Avrupa Birliği Dijital Düzenlemeleri Etki Analiz Çalışması

Veri Hukuku

Ürün Sorumluluğu Hukuku

Siber Güvenlik Hukuku

Prof. Dr. Mesut Serdar Çekin

Türk-Alman Üniversitesi Hukuk Fakültesi
Medeni Hukuk Anabilim Dalı

Doç. Dr. Mehmet Bedii Kaya

İstanbul Bilgi Üniversitesi Hukuk Fakültesi
Bilişim ve Teknoloji Hukuku Anabilim Dalı

İçindekiler

Giriş

Küreselleşen ve dijital teknolojilerle şekillenen modern dünyada, hukuk düzenleri de giderek daha yoğun bir dönüşüm sürecinden geçmektedir. Bilgi ve iletişim teknolojilerindeki gelişmeler, sadece iş yapma yöntemlerini ve günlük hayatı değil, aynı zamanda düzenleyici çerçeveleri ve devletlerin yasal politikalarını da köklü biçimde etkilemektedir. Avrupa Birliği (AB), bu dönüşüme eşlik etmekle kalmayıp onu yönlendiren aktörlerden biri olarak, veri hukuku, ürün sorumluluğu ve siber güvenlik alanlarında kapsamlı düzenlemeler hazırlamakta ve yürürlüğe koymaktadır. Bu rapor, AB'nin son dönemde hayata geçirdiği veya güncellediği kritik düzenlemeleri ele alarak, bunların Türkiye üzerindeki muhtemel etkilerini detaylı bir bakış açısıyla değerlendirmeyi amaçlamaktadır. Özellikle veri paylaşımı, dijital ürünlerden doğan sorumluluk ve siber güvenlik konuları, hem ekonomik hem de hukuki açıdan kritik bir önem taşımaktadır; zira günümüzde veri, teknolojik inovasyonun en büyük tetikleyicisi hâline gelmiş, siber tehditler ise ulusal ve uluslararası güvenlik meselesi olarak görülmeye başlanmıştır.

Dijital dönüşümün arkasındaki itici güç, genellikle "veri" kavramına dayanmaktadır. Verinin yalnızca korunması ve gizliliğinin sağlanması değil, aynı zamanda ekonomik değerinin açığa çıkarılması ve bu verinin doğru şekilde paylaşılması, modern hukuk politikalarının en önemli gündem maddelerinden biridir. AB, 2016 yılında Genel Veri Koruma Tüzüğü (GDPR) ile kişisel verilerin korunmasında küresel bir "altın standart" belirlemiş, ancak sonraki aşamada yayınladığı "Avrupa Veri Stratejisi Belgesi" ile veri ekonomisinin geliştirilmesi noktasında "paylaşımcı" bir paradigma oluşturmuştur. Bu yeni yaklaşım, Veri Yönetişimi Yasası (Data Governance Act) ve Veri Yasası (Data Act) gibi düzenlemelere zemin hazırlamıştır. Söz konusu yasalar, kişisel olmayan verilerin (örneğin makine verilerin) hangi şartlarda paylaşılabileceğini, hangi yükümlülüklerin üreticiler, veri işleme hizmeti sağlayıcıları ve tüketiciler üzerinde doğacağını ayrıntılı şekilde düzenlemektedir. KOBİ'lerin büyük teknoloji şirketleri karşısında korunması, haksız sözleşme şartlarının bertaraf edilmesi ve veri işleme hizmetleri arasında "geçiş kolaylığı" gibi ilkeler, AB'nin rekabetçi ve açık bir veri pazarı kurma hedefinin yansımasıdır.

Öte yandan, dijitalleşmeyle ivme kazanan bir diğer önemli konu da "ürün sorumluluğu" kavramının yeniden tanımlanmasıdır. Geleneksel mevzuatta fiziki kusurlara veya üretim hatalarına odaklanan ürün sorumluluğu rejimi, bugün bir akıllı ev sistemindeki yazılım açığı, bir otonom araçtaki sensör verisi tutarsızlığı ya da bir endüstriyel robot kolunun güncelleme esnasında hata vermesi gibi karmaşık senaryoları kapsayacak şekilde genişlemeye ihtiyaç duymaktadır. AB, Ürün Sorumluluğu Direktifi'nde yaptığı yeniliklerle yazılımları da "ürün" niteliği taşıyabilecek unsurlar arasında saymakta ve bu tür

dijital unsurlu ürünlerin güvenlik açığı sebebiyle yaşanabilecek zararlarda üretici, dağıtıcı veya ithalatçı gibi tedarik zinciri aktörlerinin sorumluluğunu yeniden çizmektedir. Burada amaç, hem tüketici haklarını çağın gereklerine uygun biçimde korumak hem de teşebbüslere güncel teknoloji koşullarına göre risk yönetimini zorunlu kılmaktır.

Bununla birlikte, dijital dönüşümün belki de en kırılgan ve kritik boyutu "siber güvenlik"tir. İnternet tabanlı hizmetlerin ve IoT cihazlarının sayısı her geçen gün artmakta; bu büyüme, siber saldırılar ve veri ihlalleri gibi riskleri de katlanarak çoğaltmaktadır. Son yıllardaki saldırıların, sadece özel şirketlerin itibarını zedelemek veya bireysel kullanıcıların verilerini sızdırmakla kalmayıp, kritik altyapılardan devlet kurumlarına kadar geniş bir yelpazede yıkıcı sonuçlar doğurabildiği bilinen bir gerçektir. AB, bu riskleri gözeterek siber güvenlik alanında da bir dizi düzenleme ve direktif hazırlamıştır. Öncelikle NIS 1 Direktifi (Ağ ve Bilgi Sistemleri Güvenliği Direktifi), temel hizmet operatörlerinin ve dijital hizmet sağlayıcılarının asgari siber güvenlik standartlarını belirleyerek bir "ilk hat" oluşturmuş; ancak teknolojik tehditlerin giderek çeşitlenmesiyle NIS 2 Direktifi gündeme gelmiştir. NIS 2, kapsamı genişletilmiş ve yükümlülükleri netleştirilmiş bir çerçeve sunmakta, bu sayede enerji, ulaşım, sağlık ve bankacılık gibi kritik sektörlerde yer alan kurumların siber dayanıklılık düzeyini artırmayı hedeflemektedir.

Aynı doğrultuda hazırlanan "Siber Dayanıklılık Yasası" (Cyber Resilience Act – CRA) ise, piyasaya sürülen dijital unsurlu ürünlerin en başından itibaren siber tehditlere karşı korunaklı tasarlanmasını emredici şekilde düzenlemektedir. Akıllı buzdolaplarından endüstriyel IoT sistemlerine, otonom araçlardan robotik tıbbi cihazlara kadar uzanan bu geniş yelpaze, üreticilerin "güvenlik odaklı tasarım" (security by design) ilkelerine uygun hareket etmesini gerektirir. CRA, üretici, ithalatçı ve dağıtıcılar arasında sorumluluk paylaşımını da ayrıntılandırmakta ve güvenlik açığı tespit edildiğinde güncellemelerin veya yamaların sunulmasına kadar uzanan bir süreçte yasal yaptırımlar öngörmektedir. Dijital ekonomi aktörlerini, sadece rekabetin değil, aynı zamanda regülasyonun da gerektirdiği yüksek standartları benimsemeye zorlayan bu düzenleme, AB'nin dijital pazarda sahip olduğu belirleyici rolü bir kez daha öne çıkarmaktadır.

İşbu raporda da Avrupa Birliği nezdinde yaşanan bu gelişmelerin Türk hukukuna etkileri ele alınmaya çalışılmıştır. Zira Türkiye ve AB arasındaki ticari entegrasyon Gümrük Birliği çerçevesinde hâlihazırda ileri bir düzeydedir. Dolayısıyla AB pazarına mal veya dijital hizmet sunan Türk firmalarının, veri koruma, veri paylaşımı, siber güvenlik, ürün güvenliği ve sorumluluğu gibi konularda AB standartlarına uyum sağlaması neredeyse kaçınılmazdır. Aksi halde firmalar, ihracatta zorlanacak, yaptırım ve

cezalarla karşılaşabilecek ya da rekabet dezavantajına maruz kalabilecektir. İkinci olarak, küresel teknoloji trendleri göz önüne alındığında, AB düzenlemelerini yakalamak, Türkiye'nin uluslararası yatırımlar bakımından cazibesini korumasına ve dijital pazarda güvenilir bir aktör olarak konumlanmasına yardımcı olacaktır. Bu bağlamda işbu raporun temel amacı, AB'nin veri hukuku, ürün sorumluluğu ve siber güvenlik alanlarındaki güncel düzenlemelerini etraflıca inceleyerek, Türkiye'ye yönelik potansiyel etkiler ve uyum stratejileri üzerine bir değerlendirme sunmaktır. Bununla birlikte AB düzenlemelerine uyum sağlamanın Türkiye açısından hangi riskleri ve fırsatları barındırdığı da incelenmeye çalışılmıştır. Gerçekten de tam uyum senaryosunda Türkiye'deki teşebbüslerin küresel pazara açılması kolaylaşacak, rekabetçi konumları pekişecektir. Bununla birlikte "aşırı regülasyon" endişesi, özellikle KOBİ'lerin yüksek uyum maliyetleriyle karşılaşma riskini de beraberinde getirebilir. Aynı şekilde, siber güvenlik gibi alanlarda AB ile tam entegrasyon, milli güvenlik ve veri egemenliği politikalarının yeniden şekillenmesini gerektirebilir. Bu nedenle rapor, AB düzenlemelerine kısmi uyum, sektörel uyum gibi farklı senaryoları da masaya yatırmakta; artı ve eksi yönlerini analiz etmektedir.

1. Kısım: Veri Hukuku ve Ürün Sorumluluğu

Giriş

Dijital teknolojilerin hızlı yükselişi, küresel ekonomiyi ve hukuki düzenleri derinden dönüştürürken "veri" kavramı da stratejik bir kaynak hâline gelmiştir. Avrupa Birliği (AB), bu dönüşüme cevap verebilmek adına veri hukuku ve ürün güvenliği alanlarında köklü reformlar gerçekleştirmiştir. Özellikle Veri Yönetişimi Yasası (Data Governance Act), Veri Yasası (Data Act) ve yenilenen Ürün Sorumluluğu düzenlemeleri, AB üyesi olsun olmasın, Birlik ile ticari ilişkileri bulunan tüm ülkeleri yakından ilgilendirmektedir.

Veri hukuku alanında, kişisel verilerin korunmasına dair uzun süredir uygulanan kurallar (GDPR) artık "büyük veri", "yapay zekâ" ve "Nesnelerin İnterneti (IoT)" gibi olgularla genişleyen bir ekosistemin yalnızca bir bölümünü oluşturur hâle gelmiştir. AB, veri ekonomisini büyütebilmek için "Avrupa Veri Stratejisi Belgesi"yle yeni bir vizyon geliştirmiş; bu vizyonu hayata geçiren Veri Yönetişimi Yasası ve Veri Yasası, verilerin hakkaniyetli, güvenli ve şeffaf biçimde paylaşımını kolaylaştırmayı hedeflemiştir. Bu düzenlemeler, bağlantılı cihazların ürettiği verinin kullanıcıya sunulması, veri alıcıları arasında ayrım yapılmaması ve bulut bilişim hizmetlerinde geçiş kolaylığı gibi yenilikçi hükümler içerir. Ayrıca, kişisel verileri koruma yükümlülükleri de tüm bu süreçte geçerliliğini korumaktadır.

Öte yandan, dijitalleşen dünyada "ürün güvenliği ve sorumluluğu" kavramı da yeniden tanımlanma ihtiyacı doğurmuştur. Geleneksel mevzuatta üretim hatası veya fiziksel kusura atfedilen sorumluluk, artık yazılım güncellemeleri, veri temelli hatalar ve otonom sistemlerin sebep olabileceği riskleri de kapsayacak şekilde genişlemektedir. AB, mevcut Ürün Sorumluluğu Direktifi'ni dijital çağın ihtiyaçlarına uyarlayarak, akıllı ürünlerdeki güvenlik açıklarının sorumluluğunu hem üreticiye hem de ilgili hizmet sağlayıcısına yükleyebilecek bir çerçeve oluşturmuştur.

Türkiye bakımından bu gelişmeler, AB pazarına mal veya dijital hizmet sunan şirketlerin uyum maliyetlerini ve hukuki risklerini doğrudan etkilemektedir. Veri Yasası kapsamında, bağlantılı ürün üreten veya yazılım geliştiren işletmeler, kullanıcı verilerine erişim hakkı sağlamak, bu verileri koruyup adil şartlar altında paylaşmak zorundadır. Ürün sorumluluğu cephesinde, yazılımın kusurlu hâle gelmesi veya güncellemeler sonrası yaşanabilecek arızalar, Türk üreticiler açısından ciddi hukuki sonuçlar doğurabilir. Dolayısıyla veri hukuku ve ürün sorumluluğu kısmında yukarıda anılan düzenlemelerin içeriği ve akabinde Türkiye'ye yansımaları ayrıntılı olarak tartışmakta ve uyum stratejilerine ilişkin öneriler sunulmaktadır.

I. Avrupa Birliği Mevzuatına İlişkin Değerlendirmeler

A. Avrupa Birliği Veri Hukuku Temel Çerçevesi

Avrupa Birliği'nin veriye hukuki açıdan yaklaşımı uzun bir geçmişe sahip olmakla birlikte, hukuki düzenlemeler niteliği itibariyle koruyucu nitelikteydi. Zira kişisel verilerin korunmasına yönelik Birlik nezdindeki ilk düzenleme 95/46/EC no.lu Kişisel Verilerin Korunmasına İlişkin Direktif olmuş, bu Direktifi takiben bilhassa elektronik alanda yine kişisel verilerin korunmasına ilişkin düzenlemeler hayata geçirilmiştir.

Veri miktarının artması ile bilişim teknolojilerinde yaşanan gelişmeler ise 2010lardan sonra bilhassa büyük veri (Big Data), makine öğrenmesi ve yapay zekâ teknolojilerinde ciddi gelişmelere sebebiyet vermiş, bu gelişmeleri mümkün kılan etkenlerden birisinin de veri olduğu kabul görmüştür. Şöyle ki büyük veri teknolojilerinde adından da anlaşılacağı üzere çok farklı kaynaklardan elde edilen çok farklı veri tiplerinin birleştirilmesiyle veriye yeni anlamlar katılması, makine öğrenmesi ve yapay zekâ teknolojileri sayesinde veriden daha fazla katma değer elde edilmesi mümkün hale gelmiştir. Bununla birlikte söz konusu verilerin hukuki niteliğine ilişkin tartışmalar da önem kazanmaya başlamış, hukuk düzeninin veriye münhasıran kişilik hakkı ve kişisel verilerin korunması ekseninde yaklaşmasının yetersiz olacağı dile getirilmiştir. Birlik nezdinde meydana gelen bu paradigma değişiminin en önemli

örneği kuşkusuz, otonom araçların ilk olarak geliştirildiği ve piyasaya sürüldüğü dönemlerde bu araçlardan elde edilecek olan veriler üzerindeki hak ile alakalı tartışmaların yaşandığı Almanya'dır. Zira otomotiv sektöründe güçlü olan Alman üreticiler, otonom araçların geliştirilmesi için bir yandan çokça veriye ihtiyaç duymakta, diğer yandan elde edilen verilerin kendi hakimiyetinde kalması, rakipler ve özellikle ABD menşeli teknoloji şirketleri tarafından kullanılmasının önlenmesi doğrultusunda önemli menfaatlere sahiptiler. 2015 yılında Alman asıllı AB Komiseri Günther Oettinger, veri üzerinde münhasırlık sağlayacak olan bir mülkiyet hakkının kabul edilmesine ilişkin öneride bulunmuş[1], 2017 yılında ise dönemin Almanya Şansölyesi Angela Merkel, veri üzerinde mülkiyet hakkı kavramını açıkça zikrederek bu hususun Birlik nezdinde üye ülkeler tarafından tartışılması gerektiğini savunmuştur[2].

