXiv.2412.06261, Erişim Tarihi: 22.08.2025)

Saeed, Saqib/ Altamimi, Salha A./ Alkayyal, Norah A./ Alshehri, Ebtisam/ Alabbad, Dina A., "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations", Sensors, 2023, C. 23, S. 15, s. 6666.

Schoo, Peter. "Navigating the CRA: A Brief Analysis of European Cyber Resilience Act and Resulting Actions for Product Development", Proceedings of the 9th International Conference on Internet of Things, Big Data and Security, 2024, s.245-251.

Schütte, Béatrice, "Product Liability in the Future framework of AI (Technology) Regulation", EU law in the digital age: Swedish Studies in European Law içinde, Hart Publishing, 2025, C. 19, S. 6, s. 85-104.

Shaffique, Mohammed Raiz, "Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark?", Computer Law & Security Review, 2024, C. 54, s. 106009

"Study on the Need of Cybersecurity Requirements for ICT Products", Shaping Europe's Digital Future. (https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products., Erişim Tarihi: 22.08.2025)

Tang, Xunzhu/ Kim, Kisub/ Ezzini, Saad/ Song, Yewei/ Tian, Haoye/ Klein, Jacques/ Bissyande, Tegawende, "Just-in-Time Detection of Silent Security Patches", arXiv preprint arXiv:2312.01241, 2023.

Tartaro, Alessio/ Smith, Adam Leon/ Shaw, Patricia, "Assessing the Impact of Regulations and Standards on Innovation in the Field of AI", SSRN

Electronic Journal, 2023.

Timis, David, "How to regulate AI without stifling innovation", World Economic Forum, 2023. (https://www.weforum.org/stories/2023/06/how-to-regulate-ai-without-stifling-innovation, Erişim Tarihi: 22.08.2025)

Wagner, Gerhard, "Liability Rules for the Digital Age- Aiming for the Brussels Effect", Journal of European Tort Law, 2022, Vol. 13, No. 3, s. 191-243.

1. Finansal Destek Beyanı | Financial Support Statement

Bu çalışma herhangi bir finansal destek almadan gerçekleştirilmiştir. | This research received no financial support.

2. Çıkar Çatışması Beyanı | Conflict of Interest Statement

Yazar, çıkar çatışması bulunmadığını beyan etmektedir. | The author declare no conflict of interest.

3. Etik Kurul Onayı | Ethics Committee Approval

Bu çalışma için etik kurul onayı gerekmemektedir. | Ethics committee approval was not required for this study.

4. Yazar Katkı Beyanı | Author Contributions

Bu makale yazar tarafından tek başına hazırlanmıştır. | This article was solely authored by the writer.

5. Araştırma ve Yayın Etiği Beyanı | Research and Publication Ethics Statement

Yazar, çalışmada akademik etik kurallara uyulduğunu ve herhangi bir etik ihlal bulunmadığını beyan etmektedir. | The author declare that all ethical guidelines for research and publication have been followed and that no violations have occurred.

6. İntihal Taraması ve Hakemlik Süreci | Plagiarism and Peer Review Statement

Makale, intihal programıyla taranmış ve çift kör hakemlik sürecinden geçmiştir. | This article was screened by plagiarism detection software and evaluated through a double-blind peer-review process.