Ancak Birlik, öncelikle 1995 yılında yayımlanan kişisel verilerin işlenmesine dair Direktif'i güncellemiş ve 2016 yılında bütün dünya çapında "altın standart" olarak nitelendirilecek olan Genel Veri Koruma Tüzüğü'nü (GVKT) hayata geçirmiştir. Dolayısıyla veriye ilişkin düzenlemelerin odak noktasında öncelikle kişisel veriler ve bunların korunması olmuştur. Bunun sebebi ise özellikle web2 olarak nitelendirilen ve karşılıklı etkileşim unsurları içeren, bununla birlikte verilerin büyük teknoloji şirketlerinin elinde toplanmasını mümkün kılan iş modellerinin yaygınlaşması, bilhassa ABD menşeli büyük sosyal medya şirketlerinin kişisel veri toplayıp bunları çeşitli şekillerde işlemesi, bunlardan gelir elde etmesi ve Birlik ekonomisinin bu gelirlerden herhangi bir pay elde edememesi olarak belirtilebilecektir. Dolayısıyla sosyal medyanın gittikçe etkisini hissettirdiği bir dönemde Birlik kanun koyucusunun kişilik hakları ve kişisel veriler ekseninde düzenlemelere öncelik tanıması doğal bir tepki olarak tanımlanabilecektir. Kaldı ki uzun zamandan beri yürürlükte olan ve güncellenmesi aciliyet teşkil eden bir düzenleme de halihazırda 95/46/EC no.lu Direktif olarak halihazırda mevcuttur.

Bununla birlikte GVKT'nin yürürlüğe girmesinden sonraki dönemde verinin sadece korunması değil, verinin potansiyelinden de istifade edilmesi gerektiği düşüncesi, yukarıda işaret edilen inisiyatifler ışığında kabul görmeye başlamış, bu bağlamda bir başlangıç noktası olarak Avrupa Veri Stratejisi belgesi yayımlanmış, akabinde ise somut düzenlemelere yer verilmiştir. Veriye ilişkin bu paradigma değişimi, verinin ekonomik bir değer olarak açıkça kabul edilmesi ve paylaşımı ile kullanımının teşvik edilmesi zorunluluğunu vurgulamaktadır. Aşağıda öncelikle Avrupa Veri Strateji Belgesi, akabinde ise

[1] Oettinger'in konuşması için bkz.: http://www.compliancedigital.de/.download/123622/zfc_20150202.pdf.

[2] Merkel tarafından kullanılan "Dateneigentum" kavramı için bkz.: https://www.bundesregierung.de/resource/blob/1982118/762794/b667f856d61e481f6dcb6fe517177be7/download-pdf-data.pdf?download=1.

Veri Yasası ve Veri Yönetişimi Yasası ele alınacak, ardından özellikle dijital unsurlar boyutuyla Ürün Sorumluluğu Direktifi ele alınacaktır.

1. Avrupa Veri Stratejisi Belgesi

a. Giriş

Avrupa Birliği'nin veri hukukuna ilişkin düzenlemelerinin temelinde Avrupa Veri Stratejisi belgesi yatmaktadır[3]. Söz konusu strateji belgesi, Birliğin veri hukukuna ilişkin hukuk politikasının temelini teşkil etmekte, bu strateji belgesi çerçevesinde veriye ilişkin farklı düzenlemeler şekillenmektedir. Dolayısıyla Avrupa Birliği'nin veri hukukuna yaklaşımını anlayabilmek, bilhassa bu kapsamda benimsenen hukuk politikalarını kavrayabilmek için öncelikle söz konusu belgenin kısaca incelenmesi gerekecektir.

Strateji belgesinde öncelikle dijital teknolojilerin ekonomi ve toplum açısından dönüştürücü etkisine dikkat çekilmekte, verinin ise bu dönüşümün merkezinde olduğu vurgulanmaktadır. Bu bağlamda örnek olarak kişiselleştirilmiş tıp, yeni mobilite çözümleri ve Avrupa Yeşil Mutabakatı'na katkılar gibi alanlarda veri kullanımının büyük faydalar sağlayacağı ifade edilmektedir. Bununla birlikte veriyi elde etme ve sonrasındaki kullanım süreçlerinde Birlik değerlerine, temel hak ve özgürlükler ile mevcut hukuki düzenlemelere uyumun önemine dikkat çekilmektedir. Nitekim bu unsurlara uyumlu veri elde etme ve işleme süreçleri, vatandaşların da veri paylaşımı noktasında güvenini teşvik edecektir[4].

b. Amaçlar ve Engeller

Bu çerçevede Birlik, verinin kullanımını teşvik etmek suretiyle daha bilinçli kararlar alabilen bir toplum hedefini benimsemektedir. Bunun için verilerin daha geniş kitlelerin erişimine sunulması ve inovasyonun teşvik edilmesi amaçlanmaktadır. Söz konusu belgede belirtildiğine göre verinin güvenli ve şeffaf bir şekilde erişime açılması, paylaşıma konu olması, aynı zamanda Avrupa Birliği'nin veri ekonomisinde lider bir rol oynamasını sağlayacaktır[5].

Strateji belgesi aynı zamanda veri yönetişimi ve paylaşımı noktasındaki engellere de işaret etmektedir. Şöyle ki öncelikle üye devletler arasındaki farklı hukuki düzenlemeler, "ortak" bir Avrupa veri alanının oluşturulmasında büyük bir engel teşkil etmektedir. Dolayısıyla hukuki çerçevenin yeknesaklaştırılması önem kazanmaktadır. Diğer yandan bilhassa yapay zekâ teknolojilerinin gelişimi için çok büyük çapta

[3] From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A European strategy for data, COM(2020) 66, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020DC0066 [Erişim: Ekim 2024].
[4] Veri Stratejisi Belgesi, s. 1-2.
[5] Veri Stratejisi Belgesi, s. 5-6.

veriye ihtiyaç duyulmakta, ancak mevcut durumda yeterli veriye erişilemediği tespit edilmektedir. Pazar içerisindeki dengesizlikler noktasında ise büyük teknoloji firmalarının ellerinde büyük veri setlerini barındırdıkları, bu durumun ise bilhassa KOBİ'ler ve girişim şirketleri açısından rekabet dezavantajı oluşturduğuna işaret edilmektedir. Nihayet ihtiyaç duyulan büyük çapta veri setlerinin farklı kaynaklardan elde edilmesi halinde bunların birleştirilmesi, işlenebilir hale getirilmesi, birlikte işlerlik (interoperability) hususunun dikkate alınması gerektiğine de vurgu yapılmaktadır[6].

c. Strateji ve Eylemler

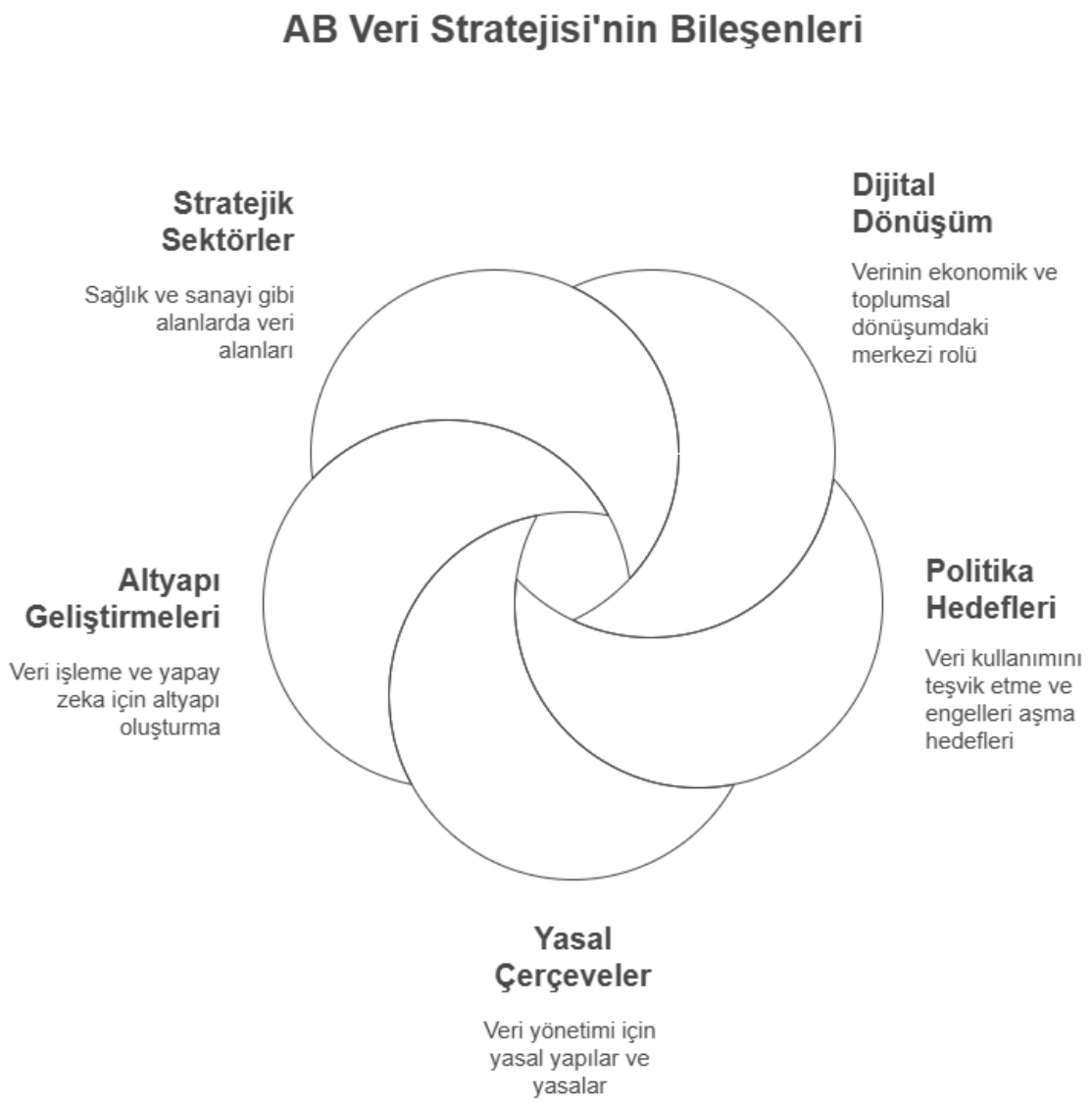
Yukarıda işaret edilen sorunların giderilmesi amacıyla Birlik, belirli alanlarda düzenlemeler yapılması gerektiğine işaret etmektedir.

Bu amaçla öncelikle veri yönetimi için bir yasal çerçevenin oluşturulması amaçlanmaktadır. Buna göre AB genelinde verilerin güvenli ve adil bir şekilde yönetilebilmesi için bir yönetişim yapısı oluşturulması öngörülmektedir. İleride ayrıntılarıyla incelenecek olan Veri Yasası (Data Act), Veri Yönetişimi Yasası (Data Governance Act) gibi düzenlemeler bu amaca hizmet etmektedir[7]. Bir diğer önemli unsur, Veri Yönetişimi Yasası'nın ana unsurlarından birisini oluşturan kamunun uhdesinde bulundurduğu verilerin erişilebilir hale getirilmesi ve bu sayede bilhassa KOBİ'lerin inovasyon alanındaki fırsatlarının güçlendirilmesidir[8]. Yine aynı doğrultuda özel teşebbüsler ile kamu kurumları arasındaki veri paylaşımını teşvik eden düzenlemelerin geliştirilmesi ve kamu yararına veri paylaşımının artırılması için düzenlemeler öngörülmektedir[9]. Nihayet veri paylaşımı ve yapay zekâ ekosisteminin geliştirilmesini destekleyen bir altyapının oluşturulması amacıyla Birlik, 2021-2027 yılları arasında mali açıdan da ciddi bir destek programı sunmayı amaçlamaktadır[10]. Özellikle veri işleme kapasitesinin artırılması ve Avrupa'da güvenli, enerji verimliliği yüksek veri işleme altyapılarının kurulması gerektiği belirtilmekte, bulut bilişim, uç bilişim (edge computing) ve yüksek performanslı bilgisayarlar gibi yeni nesil teknolojilere yatırım yapılması planlanmaktadır[11].

Strateji belgesinin ekinde ayrıca stratejik sektörler ve kamu menfaatinin bulunduğu alanlara ilişkin ortak veri alanları belirlenmektedir. Bu bağlamda sağlık, sanayi ve kamu yönetimi gibi sektörlerde büyük veri

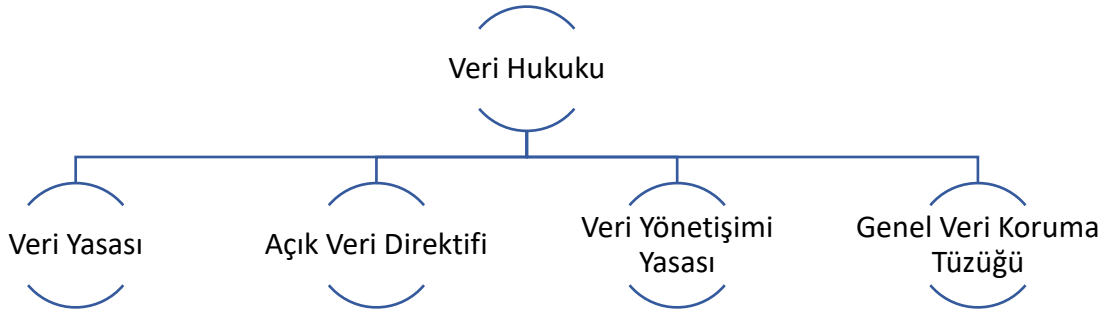
[6] Veri Stratejisi Belgesi, s. 10-12.
[7] Veri Stratejisi Belgesi, s. 14-15.
[8] Veri Stratejisi Belgesi, s. 16-17.
[9] Veri Stratejisi Belgesi, s. 18.
[10] Veri Stratejisi Belgesi, s. 19-20.
[11] Veri Stratejisi Belgesi, s. 21-22.

havuzlarının oluşturulması hedeflenmekte, veri paylaşımı için gereken teknik altyapıların ve yönetim mekanizmalarının geliştirilmesi amaçlanmaktadır[12].



[12] Veri Stratejisi Belgesi, s. 30-31.

2. Veri Düzenlemelerine Genel Bakış



Belirtildiği üzere Avrupa Veri Stratejisi Belgesi kapsamında belirlenen amaçlardan birisi de, veri yönetimi için bir yasal çerçevenin oluşturulmasıdır. Bir diğer ifade ile verinin güvenli ve adil bir şekilde kullanılması, belirli şirketlerin tekelinde toplanmaması, bilhassa KOBİ'lere rekabet avantajı sağlanması gerekçeleriyle hukuki bir altyapının oluşturulması önerilmektedir. Buradan hareketle özellikle Veri Yasası ve Veri Yönetişimi Yasası kapsamında önemli düzenlemeler öngörülmüştür.

Kasım 2020'de sunulan ve Kasım 2021'de kabul edilen Veri Yönetişim Yasası şirketler, bireyler ve kamu sektörü tarafından veri paylaşımını kolaylaştırmak için süreçler ve yapılar oluşturmaktadır. Buna karşılık Veri Yasası, veriden kimin değer yaratabileceğini ve hangi koşullar altında bunu yapabileceğini netleştirmektedir.

Veri Yasası, ekonominin tüm sektörlerinde adil veri erişimini ve kullanımını önemli ölçüde artırmayı amaçlayan yatay bir mevzuattır. Dolayısıyla Veri Yasası, sektörel bir düzenleme niteliğini haiz değildir. Bununla birlikte yasanın yürürlüğe girdiği tarihten önceki yükümlülükler saklı kalmaktadır. Ancak daha da önemlisi, Art. 44 f. 2 doğrultusunda gerekli olduğu durumlarda Veri Yasası'nın sektörel düzenlemeler vesilesiyle somutlaştırılmasına müsaade edilmesidir. Bu bağlamda özellikle pratik ve teknik şartların geliştirilmesi, güvenlik, standartizasyon gibi hususların düzenlenmesi, erişim hakları ve modalitelerine belirli sınırlandırmalar getirilmesi gündeme gelebilecektir.

Genel Veri Koruma Tüzüğü (GVKT) ile Veri Yasası (Data Act) ve Veri Yönetişimi Yasası ilişkisine bakıldığında GVKT'nin tüm kişisel veri işleme faaliyetlerine bütünüyle uygulanacağını belirtmekte fayda vardır. Nitekim Veri Yasası ve Veri Yönetişimi Yasası, kişisel verilerin korunmasını doğrudan düzenlemez. Bilakis Veri Yasasının konusu, veri paylaşımını teşvik etmek ve verilerin değerinin adil bir şekilde dağıtılmasını sağlamak, Veri Yönetişimi Yasasının amacı da şirketler, bireyler ve kamu sektörü tarafından veri paylaşımını kolaylaştırmak için süreçler ve yapılar oluşturmaktadır. Bununla birlikte bazı durumlarda Veri Yasası ve Veri Yönetişimi Yasası, GVKT'yi tamamlayıcı niteliğe bürünmektedir.

Diğer taraftan Avrupa Veri Stratejisi Belgesinin yayımlanma tarihinden önce de yürürlükte olan Açık Veri Direktifi, bilhassa yasalar tarafından korumaya tabi olan verileri düzenlemediği için yetersiz kalmış, bu sebeple Veri Yasası ve Veri Yönetişimi Yasası'nın ihdas edilmesi noktasında bir ihtiyaç meydana gelmiştir.

B. AB Veri Yasası (Data Act)

1. Veri Yasasına Genel Bakış

Veri Yasasının içeriğine bakıldığında birçok farklı hususun düzenlendiğini söylemek mümkündür.

I. Bölüm: Düzenlemenin amacı ve kapsamı, tanımlar.

II. Bölüm - IoT bağlamında işletmeler arası (B2B) ve işletmelerden tüketicilere (B2C) veri paylaşımı. IoT cihazlarının (birlikte) ürettiği verilere erişme, kullanma ve aktarma hakkı.

III. Bölüm - İşletmeler arası veri paylaşımı: Bu bölüm, bir işletmenin başka bir işletme ile veri paylaşmak zorunda kaldığı durumlarda, Veri Yasası dahil olmak üzere, yasal yükümlülükler altındaki veri paylaşımı koşullarını netleştirir.

IV. Bölüm - Haksız sözleşme şartları: Bu hükümler, özellikle küçük ve orta ölçekli işletmeler (KOBİ'ler) olmak üzere tüm işletmeleri, kendilerine dayatılan haksız sözleşme şartlarına karşı korur.

V. Bölüm - İşletmelerden kamu kurumlarına veri paylaşımı: Kamu sektörü, belirli istisnai ihtiyaç durumlarında, özel sektör tarafından tutulan belirli verilere erişim sağlayarak daha isabetli kararlar alabilecektir.

VI. Bölüm - Veri işleme hizmetleri arasında geçiş yapma: Bulut ve uç bilişim hizmeti sağlayıcıları, birlikte çalışabilirliği kolaylaştırmak ve geçişi mümkün kılmak için asgari gereksinimleri karşılamak zorundadır.

VII. Bölüm – **Üçüncü ülke hükümetlerinin hukuka aykırı veri erişimi**: AB'de tutulan kişisel olmayan veriler, yabancı hükümetlerin hukuka aykırı erişim taleplerine karşı korunur.

VIII. Bölüm - Birlikte çalışabilirlik: Veri alanlarına katılanlar, veri alanları içinde ve arasında veri akışını sağlamak için belirli kriterleri yerine getirmelidir.

IX. Bölüm – Uygulama: Üye Devletler, Veri Yasası'nı izlemek ve uygulamak için bir veya daha fazla yetkili makam atamak zorundadır. Birden fazla yetkili makam atanmışsa, ulusal düzeyde tek bir temas noktası olarak hareket edecek bir "veri koordinatörü" atanmalıdır.

Görüldüğü üzere Veri Yasası, birçok farklı hususu düzenlemektedir. Türkiye açısından bakıldığında bu bağlamda özellikle önem arz eden bazı hususları bu aşamada belirlemek ve ilerleyen bölümlerde bu hususları daha etraflıca değerlendirmek önem arz etmektedir.

Bölüm I kapsamında öncelikle Veri Yasası'nın kişi ve yer bakımından uygulama alanına bakılması gerekecektir. Nitekim bu sayede Türkiye'de IoT cihazı ya da bağlantılı bir hizmet sunan üreticinin, Veri Yasasına tabi olup olmayacağı belirlenebilecektir. Üreticinin Veri Yasasına tabi olduğu durumlarda ise bir sonraki aşamada söz konusu Yasa kapsamında öngörülen yükümlülüklerin belirlenmesi gerekmektedir. Zira bu takdirde Türk üretici söz konusu yükümlülükleri yerine getirmediği takdirde belirli yaptırımlara tabi olacaktır. Aynı zamanda Türk mevzuatının da uyumlaştırmaya ihtiyaç duyup duymadığı noktasında söz konusu yükümlülüklerin belirlenmesi önem taşımaktadır. Bu yükümlülükler, Bölüm II, III ve IV çerçevesinde ele alınmaktadır.

Bölüm V, COVİD tecrübesinden hareketle kamu sektörünün istisnai durumlarda özel teşebbüslerden veri talep edebileceğini düzenlemektedir. Bu hüküm, her ne kadar doğrudan Türk üreticileri muhatap almasa da, böyle bir talebin yine de Türk üreticilere de iletilmesi ihtimal dahilindedir. Ayrıca söz konusu hüküm, Türk hukuku açısından da gündeme gelebilecek, bilhassa kamu sektörünün özel teşebbüslerden veri taleplerine ilişkin yasal bir dayanak teşkil edebilecektir.

Bölüm II-IV, daha çok nesnelerin interneti ve bağlantılı hizmetleri esas alırken, veri ekonomisi açısından önem arz eden bir diğer unsur veri hizmetlerine ilişkindir. Bu bağlamda özellikle bulut bilişim hizmetleri sunan aktörlere ilişkin önemli yükümlülükler öngörülmektedir. Türkiye özelinde büyük çapta bulut bilişim hizmeti sunan aktörlerin sayısı çok değildir. Bununla birlikte Türkiye'den Avrupa Birliği'ne veri işleme hizmeti sunulması halinde ilgili hükümler uyarınca birlikte çalışılabilirlik ve diğer şartların yerine getirilmesi gerekmektedir. Ayrıca ilgili düzenleme, Türkiye'de de yaygın olan ve genellikle yabancı menşeli şirketler tarafından sunulan veri işleme hizmetleri açısından bir örnek olarak

değerlendirilebilecektir. Özellikle Bölüm VIII bağlamında birlikte çalışabilirliğe ilişkin hükümler sevk edilmiştir.

Türk kamu sektörü açısından önem arz edebilecek bir diğer husus ise Bölüm VII.'de yer verilen düzenlemelere ilişkindir. Şöyle ki Birlik dışındaki ülkelerin kamu otoritelerinin kişisel olmayan verilere erişim taleplerine ilişkin belirli şartlar getirilmektedir. Dolayısıyla Türk makamlarının Birlik içerisinde kişisel veri talepleri GVKT, kişisel olmayan verilere ilişkin talepleri ise Veri Yasası'na göre değerlendirilecektir. Bu şartların karşılanmaması halinde verinin Türk makamlarına aktarılması da mümkün olmayacaktır.

Son olarak Veri Yasası'na tabi olan Türk şirketlerinin muhatap olabileceği muhtemel yaptırımların da belirtilmesi amacıyla son bölümde yer alan düzenlemeler de önem arz etmektedir.

2. Veri Yasası'nın Uygulama Alanı

a. Konu Bakımından Uygulama Alanı

Veri Yasası Art. 1 f. 1'e göre konu bakımından uygulama alanı, farklı senaryoları kapsamaktadır.

Öncelikle bağlantılı ürün ve bağlantılı hizmetler esas alınmaktadır. Birlik içerisinde bağlantılı bir ürün veya ilgili hizmetin kullanıcılarının, bu bağlantılı ürün veya hizmetin kullanımıyla oluşturulan verilere zamanında erişebilmesini ve bu verileri, istedikleri üçüncü taraflarla paylaşmak da dahil olmak üzere, kullanabilmeleri amaçlanmaktadır. Bu bağlamda Tüzük, söz konusu verilerin belirli durumlarda kullanıcılara ve kullanıcının seçtiği üçüncü taraflara sunulmasını sağlama yükümlülüğünü veri sahiplerine yüklemektedir.

Tüzük ayrıca veri sahiplerinin, Tüzük konusu verileri Birlik içindeki veri alıcılarına adil, makul ve ayrım gözetmeyen şartlar altında ve şeffaf bir şekilde sunmalarını öngörmektedir.

Tüzük'ün konu bakımından uygulama alanına giren bir diğer husus, veri sahiplerinin, kamu sektörü kuruluşlarına, Komisyona, Avrupa Merkez Bankası'na veya Birlik kuruluşlarına, kamu yararına gerçekleştirilen belirli bir görevin yerine getirilmesi için gerekli verileri, istisnai bir ihtiyaç durumunda sunmalarını güvence almaktır.

Nihayet Tüzük, veri işleme hizmetleri arasında geçişi kolaylaştırmayı ve Birlik içindeki verilerin ve veri paylaşım mekanizmalarının ve hizmetlerinin birlikte çalışabilirliğini artırmayı hedeflemektedir.

Ardından Tüzük Art. 1 f. 2 çerçevesinde hangi bölümde hangi verilerin esas alındığına ilişkin açıklamalar yer almaktadır.

b. Kişi ve Yer Bakımından Uygulama Alanı

Tüzük'ün kişi ve yer bakımından uygulama alanı, Tüzük Art. 1 f. 3'te düzenlenmektedir. Hemen belirtelim ki kişi ve yer bakımından uygulama alanı birbiriyle doğrudan bağlantılı hususlardır. Şöyle ki;

- Birlik sınırları içerisinde piyasaya sürülen bağlantılı ürünlerin üreticileri (kuruluş yeri ne olursa olsun) (a bendi)
- Birlik sınırları içerisinde bağlantılı hizmet sağlayıcıları (kuruluş yeri ne olursa olsun) (a bendi)
- Birlik sınırları içerisinde bağlantılı ürün veya ilgili hizmetlerin kullanıcıları (b bendi)
- Verileri Birlik sınırları içerisinde veri alıcılarına sunan veri sahipleri (kuruluş yeri ne olursa olsun) (c bendi)
- Verilerin sunulduğu Birlik sınırları içerisindeki veri alıcıları (d bendi)
- Kamu sektörü kuruluşları, Komisyon, Avrupa Merkez Bankası ve veri sahiplerinden, kamu yararına gerçekleştirilen belirli bir görevin yerine getirilmesi için bu verilere olağanüstü bir ihtiyaç olduğunda verilerin sunulmasını talep eden Birlik kuruluşları ile bu talebe yanıt olarak verileri sağlayan veri sahipleri (e bendi)
- Birlik sınırları içerisinde müşterilerine hizmet sunan veri işleme hizmeti sağlayıcıları (kuruluş yeri ne olursa olsun) (f bendi)
- Veri alanlarına katılımcılar ve akıllı sözleşmeleri kullanan uygulama sağlayıcıları ile bir anlaşmanın ifası bağlamında başkaları adına akıllı sözleşmelerin uygulanmasıyla uğraşan kişiler, ticaret veya meslek sahipleri (g bendi),

Tüzük hükümlerine tabi kılınmaktadır. Burada esasında rekabet hukukundan gelen, fakat dijital regülasyonlarda da geniş uygulama alanı bulan Pazar ilkesinin benimsendiğini söylemek mümkündür. Bu ilkeye göre Birlik pazarını hedefleyen kişiler, bu pazarın kurallarına da riayet etmekle yükümlü kılınmaktadır.

Bununla birlikte ilgili hükmün daha iyi anlaşılabilmesi adına veri sahibi, veri alıcısı, bağlantılı ürün, bağlantılı hizmet gibi bazı kavramların açıklığa kavuşturulması gerekecektir.

aa. Bağlantılı Ürün

Madde 2(5)'e göre, bağlantılı bir ürün, "*kullanımı veya çevresiyle ilgili verileri elde eden, üreten veya toplayan ve ürün verilerini elektronik haberleşme hizmeti, fiziksel bağlantı veya cihaz üzerinde erişim yoluyla iletebilen ve birincil işlevi, kullanıcı dışındaki herhangi bir taraf adına veri depolamak, işlemek*

veya iletmek olmayan bir öğe" olarak tanımlanmaktadır. Bu tanım, esas olarak Nesnelerin İnterneti (IoT) ürünlerine atıfta bulunmaktadır. Dibace No. 14. bu konuyu şu şekilde açıklamaktadır:

"Performansları, kullanımları veya çevreleriyle ilgili verileri bileşenleri veya işletim sistemleri aracılığıyla elde eden, üreten veya toplayan ve bu verileri elektronik haberleşme hizmeti, fiziksel bir bağlantı veya cihaz üzerinde erişim yoluyla iletebilen bağlantılı ürünler, sıklıkla Nesnelerin İnterneti olarak adlandırılan ürünler, prototipler hariç olmak üzere bu Tüzüğün kapsamına girmelidir. **Bağlantılı ürünler, özel, sivil veya ticari altyapı, bağlantılı araçlar, sağlık ve yaşam tarzı ekipmanları, gemiler, uçaklar, ev ekipmanları ve tüketim malları, tıbbi ve sağlık cihazları veya tarım ve sanayi makineleri dahil olmak üzere ekonominin ve toplumun tüm alanlarında bulunmaktadır**."

Bununla birlikte Dibace No. 16 bu tanıma bazı sınırlamalar getirmektedir:

"Bir yandan, sensör donanımlı bu tür bağlantılı ürünlerin ve ilgili hizmetlerin sağlanması için olan pazarlar ile diğer yandan, genellikle fikri mülkiyet haklarıyla korunan metinsel, sesli veya görsel-işitsel içerik gibi bağlantısız yazılım ve içeriklerin sağlandığı pazarlar arasında ayrım yapmak önemlidir. Sonuç olarak, **kullanıcının içerik kaydettiği, ilettiği, görüntülediği veya oynattığı sensör donanımlı bağlantılı ürünlerin ürettiği veriler ve genellikle fikri mülkiyet haklarıyla korunan bu içeriklerin kendisi, bu Tüzüğün kapsamına girmemelidir**. Bu Tüzük ayrıca, bağlantılı ürünlerden elde edilen, üretilen veya erişilen ya da başka taraflar, özellikle kullanıcı olmayanlar adına depolama veya diğer işlem operasyonları için iletilen verileri de kapsamamalıdır. Bu durum özellikle sunucular veya tamamen üçüncü taraflar adına kullanılan bulut altyapılarıyla ilgili olarak, bilhassa çevrimiçi bir hizmet tarafından kullanıldığı durumlarda söz konusu olacaktır."

bb. Bağlantılı Hizmet

Madde 2(3)'e göre, bağlantılı hizmet, "*bir elektronik haberleşme hizmeti dışında, satın alma, kiralama veya leasing sırasında ürünle bağlantılı olan ve yokluğu durumunda bağlantılı ürünün bir veya daha fazla işlevini yerine getirmesini engelleyecek şekilde ürünle bağlantılı olan, yazılım da dahil olmak üzere her türlü dijital hizmet, ya da ürünün temin edilmesinden sonra üretici ya da üçüncü bir tarafça bağlantılı ürünün işlevlerini artırmak, güncellemek veya uyarlamak amacıyla ürüne bağlanan hizmet*" olarak tanımlanmaktadır. Komisyon, bağlantılı hizmete örnek olarak bir kullanıcının satın aldığı çamaşır makinesini vermektedir. Kullanıcı, bu makinenin içindeki farklı sensörlerden gelen verilere dayanarak çamaşır döngüsünün çevresel etkisini ölçmelerini sağlayan ve döngüyü buna göre ayarlayan

bir uygulama yükler. Bu uygulama, ilgili bir hizmet olarak kabul edilir[13]. Benzer şekilde robot süpürgenin bir uygulama vesilesiyle evin krokisini çıkartması, bu kroki dahilinde evi süpürmesi durumunda da sensörler vasıtasıyla elde edilen veriler, kullanıcının telefonuna indirdiği bir uygulama vesilesiyle üreticiye aktarılmaktadır. Bu durumda da bağlantılı bir hizmetten bahis açılabilecektir.

cc. Veri Sahibi ve Veri Alıcısı

Veri sahibi ise Madde 2 (13)'e göre "Tüzük, yürürlükteki Birlik hukuku veya Birlik hukukunu uygulamaya yönelik ulusal mevzuat uyarınca verileri – sözleşmede kararlaştırıldığı takdirde, ürün verileri veya ilgili hizmet verileri de dahil olmak üzere – kullanma ve sağlama yetkisine veya yükümlülüğüne sahip olan ve bir bağlı hizmetin sağlanması sırasında bu verileri elde eden veya üreten gerçek veya tüzel kişi" olarak tanımlanmaktadır. Bu bağlamda veri alıcısı ise Madde 2 (14)'e göre " ticari, iş, zanaat veya mesleki faaliyeti kapsamında hareket eden, ancak bağlantılı bir ürün veya bağlı hizmetin kullanıcısı olmayan ve veri sahibinden veri alan gerçek veya tüzel kişiyi ifade eder. Buna, veri sahibinin kullanıcının talebi üzerine veya başka bir Birlik hukuku ya da Birlik hukukuna uygun olarak çıkarılan ulusal mevzuat uyarınca hukuki bir yükümlülüğe dayanarak veri sağladığı üçüncü bir taraf da dahildir".

Bu tanımlardan hareketle, Türk üreticilerin

- **Birlik sınırları içerisinde bağlantılı ürünleri piyasaya sürmesi;**
- **Birlik sınırları içerisinde bağlantılı hizmet sunması;**
- **Veri sahibi sıfatıyla Birlik sınırları içerisindeki veri alıcılarına Tüzük'e konu verileri sunması;**
- **Birlik içerisinde veri işleme hizmeti sunması**;

hallerinde Veri Yasası hükümlerine riayet etmeleri gerekecektir.

3. Bağlantılı Ürün ve Bağlantılı Hizmetlere İlişkin Düzenlemeler

Veri Yasasının ikinci bölümünde "B2B ve B2C İlişkilerinde Veri Paylaşımı" konusu düzenlenmektedir. İlgili bölüm özellikle kimlerin hangi şartlar altında hangi verileri paylaşmakla yükümlü olacaklarına ilişkin detaylı düzenlemeler içermektedir. Bununla birlikte hemen belirtelim ki Veri Yasası Art. 2 f. 1/a hükmüne göre Bölüm II çerçevesinde düzenlenen yükümlülükler, bağlantılı ürünler ve hizmetler

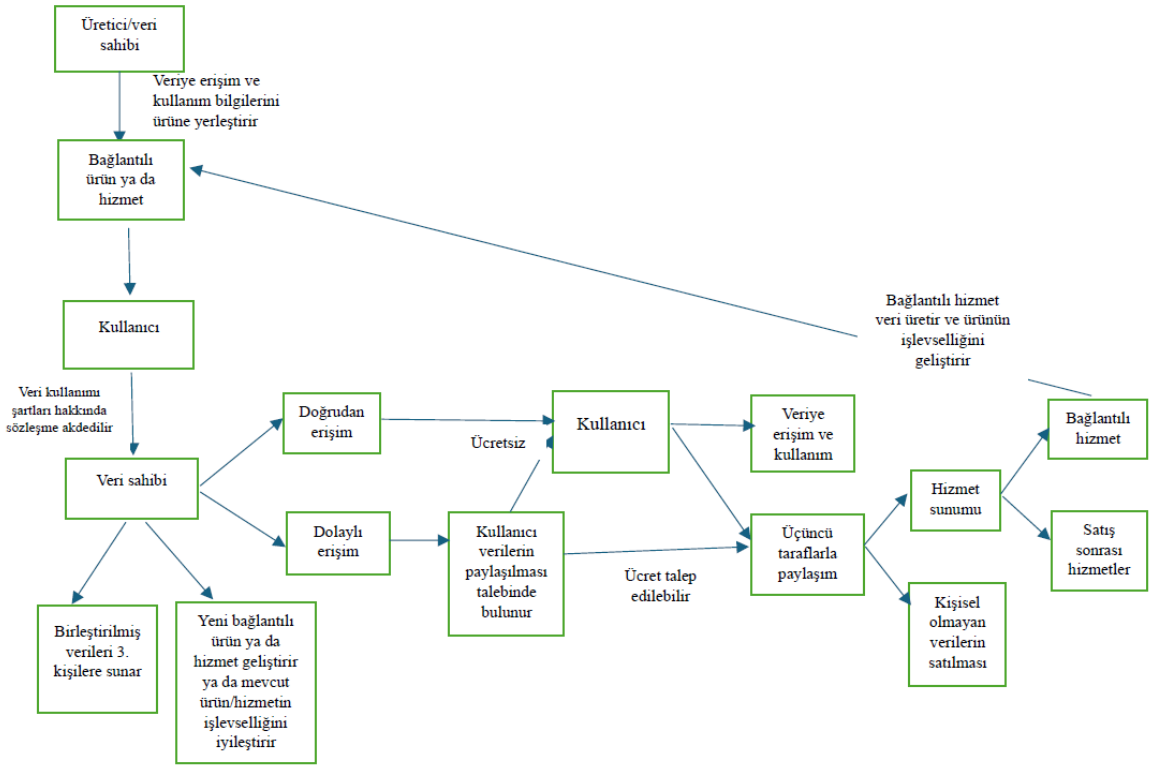
[13] EC, Data Act Explained, s. 2, https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained.

kapsamında elde edilen bütün verileri kapsamamakta, özellikle ürün ya da hizmetin performansı, kullanımı ve çevresiyle ilgili verileri kapsam dışı bırakmaktadır.

a. Düzenlemenin Kapsamı: KOBİ İstisnaları, Hükümlerin Emredici Niteliği

Veri paylaşımına ilişkin yükümlülükler, muhataplar açısından operasyonel, teknik ve mali açıdan birçok külfeti de beraberinde getirmektedir. Veri Yasasının amaçlarından birisi de veri pazarlarındaki rekabet ortamının güçlendirilmesi olduğu için söz konusu yükümlülüklerin bilhassa KOBİ'ler açısından uygulanması, KOBİ'ler açısından birçok zorluğu beraberinde getirecektir. Buradan hareketle Tüzük, Art. 7 f. 1 hükmü uyarınca küçük ve mikro ölçekli işletmelere ikinci bölümde düzenlenen yükümlülüklerin uygulanmayacağını belirtmekte, aynı şekilde orta ölçekli işletmelerin de bu statülerini bir yıldan fazla bir süre muhafaza etmedikleri takdirde kapsam dışı olacaklarını düzenlemektedir.

Art. 7 f. 2 hükmü ise düzenlemelerin emredici niteliğine vurgu yapmakta, bu sayede özellikle iktisadi açıdan daha güçlü konumda olan teşebbüslerin akdedilmesi öngörülen sözleşme hükümlerinde kendi lehlerine hükümler diretmesini engellemektedir.



Bkz. European Commission, Frequently Asked Questions, Data Act, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act, s. 6.

b. Ürün ya da Hizmetin Tasarımı: Accessibility by Design: Art. 3/1; Erişimin Konusu Olan Veriler

Tüzük, öncelikle ürün ya da hizmetin tasarımı aşamasına ilişkin bir düzenleme öngörmektedir. Art. 3 f. 1'e göre "*bağlantılı ürünler ve bağlantılı hizmetler, ürün ve hizmet verilerinin – bu verilerin yorumlanması ve kullanılması için gerekli olan ilgili meta veriler de dahil olmak üzere – kullanıcı için standart olarak kolay, güvenli, ücretsiz, kapsamlı, yapılandırılmış, yaygın ve makine tarafından okunabilir bir formatta ve uygun olduğu ve teknik olarak mümkün olduğu ölçüde doğrudan erişilebilir olacak şekilde tasarlanır ve üretilir*". Art. 1 f. 4'e göre sanal asistanlar da, bağlantılı ürün ya da bağlantılı hizmetle etkileşim halinde olduğu takdirde bu tanıma dahil edilmektedir. Ancak hükümden bu yükümlülüğün muhatabını anlamak mümkün değildir. Bunula birlikte ürünün tasarımı esnasında söz konusu tasarıma müdahale edebilecek kişiler üreticiler ve hizmetin tasarımı noktasında da sağlayıcılar olduğu için söz konusu yükümlülüğün muhataplarının da üretici ve sağlayıcılar olduğunu kabul etmek gerekmektedir[14]. Buna karşılık satıcı ya da kiraya verenlerin yükümlülük altında olduğunu söylemek imkân dahilinde gözükmemektedir.

Erişimin konusu olan veri ise bağlantılı ürün verisi, bağlantılı hizmet verisi ve gerekli olduğu takdirde meta verilerdir. Genel olarak veri, Art. 2 No. 1'e göre veri, "*ses, görüntü veya görsel-işitsel materyal şeklinde de olmak üzere eylemlerin, olguların veya bilgilerin her türlü dijital temsili ile bu eylemlerin, olguların veya bilgilerin herhangi bir şekilde derlemesi*" olarak tanımlanmaktadır. Dolayısıyla kural olarak veriden kasıt "ham veri" olacaktır. Meta veriler ise verilerin içeriği veya kullanımına ilişkin yapılandırılmış bir tanım olup, bu verilerin bulunmasını veya kullanılmasını kolaylaştırmaktadır (Art. 2 No. 2). Ürün verileri ise Art. 2 No. 15'e göre "*bir bağlantılı ürünün kullanımıyla üretilen ve üretici tarafından bir elektronik haberleşme hizmeti, fiziksel bir bağlantı veya cihaz içi erişim yoluyla bir kullanıcı, veri sahibi veya üçüncü taraf (gerekirse üretici dahil) tarafından elde edilebilecek şekilde tasarlanan veriler*" olarak tanımlanmaktadır. Nihayet Art. 2 No. 16'ya göre ilgili hizmet verileri, "*bağlantılı ürünle ilgili olarak kullanıcının eylemlerinin veya işlemlerinin dijitalleştirilmiş temsili olup, kullanıcı tarafından kasıtlı olarak kaydedilen ya da bir bağlı hizmetin sağlayıcı tarafından sunulması sırasında kullanıcının eylemlerinin yan ürünü olarak üretilen verilerdir*". Bu bağlamda Dibace No. 15'e göre şu örnekler verilmektedir:

(1) bilinçli olarak kaydedilen ya da kullanıcının eylemi sonucu dolaylı olarak oluşan veriler;

[14] Hennemann/Ebner/Karsten/Lienemann/Wienroeder, Data Act – An Introduction, 2024, s. 53.

(2) bağlı ürünün çevresi veya etkileşimlerine ilişkin veriler

(3) kullanıcı arayüzü veya ilgili bir hizmet aracılığıyla üretilen bağlı ürün kullanımına ilişkin veriler, (örnek olarak sensörler tarafından otomatik olarak üretilen veriler ve gömülü uygulamalar tarafından kaydedilen veriler, donanım durumu ve arızaları gösteren uygulamalar)

(4) kullanıcının hareketsiz olduğu zamanlarda, örneğin ürün bekleme modundayken veya kapalıyken bağlı ürün veya ilgili hizmet tarafından üretilen veriler

(5) önemli ölçüde değiştirilmemiş veriler, (ham veri)

(6) sonraki işleme ve analizden önce verilerin anlaşılır ve kullanılabilir hale getirilmesi amacıyla önceden işlenmiş veriler.

Tartışmalı olan bir husus, ürün ya da hizmet verilerinden türetilen veri ve bilgilerin de erişime konu olup olmayacağına ilişkindi. Ancak Dibace No. 15'e göre bunların kapsam dışı olduğunu söylemek mümkün olacaktır[15].

Erişim modalitesi noktasında ise Art. 3 f. 1'de öngörülen erişim imkânı, herhangi bir değerlendirmeye tabi olmaksızın kullanıcıya doğrudan ilgili verilere erişim imkânı sağlamaktan ibarettir. Birden fazla kullanıcının olduğu durumlarda ise üreticiden birden fazla veri hesabı tutması ve bu verileri ayrıştırarak ilgili kullanıcıya sunabilmesi beklenmektedir[16].

c. Bilgilendirme Yükümlülüğü:

Kullanıcının erişim hakkını nasıl ve ne şekilde kullanacağı noktasında ise Tüzük, Art. 3 f. 2 ve f. 3 hükümlerinde bağlantılı ürün ve bağlantılı hizmetlere ilişkin bilgilendirme yükümlülükleri öngörmektedir. Buna göre bağlantılı ürün ya da bağlantılı hizmeti satış, kira ya da leasing sözleşmesine dayalı olarak sunan kişiler, kullanıcıyı bilgilendirmekle yükümlü kılınmıştır. Bu bağlamda f. 2, bağlantılı ürünlere ilişkin bilgilendirme yükümlülüğünü ele alırken f. 3 kapsamında bağlantılı hizmetlere ilişkin bilgilendirme yükümlülüğünün içeriği düzenlenmiştir.

Satıcı, kiraya veren ya da leasing veren, bağlantılı ürüne ilişkin asgari olarak aşağıdaki hususlara ilişkin kullanıcıyı bilgilendirmelidir:

[15] Buna karşılık, bu tür verilerden çıkarılan veya türetilen bilgiler, özellikle özel ve karmaşık algoritmalar, bunlara dahil olan özel yazılımlar yoluyla elde edilen veriler veya içgörüler, bu Tüzüğün kapsamına girmemeli ve dolayısıyla aksi kullanıcı ile veri sahibi arasında kararlaştırılmadıkça veri sahibinin bu bilgileri bir kullanıcıya veya veri alıcısına sunma yükümlülüğüne tabi olmamalıdır.
[16] Bkz. Veri Yasası Dibace No. 21.

a) Bağlı ürünün üretebileceği veri türü, formatı ve tahmini kapsamı;

b) Bağlı ürünün sürekli ve gerçek zamanlı olarak veri üretme yeteneğine sahip olup olmadığına dair bilgi;

c) Saklama süresi de dahil olmak üzere bağlı ürünün verileri bir cihazda veya uzaktaki bir sunucuda depolama yeteneğine sahip olup olmadığına dair bilgi;

d) Kullanıcının verilere nasıl erişebileceği, verileri nasıl elde edebileceği veya gerekirse silebileceği, buna ilişkin teknik yöntemler, kullanım koşulları ve hizmet kalitesi hakkında bilgi.

İlaveten bağlantılı hizmetin sunulması halinde Art. 3 f. 3'e göre hizmeti sunan tarafından asgari olarak aşağıdaki bilgilerin sunulması gerekmektedir:

a) Potansiyel veri sahibinin elde etmesi muhtemel ürün verilerinin türü, tahmini kapsamı ve toplanma sıklığı, mümkün olduğu takdirde kullanıcının bu verilere nasıl erişebileceği ya da bu verileri nasıl elde edeceğine dair koşullar, ayrıca potansiyel veri sahibinin verilerin depolanmasına ve saklama süresine ilişkin düzenlemeleri;

b) Üretilecek bağlantılı hizmet verilerinin türü ve tahmini kapsamı, kullanıcının bu verilere nasıl erişebileceği ya da bu verileri nasıl elde edebileceğine dair koşullar, potansiyel veri sahibinin verilerin depolanmasına ve saklama süresine ilişkin düzenlemeleri;

c) Potansiyel veri sahibinin kolayca erişilebilir verileri kendisinin kullanmayı planlayıp planlamadığı, bu verilerin hangi amaçlarla kullanılacağı ve bu verileri kullanıcıyla kararlaştırılan amaçlar doğrultusunda bir veya birden fazla üçüncü tarafın kullanımına izin vermeyi planladığına dair bilgi;

d) Potansiyel veri sahibinin kimliği, örneğin ticari adı ve yerleşik olduğu adres, varsa diğer veri işleme taraflarının kimliği;

e) Potansiyel veri sahibiyle hızlı ve etkili bir şekilde iletişim kurulabilecek iletişim araçları;

f) Kullanıcının verilerin bir üçüncü tarafa aktarılmasını nasıl talep edebileceği ve bu veri aktarımını nasıl sonlandırabileceğine dair bilgi;

g) Kullanıcının, bu bölümdeki herhangi bir hükmün ihlal edilmesi durumunda, 37. maddede belirtilen yetkili makama şikâyette bulunma hakkı;

h) Potansiyel veri sahibinin, bağlı ürün üzerinden erişilen veya bir bağlantılı hizmet sağlanırken üretilen verilere dahil olan ticari sırların sahibi olup olmadığı ve potansiyel veri sahibi ticari sırların sahibi değilse, ticari sırların sahibinin kimliği;

i) Kullanıcı ile potansiyel veri sahibi arasındaki sözleşmenin süresi ve böyle bir sözleşmenin erken feshi durumunda nasıl bir düzenlemenin yapılacağı.

Bu bağlamda dikkat edilmesi gereken husus, söz konusu bilgilerin satıcı ya da kiraya veren/leasing veren tarafından sunulamamasına ilişkindir. Zira bu bilgilerin aslında doğrudan üretici ya da hizmet sağlayıcı tarafından sunulabilmesi mümkündür. Bununla birlikte kullanıcı sıfatıyla ürün ya da hizmeti satın alan ya da kiralayan, çoğu zaman doğrudan üreticiyle değil, üreticinin tedarik zinciri içerisinde bulunan acente ya da tek satıcıyla ya da hatta perakende sektöründe faaliyet gösteren satıcıyla muhatap olacaktır. Dolayısıyla bağlantılı ürün üreticisi ya da bağlantılı hizmet sunucusunun kendi tedarik zinciri bünyesinde söz konusu aydınlatma/bilgilendirme yükümlülüğünün yerine getirilebilmesi amacıyla gerekli önlemleri almış olması gerekecektir.

Bilgilendirmenin ürünün ya da hizmetin tedarik edildiği esnada sunulması gerekmekle birlikte, kullanıcının bu bilgiyi gerçekten de okuduğu ve anladığını ispat etmek gibi bir yükümlülük söz konusu değildir. Bilginin sunulmuş olması yeterlidir. Bilginin nasıl sunulacağı noktasında Dibace No. 24'e göre stabil bir URL'ye işaret edilmesi, bu URL'ye doğrudan bağlantı imkânı sunan bir karekodun kullanıcıya sunulması gibi yöntemler yeterli görülmektedir[17]. Yine bu bağlamda veri koruma hukuku ya da tüketici hukukunda mevcut olan bilgilendirme/aydınlatma yükümlülüğüne ilişkin yöntemler de söz konusu olabilecektir. Bununla birlikte söz konusu bilginin muhafaza edilebilir bir şekilde kullanıcıya sunulması gerekmekte, ayrıca bilginin içeriğinde değişiklik meydana gelmesi halinde gerekli güncellemelere ilişkin kullanıcıyı da bilgilendirmek gerekecektir.

ç. Ürün ve Bağlantılı Hizmet Verilerine Erişim Bağlamında Kullanıcı ve Veri Sahiplerinin Verilere Erişim, Verilerin Sunulması ve Kullanımı Bağlamında Hak ve Yükümlülükleri (Art. 4)

Veri Yasası Art. 3'e göre bağlantılı ürün ya da bağlantılı hizmet, kural olarak kullanıcıya doğrudan erişim imkânı sunacak şekilde tasarlanacaktır. Ancak söz konusu tasarım mutlak surette uyulması gereken bir yükümlülük olmayıp ancak "uygun ve teknik açıdan mümkün olduğu takdirde" gündeme gelecektir. Tasarım itibariyle ürün ya da bağlantılı hizmetin doğrudan erişim imkânı sunamaması halinde ise kullanıcının talebi üzerine kullanıcıya erişim imkânı sunulmalıdır. Art. 4 hükmünde ürün

[17] Hennemann/Ebner/Karsten/Lienemann/Wienroeder, Data Act – An Introduction, 2024, s. 60.

verileri ile bağlantılı hizmet verilerinin kullanıcıya sunulması yükümlülüğünün içeriği düzenlenmektedir. Buna göre ilgili hüküm kullanıcıya ürün ya da bağlantılı hizmet verilerine erişim hakkı tanımakta, söz konusu verinin üçüncü kişilerle paylaşılmasını talep etme yetkisi öngörmekte, aynı zamanda veri sahipleri ve veri alıcıları açısından verinin (ikincil amaçlarla) kullanımına dair sınırlamalar getirmektedir.

aa. Kullanıcı Tanımı

Öncelikle kullanıcı, Art. 2 No. 12'de yer verilen tanıma göre "*Bağlantılı bir ürüne sahip olan veya bağlantılı ürünü kullanmak için sözleşme yoluyla geçici haklar devredilmiş olan ya da bağlantılı hizmetleri kullanan gerçek veya tüzel kişi"* olarak tanımlanmaktadır. Bu tanım, Dibace No. 18'de şu şekilde açıklanmaktadır: *"Bir ürünün kullanıcısı, işletme veya tüketici gibi bir tüzel ya da gerçek kişi olarak, ya da kamu sektörü kuruluşları da dahil olmak üzere, ya bağlantılı bir ürünün sahibi olan, ya da kira veya leasing sözleşmesi kapsamında bağlantılı üründen elde edilen verilere erişim veya kullanma hakkı elde eden bir kişi olarak anlaşılmalıdır. Ayrıca, bu kişiler bağlantılı ürüne ilişkin hizmetleri de alabilirler. Bu erişim hakları, bağlantılı ürünü veya ilgili hizmeti kullanarak etkileşimde bulunan veri sahiplerinin, bağlantılı ürün tarafından üretilen kişisel verilere ilişkin haklarını hiçbir şekilde değiştirmemeli veya bu haklara müdahale etmemelidir. Bu tür bir kullanıcı, bağlantılı ürünü kullanmanın risklerini üstlenir ve faydalarını elde eder ve aynı zamanda ürünün ürettiği verilere erişim hakkına sahip olmalıdır. Bu nedenle, kullanıcı, o ürün tarafından üretilen verilerden ve ilgili hizmetlerden fayda elde etme hakkına sahip olmalıdır. Bir malik, kiracı veya leasing alan kişi de kullanıcı olarak kabul edilmelidir; bu, birden fazla kişi kullanıcı olarak kabul edilebildiğinde de geçerlidir. Birden fazla kullanıcı bağlamında, her kullanıcı veri üretimine farklı şekillerde katkıda bulunabilir ve veri kullanımının farklı biçimlerinde menfaat sahibi olabilir, örneğin, bir kiralama şirketi için filo yönetimi veya araç paylaşım hizmetini kullanan bireyler için hareketlilik çözümleri gibi*". Dolayısıyla burada hukuki statüden çok menfaat-külfet ilkesinden hareketle kullanıcı terimi tanımlanmaktadır. Öte yandan yukarıda yapılan açıklamalardan çıkartılacak önemli bir sonuç, veri sahibinin her bir kullanıcı özelinde kimin hangi veriyi ürettiğine ilişkin ayrım yapması ve talepte bulunan kişiye onun ürettiği veriyi sunmasıdır. Bir diğer ifade ile bir ürünün birden fazla kullanıcısı olduğu takdirde hangi kullanıcının hangi veriyi ürettiğinin tespit edilebilmesi ve doğru kişiye doğru verinin sunulabilmesi için gerekli operasyonel ve teknik altyapının da kurgulanması gerekecektir.

bb. Veri Lisansı Sözleşmesi

Veri Yasasının en önemli yeniliklerinden birisi kuşkusuz veri lisansı sözleşmesine ilişkindir. Şöyle ki bağlantılı ürün ya da hizmetten elde edilen ve kişisel veri niteliğini haiz olmayan veriler, Art. 4 f. 13 c. 1 hükmüne göre bundan sonra ancak veri lisansı sözleşmesine dayalı olarak veri sahipleri tarafından kullanılabilecektir[18].

Öncelikle veri lisansına konu olan veri, Art. 2 No. 17 kapsamında tanımlanan kolayca erişilebilen verilerdir. Bunlar, "*basit bir işleme faaliyetinden öteye geçen, veri sahibinin bağlantılı üründen veya ilgili hizmetten yasal olarak, orantısız bir çaba harcamadan elde ettiği veya elde edebileceği ürün verileri ve ilgili hizmet verileri*" olarak tanımlanmaktadır. Sözleşmenin kurulması ve geçerliliğine ilişkin hususlar ise üye ülke hukukuna göre belirlenecektir. Söz konusu sözleşme, veriler elde edilmeden evvel akdedilmelidir. Bu bağlamda yine veri sahibinin tedarik zincirini organize etmesi gerekecektir.

Bununla birlikte verilerin kullanımı noktasında c. 2'ye göre önemli bir kısıtlama öngörülmektedir. Nitekim bu hükme göre veri sahibi, "kolayca erişilebilen verileri" kullanarak kullanıcının ekonomik durumu, mal varlıkları ve üretim yöntemleri hakkında veya kullanıcının ticari faaliyet gösterdiği pazarlardaki konumunu zayıflatabilecek herhangi bir başka şekilde kullanımına ilişkin çıkarımlarda bulunamaz. Veri sahibinin kolayca erişilebilen verileri kullanımını kısıtlayan bir diğer düzenleme, Art. 4 f. 14'e göre söz konusu verilerin kullanıcının talebi üzerine üçüncü kişilere aktarıldığı durumlara ilişkindir. Bu durumda veri sahipleri, kişisel olmayan ürün verilerini, kullanıcı ile akdedilen veri lisansı sözleşmesini ifa etmek dışında hiçbir ticari veya ticari olmayan amaçla üçüncü taraflara sağlayamaz. Hatta veri sahibi, gerekli olduğu takdirde veriyi aktaracağı üçüncü kişileri de, bunlara aktarılan verileri yeniden paylaşmamaları konusunda sözleşmesel olarak yükümlü kılmalıdırlar.

İlgili düzenlemelerden anlaşılacağı üzere bağlantılı ürün ya da hizmet vasıtasıyla elde edilen ve "kolayca erişilebilen veri" tanımını haiz olan kişisel olmayan veriler, veri sahibi tarafından münhasıran veri lisansına dayalı olarak işlenebilecek, üçüncü kişilerle paylaşım da yine münhasıran veri lisansı sözleşmesinde öngörülen yükümlülüklerin ifası amacıyla ve bunun dışında herhangi bir ticari amaç gütmeksizin paylaşabilecektir. Bu açıdan bakıldığında veri sahiplerinin, bağlantılı ürün ya da hizmet tedariğine ilişkin kullanıcılarla akdedilecek olan sözleşmelere her ne kadar doğrudan taraf olmasalar da, bu kullanıcılarla gerekli veri lisansı sözleşmelerini akdetmeleri, kendi teknik ve idari altyapılarını buna

[18] Hennemann/Ebner/Karsten/Lienemann/Wienroeder, Data Act – An Introduction, 2024, s. 71 vd.

göre şekillendirmeleri, üçüncü kişilerle paylaşım noktasında da gerekli teknik ve idari tedbirleri almaları gerekecektir.

cc. Veri Sahibinin Yükümlülükleri

Veri sahibi ile kullanıcı arasındaki ilişkide Art. 4, muhtelif düzenlemeler vesilesiyle bazı kısıtlamalar öngörmektedir.

Bunlardan ilki, f. 4'e göre "karanlık tasarım" kullanımı yasağına ilişkindir. Bu düzenlemeye göre veri sahipleri, kullanıcıların bu madde uyarınca seçim yapma veya haklarını kullanmalarını, kullanıcıya taraflı bir şekilde seçenekler sunarak veya dijital bir kullanıcı arayüzünün veya bir kısmının yapısı, tasarımı, işlevi ya da işleyişi aracılığıyla kullanıcının özerkliğini, karar verme özgürlüğünü veya tercih yapma serbestisini zayıflatarak ya da engelleyerek gereksiz yere zorlaştıramaz. "Dark patterns" ya da karanlık tasarımlar olarak nitelendirilen bu gibi durumlarda bilhassa bilinçaltı yöntemlerle kullanıcının belirli bir yönde karar vermesi için çeşitli yöntemlere başvurulmaktadır. Veri Yasası, kullanıcının haklarını kullanması aşamasında söz konusu yöntemleri açıkça yasaklamaktadır[19].

Ayrıca kişisel verilerin korunması hukukundan da tanıdık olan amaca bağlılık ilkesine göre veri sahibi, kullanıcıdan, kullanıcıyı tespit etmek için gerekli olan veriden daha fazlasını talep edemeyecektir. Nitekim belirtildiği üzere aynı ürün ya da hizmet, birden fazla kişi tarafından kullanılabilecek ve hatta kullanım hakkı başka kişilere de devredilebilecektir. Doğru kişiye doğru verilerin sunulabilmesi ve bu erişim talebinin yerine getirilip getirilmediğini belgelemek amacıyla veri sahibi, gerekli verileri kullanıcıdan talep edebilecekken, erişim talebinin yerine getirilmesi dışında kalan bilgilerin talep edilmesi, f. 5 hükmüne göre mümkün olmayacaktır.

Veri sahipleri açısından önem arz eden bir diğer yükümlülük ise f. 5 kapsamında kişisel verilere ilişkindir. Şöyle ki her türlü kişisel veri işleme faaliyeti, hukuki bir sebebe dayanmalıdır. Buradan hareketle bazı durumlarda kullanıcı, bağlantılı ürün ya da hizmete ilişkin erişim talebinde bulunduğunda bu veriler, bir üçüncü kişinin kişisel verilerini de içerebilmektedir. Bu gibi durumlarda kullanıcı, kendisiyle ilgili olmayan, yani üçüncü kişinin kişisel verisine erişim talebinde bulunuyorsa, bu erişim de kişisel veri işleme faaliyeti olarak nitelendirilecek ve dolayısıyla Genel Veri Koruma Tüzüğü kapsamında hukuki bir sebebe dayandırılacaktır. Aksi takdirde erişim talebinin reddi gerekmektedir.

İlgili hükümlerden anlaşılacağı üzere veri sahibi, erişim imkanı sunarken karanlık tasarımlardan kaçınacak, kullanıcıdan erişim talebi çerçevesinde sadece kendisini tanımlamak için gerekli verileri

[19] Hennemann/Ebner/Karsten/Lienemann/Wienroeder, Data Act – An Introduction, 2024, s. 85 vd.

isteyecek ve erişim talebine konu olan verilerin kişisel veri niteliğini haiz olup olmadığını denetleyecek, kişisel verinin söz konusu olduğu durumlarda ise hukuki sebep araştırması yapacaktır. Dolayısıyla veri sahibinin söz konusu yükümlülükleri yerine getirebilmesi amacıyla gerekli teknik ve idari tedbirleri alması gerekecektir.

çç. Veri Sahibinin Hakları

Erişim talebi kapsamında Art. 4, veri sahibi açısından münhasıran yükümlülükler getirmemekte, bazı durumlarda veri sahibine talebi reddetme ya da sınırlandırma hakkı da sunmaktadır.

Öncelikle Art. 4 f. 2 hükmüne göre verilere erişim, bunların kullanımı ve üçüncü kişilere aktarımı, AB mevzuatında öngörülen güvenlik beklentilerini olumsuz şekilde etkilemeye ve bu sayede gerçek kişilerin sağlık ve güvenliğini ciddi derecede tehlikeye atmaya elverişliyse, veri sahibi akdedilmesi öngörülen sözleşme kapsamında bu erişim, kullanım ve aktarım haklarını sınırlandırabilmektedir. Veri sahibinin söz konusu talepleri reddetmesi halinde bu durumu Art. 37 çerçevesinde yetkili kuruma bildirmesi gerekmektedir. Hükümden de anlaşılacağı üzere bu bağlamda ispat yükü, veri sahibinde olacak, talebin reddi ancak istisnai durumlarda gündeme gelebilecektir.

Bir diğer önemli husus ticari sırlara ilişkindir. Gerçekten de yasama sürecinde en çok tartışmaya konu olan konulardan birisi ticari sırların erişim talebine konu olup olmayacağına ilişkindir. Bu bağlamda kural ticari sırların korunması olmakla birlikte, ancak veri sahibi ile kullanıcı tarafından ticari sırların bilhassa üçüncü kişilere karşı korunması için gerekli bütün önlemlerin alınması halinde ticari sırların da erişim talebine konu olması mümkündür. Bu bağlamda taraflar arasında kararlaştırılabilecek idari ve teknik önlemlere örnek olarak f. 6 çerçevesinde standart sözleşme hükümleri, gizlilik sözleşmeleri, katı erişim protokolleri, teknik standartlar ve davranış kuralları zikredilmektedir. Bununla birlikte f. 7'ye göre taraflar arasında bir anlaşmaya varılamaz, kullanıcı nezdinde kararlaştırılan teknik ve idari tedbirler uygulanamaz ya da kullanıcı kendi yükümlülüklerini ihlal ederse, veri sahibi veriye erişim talebini reddetme ya da sonlandırma yetkisini haiz olacaktır. Ancak veri sahibinin bu durumu gerekçeleriyle birlikte yazılı olarak kullanıcıya ve Art. 37 çerçevesinde yetkili kuruma bildirmesi gerekmektedir. Nihayet taraflar arasında bir anlaşmaya varılsa dahi istisnai durumlarda veri sahibine f. 8 çerçevesinde erişim talebini reddetme imkânı tanınmaktadır. Bu düzenlemeye göre her ne kadar taraflar idari ve teknik tedbirler üzerinde mutabakata varmış olsalar dahi, veri sahibinin söz konusu idari ve teknik tedbirlere rağmen ağır ticari zararlara uğraması ihtimal dahilindeyse belirli verilere ilişkin münferit erişim talebini reddedebilecektir. Ağır ticari zarar, özellikle üçüncü ülkelerde ticari sırların korunmasına ilişkin engeller, erişim talep edilen verinin niteliği ve hassasiyet derecesi ile bağlantılı

ürünün münhasırlığı ve yeniliğine ilişkin olabilecektir. Bu gibi istisnai durumlarda da veri sahibi kararını derhal kullanıcıya ve yetkili kuruma bildirmekle yükümlüdür.

Veri sahibini korumayı amaçlayan bir diğer hüküm, f. 10'a göre kullanıcının erişim talep ettiği verileri kullanımının sınırlandırılmasına ilişkindir. Buna göre kullanıcı, talep ettiği verileri, verilerin elde edildiği bağlı ürünle rekabet eden bir bağlı ürün geliştirmek için kullanamaz; bu verileri üçüncü bir tarafa bu amaçla aktaramaz veya üreticinin ya da ilgili durumlarda veri sahibinin ekonomik durumu, mal varlıkları ve üretim yöntemlerine ilişkin çıkarımlar elde etmek için kullanamaz. Son olarak kullanıcı, f. 11'e göre veri sahibinin bünyesindeki verilere erişmek amacıyla zorlayıcı faaliyetlerde bulunamayacağı gibi, veri sahibinin bilişim altyapısındaki boşluklardan istifade etmek suretiyle de bu verilere erişim sağlayamaz. Bir diğer ifade ile erişim talebi, kullanıcıya veri sahibinin bilişim altyapısını "hackleme" yetkisi vermez.

d. Kullanıcının Verileri Üçüncü Kişilerle Paylaşma Hakkı (Art. 5)

Art. 3 ve 4 hükümlerinde kullanıcının bağlantılı ürün ve bağlantılı hizmet çerçevesinde elde edilen kolaylıkla erişilebilen verileri talep hakkı düzenlenmekte, ayrıca bu verileri üçüncü kişilerle de paylaşma imkânı öngörülmektedir. Üçüncü kişilerle paylaşım hususu ise özel olarak Art. 5 kapsamında düzenlenmektedir. Söz konusu düzenlemeler, özü itibariyle Art. 4 kapsamındaki düzenlemelerle benzerlik göstermektedir.

aa. Veri Sahibinin Yükümlülükleri

İlgili düzenlemenin birinci fıkrasında paylaşımın genel çerçevesi belirtilmektedir. Buna göre kullanıcının talebi üzerine veri sahibi, üçüncü bir tarafa mevcut verileri ve bu verilerin yorumlanması ve kullanılması için gerekli olan meta verileri, gecikmeden, kullanıcı için ücretsiz olarak, veri sahibinin erişimine sunulan kalitede, basit, güvenli, kullanıcı için ücretsiz, kapsamlı, yapılandırılmış, yaygın ve makine tarafından okunabilir bir formatta, ilgili ve teknik olarak mümkün olduğu ölçüde sürekli ve gerçek zamanlı olarak sağlamakla yükümlü kılınmaktadır. Verinin üçüncü kişilere sunulması bağlamında ise hüküm, daha detaylı düzenlemeler içeren Art. 8 ve 9 hükümlerine atıfta bulunmaktadır.

Veri sahibi bu bağlamda da erişim yetkisini denetlemek amacıyla ancak kullanıcı ya da üçüncü kişinin tespit edilmesi için gerekli olan bilgiden daha fazlasını talep edemeyecektir. Veri sahibinin kullanım hakkını kısıtlayan bir diğer düzenlemeye göre veri sahibi, üçüncü kişinin ekonomik durumu, mal varlıkları ve üretim yöntemleri hakkında veya üçüncü tarafın faaliyet gösterdiği pazarlardaki ticari konumunu zayıflatabilecek herhangi bir başka şekilde kullanımına ilişkin çıkarımlarda bulunmak amacıyla mevcut verileri kullanamaz. Erişime konu olan verinin kişisel veri niteliğini haiz olması

halinde ise yine GVKT bağlamında hukuki bir sebebin bulunması gerekecektir. Ayrıca ilgili kişinin GVKT'den kaynaklanan haklarının ve bilhassa veri taşınabilirliği hakkının kullanımı için veri sahibi ve veri alıcısının gerekli altyapıyı kurgulaması gerekmektedir.

bb. Sınırlamalar

Üçüncü kişiyle veri paylaşımının veri sahibinin bilişim sistemlerine hukuka aykırı şekilde erişim anlamına gelmeyeceğine ilişkin Art. 4'e benzer bir düzenleme bu bağlamda da söz konusudur. Yine ticari sırlara ilişkin düzenlemeler de Art. 4 hükmündeki fıkralara benzerlik göstermektedir.

Bu bağlamda en önemli sınırlandırma ise Digital Markets Act (EU/2022/1925) Art. 3 bağlamında kapı bekçisi (gatekeeper) olarak tanımlanan aktörlere ilişkindir. Her ne kadar kullanıcı, veri sahibinden kendisine ve üçüncü kişiler lehine erişim talep etme yetkisine sahip olsa da, bu yetki, kapı bekçilerini kapsamamaktadır. Bu bağlamda kapı bekçileri;

- Bir kullanıcıyı, doğrudan ya da finansal veya başka bir karşılık da dahil olmak üzere herhangi bir şekilde ticari teşviklerle, 4. madde 1. fıkrası uyarınca elde edilen verileri kendi hizmetlerinden biri için sağlamaya teşvik etmek veya bu konuda talepte bulunmak;
- Bir kullanıcıyı, veri sahibinden bu maddenin 1. fıkrası uyarınca kendi hizmetlerinden biri için veri sağlamasını talep etmeye teşvik etmek veya bu konuda ticari teşvikler sunmak;
- Kullanıcının, 4. madde 1. fıkrası uyarınca elde ettiği verileri kendisinden alması;

şeklindeki uygulamalardan men edilmiştir. Bu düzenlemenin amacı, halihazırda veri siloları oluşturmuş olan kapı bekçilerinin, bilhassa tüketicilere kendi ticari konumlarını da kullanmak suretiyle verileri kendileriyle paylaşmaya teşvik etmek ve rekabet ortamını daha da olumsuz şekilde etkilemelerinin önlenmesidir.

e. Veriyi Elde Eden Üçüncü Kişilerin Yükümlülükleri (Art. 6)

Üçüncü kişi, elde ettiği verileri ancak kullanıcı ile mutabakata vardığı amaçlar doğrultusunda işleyebilecektir. Söz konusu verilerin kişisel veri niteliğini haiz olması halinde ise ayrıca GVKT dikkate alınacaktır. Bu bağlamda üçüncü kişinin kullanım hakkına çeşitli sınırlandırmalar getirilmiştir.

Bu bağlamda öncelikle kullanıcılara ilişkin karanlık tasarım yasağı kullanıcı-üçüncü kişi ilişkisinde de aynı şekilde söz konusudur. Üçüncü kişinin profilleme yapması da, kullanıcı tarafından talep edilen hizmetin sağlanması için gerekli olmadığı takdirde yasaklanmaktadır. Üçüncü tarafın elde ettiği veriler, ancak kullanıcıyla yapılacak olan bir sözleşme ile mümkün olacak, bu ilişkide de kullanıcı ile üçüncü kişi arasında öngörülen gizliliğe ilişkin bütün tedbirler aynı şekilde uygulanacaktır. Üçüncü kişinin elde ettiği verileri kapı bekçileriyle paylaşması da yasaklanmaktadır. Ayrıca üçüncü kişi, elde ettiği verileri,

verilerin geldiği bağlı ürünle rekabet eden bir ürün geliştirmek için kullanamayacak veya bu amaçla başka bir üçüncü tarafa sağlayamayacaktır. Üçüncü taraflara ayrıca kendilerine sağlanan kişisel olmayan ürün verilerini veya bağlı hizmet verilerini, veri sahibinin ekonomik durumu, mal varlıkları, üretim yöntemleri veya veri sahibinin kullanımı hakkında çıkarım yapmak amacıyla kullanmaları da yasaktır. Üçüncü kişi elde edilen verileri, bağlı ürünün veya hizmetin güvenliğine zarar verecek şekilde kullanamayacak, veri sahibi veya ticari sırların sahibi ile 5. madde 9. fıkra uyarınca üzerinde anlaşmaya varılan tedbirleri ihlal ederek, ticari sırların gizliliğini zayıflatamayacak, bir tüketici olan kullanıcıyı, elde edilen verileri diğer taraflara sağlamasını engelleyemeyecektir.

4. Üçüncü ve Dördüncü Bölüm: Veri Paylaşımına İlişkin Düzenlemeler

Veri Yasası, üçüncü bölüm kapsamında veri sahiplerinin veriye erişim bağlamında yükümlülüklerinin somutlaştırmaktayken, ilerleyen dördüncü bölümde ise haksız ticari şartlara ilişkin önemli düzenlemeler içermektedir. Her iki bölüm de teşebbüsler arasındaki veri paylaşımının genel çerçevesini belirlediği için bir bütün olarak ele alınacaktır.

a. FRAND İlkeleri

Öncelikle Art. 8, veri sahibinin hangi şartlar altında veri alıcısına verileri sunması gerektiğini düzenlemektedir. Öncelikle Art. 5 hükmü çerçevesinde veri sunma yükümlülüğü altında olan veri sahibi, ticari bir ilişki çerçevesinde veri alıcısına veri sunmakla yükümlü kılındıysa bu kişiyle, adil, makul ve ayrımcılığa sebebiyet vermeyecek şartlar altında şeffaf bir şekilde verinin ne şekilde sunulacağına ilişkin mutabakata varmalıdır. Bu bağlamda rekabet ve fikri mülkiyet hukukunda uygulama alanı bulan FRAND (fair, reasonable, non-discrimanatory) ilkeleri benimsenmektedir. Ancak bu ilkelerin içeriği, bilhassa hangi durumlarda haksız şartın söz konusu olacağı, Art. 13 hükmünde özel olarak düzenlenmektedir. Verinin hangi şartlar altında erişime sunulacağı noktasında özel olarak düzenleme alanı bulan husus ücrete ilişkindir. Art. 9 hükmüne göre veri sahibinin veri alıcısından talep edeceği ücret özellikle eşitlik ilkesine aykırılık teşkil etmeyecektir. Ücretin hesaplanmasına verinin erişime sunulabilmesi için yapılan masraflar ile verinin elde edilebilmesi için veri sahibi tarafından yapılan yatırımlar dikkate alınabilecektir. Bununla birlikte veri alıcısının mikro ya da küçük ölçekli bir teşebbüs olduğu durumlarda ücret, münhasıran verinin teknik açıdan erişime sunulabilmesi için gerekli masraflarla sınırlandırılmaktadır. Bu bağlamda talep halinde veri sahibinin ücreti nasıl hesapladığı hususunda hesap vermesi de gündeme gelebilecektir.

Her ne kadar teşebbüsler arasında veri paylaşımına ilişkin akdedilecek olan sözleşme hükümlerinde genel olarak FRAND ilkeleri esas alınacak olsa da, hangi hallerde haksız şartlardan bahis açılabileceği

ancak 13. madde kapsamında düzenlenmektedir. Art. 13 hükmü, aynı zamanda veri sözleşmeleri bağlamında haksız şartlara ilişkin özel bir düzenleme teşkil etmekle birlikte, veri lisanslandırma uygulamaları açısından da son derece önemli bir hükümdür. Bu sebeple ilgili hükmün etraflıca incelenmesi gerekmektedir. Zira bundan sonra veri tedariğine ilişkin akdedilecek sözleşmelerde esas alınacak model, muhtemelen ilgili hüküm doğrultusunda şekillenecek, bir diğer ifade ile Art. 13 hükmü veri tedarik sözleşmelerinde altın standart teşkil edecektir.

b. B2B İlişkilerinde Veri Paylaşımına Dair Haksız Şartlar (Art. 13)

Veri Yasası, teşebbüsler arasındaki veri paylaşımında tarafların belirli konular üzerinde mutabakata varmaları gerektiğini öngörmekte, bu mutabakatın enstrümanı olarak ise sözleşmeleri esas almaktadır. Bununla birlikte Veri Yasası, taraflar arasındaki bilhassa ekonomik güç dengelerini de gözeterek sözleşme serbestisi ilkesinin aksine sözleşme içeriğini bütünüyle tarafların keyfiyetine bırakmamaktadır. Bu çerçevede öncelikle sözleşmelerin FRAND ilkelerine uyumlu olması gerektiği belirtilmişti. Bu genel ilkelere ilaveten Veri Yasası, Art. 13 kapsamında haksız şartları düzenlemektedir. Bu düzenleme, öncelikle genel kural, ardından nisbi haksız şartlar ve son olarak mutlak haksız şartlar şeklinde üç kısımdan ibarettir. Bu sistematik, 6102 sayılı Türk Ticaret Kanunu'nun haksız rekabete ilişkin hükümlerinde de benzer bir şekilde mevcuttur. Zira TTK md. 54 f. 2'de haksız şart, soyut bir şekilde "rakipler arasında veya tedarik edenlerle müşteriler arasındaki ilişkileri etkileyen aldatıcı veya dürüstlük kuralına diğer şekillerdeki aykırı davranışlar ile ticari uygulamalar" şeklinde tanımlandıktan sonra, md. 55 kapsamında tahdidi nitelikte olmayacak şekilde örnekler sunulmaktadır.

Veri Yasası da benzer şekilde öncelikle hangi sözleşme hükümlerinin haksız şart teşkil edebileceğini düzenlemektedir. Buna göre "*Bir teşebbüsün bir başka teşebbüse tek taraflı dayattığı veri erişimi ve veri kullanımı ile ilgili sözleşme hükümleri veya veri ile ilgili yükümlülüklerin ihlali ya da sona erdirilmesi durumunda sorumluluk ve hukuki yolları kapsayan hükümler, kötüye kullanıldığı takdirde, dayatılan teşebbüs açısından bağlayıcı değildir*". Bununla birlikte ilgili hükümlerin Birlik Hukukundaki emredici hükümlere uygun olması halinde haksız şart söz konusu olmayacaktır. Haksız şartın tanımı ise f. 3 kapsamında şu şekilde yapılmıştır: "*Sözleşme hükümleri, veri erişimi ve veri kullanımı konularında iş ilişkilerinde geçerli iyi uygulamalardan ciddi bir sapma oluşturduğunda veya dürüstlük kuralına aykırı olduğunda haksız şart teşkil eder*." Ancak belirtildiği üzere bu tanım son derece soyuttur. Hatta veri erişimi ve kullanımı noktasında "iş ilişkilerinde iyi uygulamaların" ne olduğunun an itibariyle tespit edilmesinin mümkün olmadığı dahi söylenebilecektir.

Buradan hareketle Veri Yasası Art. 13 f. 4, öncelikle hangi hallerde bir sözleşme hükmünün haksız şart olarak değerlendirilebileceğini düzenlemektedir. Hemen belirtelim ki burada mutlak bir karine söz konusu olmayıp çok istisnai hallere mahsus olsa da aksinin ispatının mümkün olduğu da anlaşılmaktadır. Bu bağlamda ilgili fıkra, bir sözleşme hükmünün amacı ya da etkisinin aşağıdaki durumlara sebebiyet vermesi halinde haksız şart teşkil edeceğini düzenlemektedir:

> *a) Hükmü tek taraflı olarak dayatan tarafın kasıt ya da ağır kusurlu davranışları sebebiyle sorumluluğu ortadan kaldıran ya da sınırlayan sözleşme hükümleri;*
>
> *b) Sözleşmeden kaynaklanan borçların ifa edilmemesi halinde hükmün tek taraflı olarak dayatıldığı tarafın hak arama yollarını ortadan kaldıran ya da hükmü dayatan tarafın bu yükümlülüklerin ihlali durumunda sorumluluktan muafiyetini sağlayan hükümler;*
>
> *c) Hükmü tek taraflı olarak dayatan tarafın tek taraflı olarak sağlanan verilerin sözleşmeye uygun olup olmadığını belirleme veya sözleşme hükümlerini yorumlama hakkını veren sözleşme hükümleri*.

Hemen belirtelim ki söz konusu hükümler, esasında münhasıran veriye erişim ve veri kullanımı sözleşmelerine mahsus değildir. Bilakis benzer düzenlemelerin her türlü sözleşme ilişkilerinde haksız şart teşkil etmesi söz konusudur. Bu açıdan bakıldığında f. 4 hükmünde düzenleme bulan haksız şartların veri ekosistemine özgü düzenlemeler niteliğinde olmadığı söylenebilecektir.

Veri sözleşmelerine mahsus düzenlemeler içeren f. 5 hükmüne göre ise bir sözleşme hükmü, özellikle aşağıdaki hususları amaçlıyor ya da hükmün uygulanması aşağıdaki hususlara sebebiyet veriyorsa haksız şarttan bahis açılacaktır:

> *a) Sözleşme yükümlülüklerinin yerine getirilmemesi durumunda hukuki yolların orantısız bir şekilde kısıtlanması veya sorumluluğun genişletilmesi;*
>
> *b) Hükmü tek taraflı olarak dayatan tarafın, diğer sözleşme tarafının meşru menfaatlerine ciddi derecede zarar verecek şekilde verilerine erişme ve bunları kullanma hakkı kazanması; bu durum, özellikle erişime konu olan verilerin hassas ticari veriler içermesi ya da hukuken ticari sır veya fikri mülkiyet olarak korunması hallerinde söz konusu olacaktır;*
>
> *c) Hükmü dayatılan tarafın, sözleşme süresi boyunca sağladığı veya ürettiği verileri kullanmasını engellemek veya bu verilerin makul bir şekilde kullanılmasına, erişilmesine, toplanmasına, kontrol edilmesine veya değerlendirilmesine yönelik bir sınırlama getirmek;*
>
> *d) Hükmü dayatılan tarafın, sözleşmeyi makul bir süre içinde feshetmesini engellemek;*

e) Hükmü dayatılan tarafın, sözleşme süresi boyunca veya sözleşmenin sona ermesinden makul bir süre sonra sağladığı veya ürettiği verilerin bir kopyasını elde etmesini engellemek;

f) Hükmü dayatan tarafın, diğer sözleşme tarafının benzer başka bir hizmete geçme olasılığını ve fesih nedeniyle oluşacak maddi zararı dikkate almaksızın, sözleşmeyi makul olmayan bir süre içinde feshetme hakkına sahip olması;

g) Hükmü dayatan tarafın, sözleşmede belirtilmiş geçerli bir gerekçe olmaksızın, sözleşmede kararlaştırılan fiyatı veya verilerin türü, formatı, kalitesi ya da miktarına ilişkin diğer önemli bir koşulu önemli ölçüde değiştirme hakkına sahip olması ve diğer tarafın böyle bir değişiklik durumunda sözleşmeyi feshetme hakkına sahip olmaması.

Bununla birlikte g) bendi çerçevesinde haksız şart teşkil eden bir hüküm, süresiz sözleşme ilişkilerinde belirli şartlar altında gündeme gelmeyecektir. Bunun için öncelikle tek taraflı değişiklik yetkisinin sözleşmede belirtilen geçerli bir gerekçeye dayanması, hükmü dayatan tarafın diğer sözleşme tarafını makul bir süre önceden bu değişiklikten haberdar etmesi ve diğer tarafın böyle bir değişiklik durumunda sözleşmeyi herhangi bir bedel ödemeksizin feshetme hakkının bulunması gerekmektedir.

İlgili hükümler, emredici niteliktedir ve aksi taraflarca kararlaştırılamayacaktır. Bununla birlikte f. 8 hükmünde önemli bir hususa açıklık getirilmiştir. Buna göre asli edime ilişkin hükümler, haksız şart denetimine tabi değildir. Gerçekten de genel işlem şartları bağlamında da kabul edildiği üzere haksız şart ya da genel işlem şartı denetimi, asli edimleri konu edinemez. Asli edimler arasındaki dengesizlik, olsa olsa gabin ya da sözleşmenin uyarlanmasının konusu olabilir, ancak hukuk düzeni kural olarak asli edimlere müdahale etmez. Bununla birlikte veri sahibinin üçüncü kişilere veri sunarken talep edebileceği ücrete ilişkin Art. 9 kapsamında yine de düzenlemeler mevcuttur. Ancak bunlar haksız şart niteliğinde değil, doğrudan emredici hükümler çerçevesinde kaleme alınmıştır. Bununla birlikte haksız şarta aykırılık doğrudan geçersizliğe sebebiyet verecekken Art. 9 hükmüne aykırılığın yaptırımı konusunda tam bir netlik söz konusu değildir.

4. Bölüm VI: Veri Hizmet Sunucuları Arasında Değişim

a. Gerekçe ve Amaç

AB Komisyonu tarafından hazırlanan Etki Değerlendirme Raporuna göre veri hizmetlerinden istifade eden müşteriler, bir hizmet sunucudan diğer bir hizmet sunucuya geçiş yapmak istedikleri takdirde, belirli bir hizmet sunucunun kendi bulut bilişim ekosisteminde birçok hizmeti birleştirmesi sebebiyle

diğer bir hizmet sunucuya geçiş aşamasında mali ve teknik açıdan ve ayrıca sözleşmesel yükümlülükler sebebiyle birçok engelle karşılaşmaktadır.

Bu bağlamda davranışsal ekonomi mekanizmalarını da dikkate almak gerekecektir. Zira bir bulut hizmetinin değeri müşteri tabanının genişliğiyle doğrudan bağlantılıdır. Dolayısıyla müşteri tabanı genişledikçe doğrudan ya da dolaylı olarak ağ etkileri ortaya çıkacak ve müşteri yoğunlaşması da bu sayede artacaktır. Özellikle hizmet olarak yazılım (Software as a service-SaaS) ve hizmet olarak platform (Platform as a service-PaaS) modellerinde müşteri açısından belge ve uygulamaların sorunsuz bir şekilde diğer iş ortaklarıyla paylaşılabilmesi büyük önem arz etmektedir. Bu açıdan müşteri, kural olarak herkesin kullandığı hizmet ortamlarını öncelikle tercih edecektir. Bu sayede de üçüncü taraf geliştiriciler, en fazla müşterinin mevcut olduğu ortamlarda faaliyet göstermek zorunda kalacaktır. Müşterinin kendi çalışanları dahi meslek hayatları esnasında belirli bir platformun eğitimlerini ve sertifikalarını aldıkları ve bu alanda yetkinliklerini kazandıkları için genellikle bu hizmet sunucunun ürünlerini tercih edecek, başka bir hizmet sunucuya geçişten imtina edecektir. İşaret edilen söz konusu ağ etkileri, bulut ekosistemlerindeki aktörlerin dikey alanda entegre olması sebebiyle daha da güçlenmektedir. Zira bu sayede hizmet sunan aktör, belirli bir hizmetten veri temin edip başka bir hizmeti daha hedefli bir şekilde sunabilir ve tamamlayıcı ürünleri bir araya getirebilir. Bu bağlamda ortaya çıkan kilitlenme etkileri, 2022 yılında yapılan ve kamuya açık IaaS piyasalarını esas alan bir araştırmada çarpıcı bir şekilde ortaya çıkmaktadır: Amazon, Microsoft, Google, Alibaba ve Huawei, piyasanın % 81.1'ine hakimdirler. Bu bağlamda endişe veren bir diğer husus, söz konusu bilişim hizmetlerine ilişkin maliyetlerin de artış göstermesidir.

Bu bulgulardan hareketle Birlik, bir taraftan Avrupa menşeli veri hizmeti sunucularının pazara giriş engellerini bertaraf etmek[20], diğer yandan Birlik içerisinde "çoklu satıcıların bulunduğu bir bulut ortamı" ihdas etmek istemektedir[21].

Verinin paylaşımı ve yeniden kullanımı noktasında en büyük sorunlardan birisi de, teknik engellerdir. Bilhassa PaaS ve IaaS hizmetleri ve kamuya açıklanmayan API'lar çerçevesinde söz konusu engeller önem taşımaktadır. Şayet teknik standartların oluşturulmasında piyasa kendi başına bir inisiyatif alamıyorsa, Komisyon'un talebi üzerine AB standartlaştırma kuruluşlarının müdahale etmesi gerektiği belirtilmektedir.

[20] Veri Yasası, Dibace 78.
[21] Veri Yasası, Dibace No. 100.

b. Hizmetler Arası Değişim

aa. Müşteriye Sunulan İmkanlar

Her ne kadar bölüm başlığı, "veri işleme hizmetleri arasında geçiş" olsa da, esasında Bölüm VI kapsamında ele alınan düzenlemeler münhasıran geçiş işlemleriyle sınırlı değildir. Bilakis müşteri lehine çeşitli imkanlar öngörülmektedir:

- Hedef sağlayıcıya geçiş (Madde 23(c), Madde 25(2)(a), Madde 25(3)(a))
- Yerinde (on-premises) altyapıya transfer (Madde 23(c), Madde 25(2)(a), Madde 25(3)(b))
- Müşterinin aktarılabilir verilerinin ve dijital varlıklarının silinmesi (Madde 25(2)(c)(ii), Madde 25(2)(h), Madde 25(3)(c))
- Birden çok veri işleme hizmetlerinin paralel olarak kullanımı (Madde 34(1)).

Müşteriye sunulan bu genel imkanlardan hareketle öncelikle Bölüm VI hükümlerinin uygulama alanına değinilecektir. Bu bağlamda özellikle veri işleme hizmetleri, kaynak sağlayıcı ve hedef sağlayıcı terimlerinin açıklanması gerekmektedir.

bb. Uygulama Alanı

23-31. maddelerde esas alınan hizmet modeli, veri işleme hizmetleridir (data processing services). Veri işleme hizmeti, Veri Yasası Art. 2 f. 8 hükmünde son derece karmaşık bir şekilde tanımlanmaktadır. Buna göre veri işleme hizmeti, bir müşteriye sağlanan ve merkezi, dağıtılmış veya son derece dağıtılmış türdeki yapılandırılabilir, ölçeklenebilir ve esnek bilgi işlem kaynaklarının paylaşılan bir havuzuna kapsamlı ve talep üzerine mevcut olan ağ erişimini sağlayan bir dijital hizmettir; bu kaynaklar, hizmet sağlayıcısının minimum yönetim çabası veya minimum etkileşimiyle hızla sağlanabilir ve serbest bırakılabilir. Bu tanımda yer verilen bazı hususlara açıklık getirmek gerekmektedir. Bu bağlamda:

- "Bilgi işlem kaynakları" terimi geniş anlamda kullanılır ve ağları, sunucuları ya da diğer sanal veya fiziksel altyapıları, yazılımı, depolamayı, uygulamaları ve hizmetleri içerir. Özellikle, çoğu IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) ve SaaS (Software-as-a-Service) sağlayıcıları bu kapsama girer.
- "Ortak havuz" terimi, bilgi işlem kaynaklarının birden çok kullanıcıya sunulmasını gerektirir.
- "Konumdan bağımsızlık", veri işleme işlevlerinin ağ üzerinden sağlanması gerektiğini belirtir ve erişim, çeşitli Thin ya da Thick-client platformlarına (web tarayıcılarından mobil cihazlara ve masaüstü bilgisayarlara kadar) desteklenmelidir.

- "Ölçeklenebilirlik", hizmet sağlayıcısının bilgi işlem kaynaklarını coğrafi konumdan bağımsız olarak, talep dalgalanmalarına yanıt verecek şekilde esnek bir şekilde tahsis edebilmesini ifade eder.
- "Esneklik", bilgi işlem kaynaklarının talebe bağlı olarak hızlı bir şekilde tahsis edilmesi ve serbest bırakılması gerektiğini belirtir.

Her ne kadar Veri Yasası'nın tanımlar kısmında yer verilmemiş olsa da Bölüm VI, özü itibariyle kaynak sağlayıcı ve hedef sağlayıcı terimlerini kullanmakta, bunlar arasındaki geçiş işlemlerini esas almaktadır. Kaynak sağlayıcı, müşterinin hâlihazırda bir sözleşme ilişkisi içinde bulunduğu eski sağlayıcıdır. Hedef sağlayıcı, müşterinin geçiş yapmak istediği yeni sağlayıcıdır.

Son olarak Art. 31 çerçevesinde belirli hizmetler açısından muafiyet söz konusudur. Şöyle ki bir veri işleme hizmeti, özellikle bireysel müşterilerin ihtiyaçlarına göre tasarlanmış ise bu tür hizmet sağlayıcıların yükümlülükleri hafifletilmekte, test ya da deneme sürümleri açısından ise bütünüyle muafiyet gündeme gelmektedir. Ne var ki hizmet sağlayıcının müşterisini söz konusu kısmi ya da tam muafiyet hususunda sözleşme akdedilmesi aşamasında bilgilendirmesi gerekmektedir[22].

cc. Art. 23: Geçiş Engellerinin Kaldırılması

Madde 23'e göre, veri işleme hizmet sağlayıcıları, müşterilerinin başka bir sağlayıcıya geçişini ya da aynı anda birden fazla sağlayıcıyı kullanmasını mümkün kılmak için geniş çapta önlemler almak zorundadır. Özellikle, veri işleme hizmet sağlayıcıları, müşterilerine ticari, teknik, sözleşmesel ya da organizasyonel hiçbir engel koymamalı ve mevcut olan engelleri mümkün olduğunca ortadan kaldırmalıdır. Bu bağlamda özellikle aşağıdaki hususlara ilişkin engellerin ortadan kaldırılması gerekmektedir:

- Aynı hizmet türü için başka bir veri işleme hizmet sağlayıcısıyla yeni bir sözleşme yapma; (Madde 29, bu amaçla geçiş ücretlerinin kademeli olarak kaldırılmasını öngörmektedir).
- Müşterinin aktarılabilir verileri ve diğer dijital varlıklarını yeni sağlayıcıya taşıması.
- Yeni sağlayıcıda işlevsel eşdeğerliğin sağlanması; ancak işlevsel eşdeğerlik, sağlayıcının ilgili hizmeti hedef sağlayıcının altyapısında yeniden oluşturma zorunluluğu olduğu anlamına gelmemelidir.
- Teknik olarak mümkün olduğu ölçüde, sağlayıcıya bağlı belirli hizmetlerin ayrılması (unbundling).

[22] Bkz. Bomhard, Auswirkungen des Data Act auf die Geschäftsmodelle von Cloud-Anbietern, MMR 2024, s. 109, 111.

Ayrıca belirtelim ki Veri Yasası, veri işleme hizmet sağlayıcılarını yeni hizmetler geliştirmeye zorlamamaktadır. Bununla birlikte eski sağlayıcı, işlevsel eşdeğerliğin sağlanmasına yardımcı olmak için elindeki tüm makul araçları kullanmak, imkanları sunmak zorundadır (uygun bilgi, dokümantasyon, teknik destek ve gerekirse gerekli araçlar).

çç. Art. 25: Bulut Müşterileri İçin Sözleşmesel Geçiş İmkanları

Art. 25 f. 1, öncelikle veri işleme hizmet sağlayıcısı ile müşteri arasında farklı sağlayıcılar arasında geçiş ya da yerinde altyapıya transfer gibi hususlara ilişkin bir sözleşme yapılması, bu sözleşmenin müşteriye sözleşme akdedilmeden evvel saklayabilecek ve çoğaltabilecek şekilde sunulması zorunluluğunu öngörmektedir.

Art. 25 f. 2 b. d)'ye göre ise müşteri, sözleşme süresi içerisinde her zaman en fazla iki ay önceden bildirimde bulunmak suretiyle geçiş sürecini başlatabilir. Bu bildirim süresi sona erdiğinde artık geçiş dönemi başlar. Sağlayıcı, sözleşmede bağlayıcı bir geçiş süresi belirlemek zorundadır; bu süre en fazla 30 gün olabilir. Eğer belirli bir durumda bu süre yetersiz kalırsa, sağlayıcı bu süreyi en fazla yedi aya kadar uzatabilir. Ayrıca, sözleşme, müşteriye geçiş süresini bir kez daha uzatma hakkı tanıyan bir madde içermelidir. B. c)'ye göre geçiş sürecinin başarılı bir şekilde sonlandırılmasıyla birlikte sözleşme de sona ermiş kabul edilir.

Ayrıca Art. 25, sağlayıcının müşteriye belirli geçiş desteği sağlamasını zorunlu kılan diğer birçok sözleşme yükümlülüğünü de öngörmektedir. Bu yükümlülükler, güçlü pazarlık pozisyonuna sahip müşterilerin bile bugün bulut hizmetleri müzakerelerinde elde edebileceklerinden çok daha ileri gitmektedir. Bu bağlamda Birlik Kanun Koyucusunun sözleşme serbestisi ilkesine, bulut hizmet sağlayıcıları aleyhine ciddi derecede bir müdahalede bulunduğunu göstermektedir. Bu hükümlere örnek olarak şu hususlar verilebilir:

"Müşteriye ve onun yetkilendirdiği üçüncü kişilere geçişi gerçekleştirme konusunda uygun destek sağlamak."

- "İş sürekliliğini sağlamak için gereken özeni göstermek ve sözleşmeye dayalı işlevlerin veya hizmetlerin sunumunu sürdürmek."
- "Bilinen kesintisiz işlev veya hizmet sunumu riskleri konusunda açık bilgi sağlamak."
- "Geçiş sürecinde yüksek düzeyde güvenlik sağlamak."

Bu zorunlu çıkış yönetiminin teknik detayları büyük ölçüde belirsizdir ve daha fazla netleştirilmesi gerekmektedir. Ayrıca, Art. 25'e aykırılık durumunda hangi yaptırımların gündeme geleceği hususu da belirsizdir.

dd. Art. 26: Bilgilendirme Yükümlülükleri

Madde 26, veri işleme hizmet sağlayıcılarını (potansiyel) müşterilerine belirli bilgileri sağlama konusunda yükümlü kılmaktadır. Bu bilgilere şunlar dahildir:

- Geçiş ve içerik transferi için mevcut prosedürler hakkında bilgiler: Geçiş ve transfer yöntemleri ve formatları hakkında bilgiler, ayrıca sınırlamalar ve teknik kısıtlamalar.
- Veri yapıları ve veri formatları hakkında ayrıntılar: İlgili standartlar ve açık birlikte çalışabilirlik (interoperability) özelliklerine dair bilgiler.

ee. Art. 27: İyi Niyetle Hareket Etme Yükümlülüğü

Madde 27 dikkat çekicidir. Buna göre taraflar, geçişin etkili bir şekilde gerçekleştirilmesi, verilerin zamanında aktarılabilmesi ve veri işleme hizmetinin sürekliliğinin sağlanması amacıyla **iyi niyetle** iş birliği yapmak zorundadır. Bu tür hükümler doğrudan zorlayıcı olmasa da, bir hizmet sağlayıcının Madde 27 kapsamında belirli teknik işlemleri veya sözleşme müzakerelerini reddetmesi, olası ikincil hukuki sonuçlara (örneğin, kamu otoriteleri tarafından para cezası ya da sivil hukuk kapsamındaki tazminat talepleri) neden olabilir.

ff. Art. 30: Teknik Yükümlülükler

Madde 30, sağlayıcı değişikliklerini kolaylaştırmak amacıyla teknik sağlayıcı yükümlülüklerini düzenlemektedir. Belirli sağlayıcılar, Madde 30'un 2. fıkrasına göre müşterilerine, hizmet hakkında yeterli bilgi içeren **açık arayüzleri** ücretsiz olarak sağlamak zorundadır. Bu bilgiler, veri taşınabilirliği ve birlikte çalışabilirlik (interoperability) amaçlarıyla hizmetlerle iletişim kuracak yazılımların geliştirilmesi için gereklidir.

6. Bölüm VIII: Birlikte Çalışabilirlik

Veri ve veri paylaşımının teknik düzeyde standartlaştırılması, Avrupa Birliği'nde işlevsel bir veri pazarı oluşturmayı hedefleyen Data Act'in VIII. bölümünde düzenlenmektedir. Bu bağlamda Art. 33 ila 36 hükümleri arasında veri paylaşımı anlaşmalarının ifası için veri alanları, veri işleme hizmetleri ve akıllı sözleşmelere ilişkin standartların oluşturulması için gereksinimler ve süreçler ele alınmaktadır. Bu bağlamda ise birlikte çalışabilirlik (interoperatibility) kavramı önem arz etmektedir.

Gerçekten de her ne kadar hukuki yükümlülükler vesilesiyle veri piyasalarındaki rekabetin güçlendirilmesi, veri paylaşımı mekanizmalarının kolaylaştırılması mümkün olsa da, bu mekanizmaların fiili olarak işlevsel bir şekilde hayata geçirilebilmesi için teknik düzeyde standartların oluşturulması kaçınılmazdır. Bu bağlamda Art. 33-36 hükümlerinde veri alanlarının ve akıllı

sözleşmelerin birlikte çalışabilirliği için temel gereksinimlerin ve standartların, ayrıca veri işleme hizmetlerinin birlikte çalışabilirliği ve taşınabilirliği için standartların oluşturulması amaçlanmaktadır. Ayrıca bu standartlar, Bölüm VI. kapsamında öngörülen veri işleme hizmet sunucuları arasındaki değişim mekanizması açısından da önemli bir unsurdur. Zira ancak standartların oluşturulması halinde bir hizmet sağlayıcıdan diğer bir hizmet sağlayıcıya geçiş kolaylaşacaktır.

a. Veri Alanlarına İlişkin Yasal Gereksinimler

Art. 33 hükmü, veriler, verinin paylaşımına ilişkin mekanizmalar ve hizmetler ile Birlik veri alanları arasında birlikte çalışabilirliğe ilişkin esaslı gereksinimleri düzenlemektedir. Hemen belirtelim ki veri alanı kavramı, Veri Yasası kapsamında tanımlanmamıştır. Buna karşılık Art. 33, veri alanlarına katılım sağlamak isteyen aktörlerin yükümlülüklerine ilişkin detaylı düzenlemeler içermektedir. Bu bağlamda veri alanına katılan ve diğer paydaşlara veri veya veri hizmeti sunan kişiler, veri alanının işlevselliğini mümkün kılmak adına bazı hususları dikkate almak zorundadırlar. Özellikle belirtelim ki söz konusu veri alanları, belirli bir amaca yönelik, belirli bir sektöre yönelik ya da sektörler arası bir veri alanı teşkil edebilirler. Söz konusu alanların amacı, yeni ürünler ve hizmetlerin geliştirilmesi, bilimsel araştırma ya da sivil toplum girişimlerinden ibaret olabilecektir. Veri alanlarının işleyişi esnasında öngörülen birlikte çalışabilirlik kriterleri şu şekildedir:

> **a)** Veri seti içerikleri, kullanım kısıtlamaları, lisanslar, veri toplama yöntemleri, veri kalitesi ve belirsizlikler, alıcının verileri bulmasına, erişmesine ve kullanmasına olanak tanıyacak şekilde yeterince açıklanmalıdır, gerektiğinde makine tarafından okunabilir formatta olmalıdır;
>
> **b)** Veri yapıları, veri formatları, kelime dağarcıkları, sınıflandırma sistemleri, taksonomiler ve kod listeleri mevcutsa kamuya açık ve tutarlı bir şekilde açıklanmalıdır;
>
> **c)** Veri erişimi için kullanılan teknik araçlar, örneğin uygulama programlama arayüzleri (API'ler), kullanım şartları ve hizmet kalitesi, taraflar arasında otomatik veri erişimini ve veri aktarımını - sürekli, toplu indirme ya da gerçek zamanlı olarak makine tarafından okunabilir bir formatta - mümkün kılacak şekilde yeterince açıklanmalıdır, teknik olarak mümkün olduğu ve bağlı ürünün sorunsuz çalışmasını etkilemediği sürece;
>
> **d)** Akıllı sözleşmeler gibi veri paylaşımına yönelik sözleşmelerin otomatik ifasını sağlayan araçların birlikte çalışabilirliğini mümkün kılan araçlar gerektiğinde sağlanmalıdır[23].

[23] Siglmüller: Standardisierungsbestrebungen für das Rückgrat der europäischen Digitalwirtschaft, MMR 2024, s. 112, 113 vd.

b. Veri İşleme Hizmetlerine İlişkin Yasal Gereksinimler

Veri Yasası Art. 34 ve 35 hükümlerinde veri işleme hizmetlerine ilişkin yasal yükümlülükler düzenlenmektedir. Bunlar bilhassa birlikte çalışabilirlik (Art. 35 f. 1 b. a) ve taşınabilirlik (Art. 35 f. 1 b. b) konularıdır. Her ne kadar Veri Yasası, birlikte çalışabilirliği bir üst kavram olarak nitelendirip bu başlık altında ayrıca taşınabilirliği de düzenlemiş olsa da, teknik olarak bakıldığında birlikte çalışabilirlik ile taşınabilirliğin iki farklı husus olduğunu söylemek mümkündür. Zira birlikte çalışılabilirlik, iki veri işleme hizmetinin aynı anda uzun vadeli kullanımını konu edinirken taşınabilirlik, bir veri işleme hizmetinden diğerine geçişi ifade eder. Ayrıca Art. 30 kapsamında müşterilerine müşterilerine ilgili hizmetlere erişim imkanı sunmayan veri işleme hizmetleri Art. 35 f. 1 b. c)'ye göre işlevsel eşdeğerliği sağlamalıdır. Nihayet bütün bu yükümlülükler yerine getirilirken güvenlik ve veri hizmetlerinin bütünlüğü zarar görmemeli (Art. 35 f. 1 b. d) ve teknik gelişim, yeni işlevler ve inovasyon sağlanmalıdır (Art. 35 f. 1 b. e). Dolayısıyla bundan sonraki aşamada birlikte çalışabilirlik ve taşınabilirlik kavramlarının incelenmesi gerekecektir.

aa. Birlikte Çalışılabilirlik

Birlikte çalışılabilirlik, Art. 2 f. 40'a göre iki veya daha fazla veri alanının ya da iletişim ağlarının, sistemlerin, ağ bağlantılı ürünlerin, uygulamaların, veri işleme hizmetlerinin veya bileşenlerin verileri paylaşma ve kullanma yeteneği olarak tanımlanmaktadır. Bu düzenlemelerin amacı, kullanıcıların farklı sağlayıcılara ait birden fazla veri işleme hizmetini mümkün olduğunca verimli şekilde kullanmalarını ve bu hizmetlerin birbirleriyle uyumlu olmasını sağlamaktır. Bu bağlamda özellikle veri işleme hizmeti sağlayıcılarının, verilerin taşınması aşamasında birlikte çalışılabilirliği, sözdizimsel (sentaktik) birlikte çalışılabilirlik, semantik veri bağlamında birlikte çalışılabilirliği, davranışsal birlikte çalışılabilirlik ve kuralların birlikte çalışılabilirliğini sağlamak yönünde yükümlülükleri, Art. 35 f. 2 b. a) çerçevesinde gündeme gelmektedir.

bb. Taşınabilirlik

Taşınabilirlik kavramı Veri Yasası kapsamında tanımlanmamıştır. Bununla birlikte taşınabilirlikle amaçlanan husus, veri işleme hizmetleri arasında geçiş yapılması veya bu hizmetleri şirketin kendi bünyesinde bulunan altyapıya taşımasını teknik olarak mümkün kılmaktır. Taşınabilirlik, verilerle ilgili olup, özellikle sözdizimsel (sentaks) veri taşınabilirliği, anlamsal (semantik) veri taşınabilirliği ve veri kurallarının taşınabilirliği (Art. 35 f. 2 b. b) ile uygulamalarla ilgili olup, özellikle uygulama komutlarının, meta verilerinin, davranışlarının ve kurallarının taşınabilirliğini (Art. 35 f. 2 b. c) hususlarını kapsamaktadır.

Ancak birlikte çalışabilirlik ile taşınabilirliğe ilişkin gereksinimler, "aynı türdeki veri işleme hizmetleriyle sınırlıdır. Bir diğer ifade ile veri işleme hizmeti sağlayıcıları, yalnızca aynı türdeki hizmetler arasında birlikte çalışılabilirlik ve taşınabilirlik kıstaslarını sağlamakla yükümlüdürler. Bu kapsamda, veri işleme hizmetleri grupları, aynı temel amacı ve aynı temel işlevleri, ayrıca hizmetin operasyonel özellikleriyle ilgili olmayan aynı tür veri işleme modellerini paylaşmalıdır. Buradan da anlaşılacağı üzere aynı türdeki veri işleme hizmeti kavramı, ilgili hükümlerin uygulama alanı açısından büyük önem taşımaktadır. Nitekim örnek olarak **Amazon Web Services (AWS)** ve en büyük rakibi **Microsoft Azure**, ürün portföylerinde yer alan 200'den fazla hizmete sahip olup, bu hizmetler işlev ve kullanım amacı açısından büyük farklılıklar göstermektedir. Bir sağlayıcının sunduğu bir hizmet, başka bir sağlayıcıda birden fazla farklı hizmete karşılık gelebilir. Dolayısıyla ilgili hükümlerin bu gibi durumlarda ne şekilde uygulanacağı an itibariyle belirsizdir[24].

cc. Akıllı Sözleşmelere Yönelik Gereksinimler

Art. 2 f. 39'a göre akıllı sözleşmeler, bir sözleşmenin veya onun bir kısmının otomatik olarak ifası için kullanılan bilgisayar programları olarak tanımlanmaktadır. Söz konusu programlar bir dizi elektronik veri kaydını kullanmakta ve bu kayıtların bütünlüğünü ve kronolojik sıralarının doğruluğunu sağlamaktadır. Akıllı sözleşmelerin veri paylaşımı sözleşmeleri bağlamında kullanılabilmesi için öngörülen şartlar şu şekildedir:

- **Sağlamlık**: Veri paylaşım sözleşmelerinin ifası için kullanılan akıllı sözleşmeler, üçüncü taraflarca yapılan müdahalelere ve fonksiyon bozukluklarına karşı yüksek derecede sağlam olmalıdır (Art. 36 f. 1 b. a) ve sıkı erişim kontrol mekanizmalarına tabi olmalıdır (Art. 36 f. 1 b. d).
- **Durdurma Mekanizması**: Gelecekte istenmeyen işlemlerin yürütülmesini engellemek için bir mekanizma, işlemlerin durdurulmasını sağlayabilmelidir (Art. 36 f. 1 b. b).
- **Veri Arşivleme**: Tüm işlem verileri, mantık ve program kodu arşivlenmelidir, böylece gerçekleştirilen işlemler kaydedilebilmelidir (Art. 36 f. 1 b. c).
- **Doğruluk**: Son olarak, akıllı sözleşmeler veri paylaşım sözleşmesi hükümleriyle uyumlu olmalıdır (Art. 36 f. 1 b. e).

[24] Daha geniş bilgi için bkz. Siglmüller, s. 115 vd.

c. Standardizasyon

Her ne kadar Veri Yasası Art. 33 ila 36 hükümlerinde verilerin, meta verilerin, veriye erişimin, uygulamaların ve veri hizmetlerinin standartlaştırılması amaçlansa da, bu standartlaştırılma doğrudan Veri Yasası kapsamında gerçekleştirilmemektedir. Bilakis söz konusu teknik standartların oluşturulabilmesi için bir taraftan Komisyona yasal düzenlemeler yapma noktasında yetkiler verilmekte, ayrıca standart belirlemeye yetkili kuruluşlara ilişkin de düzenlemelere yer verilmektedir[25].

7. Yetkili Otorite ve Yaptırımlar

a. Yetkili Otorite

Veri Yasası Art. 37'ye göre **h**er üye devlet, Veri Yasası'nın uygulanması ve yürütülmesinden sorumlu bir veya daha fazla yetkili otorite atamakla yükümlüdür. Bu otoriteler yeni kurulabileceği gibi mevcut otoritelerden de seçilebilir. Bununla birlikte şayet birden fazla yetkili otorite atanmışsa, üye devletler bu otoriteler arasından bir "veri koordinatörü" belirlemelidirler. Veri koordinatörü, otoriteler arasındaki iş birliğini kolaylaştırmak ve Yasa'nın uygulanmasıyla ilgili konularda ilgili taraflara destek sağlamakla yükümlüdür.

Yetkili kılınan otorite ya da otoritelerin görevlerini şu şekilde özetlemek mümkündür:

- **Farkındalık ve Eğitim:** Kullanıcılar ve düzenleme kapsamındaki kuruluşlar arasında veri okuryazarlığını ve düzenlemedeki hak ve yükümlülükler konusunda farkındalığı artırmak.
- **Şikayetlerin Ele Alınması:** İddia edilen ihlallerle ilgili şikayetleri, ticari sırlarla ilgili olanlar da dahil, ele almak ve uygun şekilde soruşturmak.
- **Soruşturmalar:** Bu düzenlemenin uygulanmasıyla ilgili konularda, diğer yetkili otoritelerden veya kamu otoritelerinden alınan bilgiler temelinde de dahil olmak üzere, soruşturmalar yürütmek.
- **Yaptırımlar:** Etkili, orantılı ve caydırıcı mali cezalar uygulamak veya para cezalarının uygulanması için yasal işlemleri başlatmak.
- **Teknolojik ve Ticari Gelişmelerin İzlenmesi:** Veri sağlanması ve kullanımıyla ilgili teknolojik ve ticari gelişmeleri izlemek.
- **Ulusal ve Uluslararası İş Birliği:** Diğer üye devletlerin yetkili otoriteleriyle ve gerektiğinde Komisyon veya Avrupa Veri İnovasyon Kurulu (EDIB) ile iş birliği yaparak, düzenlemenin tutarlı ve etkili bir şekilde uygulanmasını sağlamak.

[25] Siglmüller, s. 116 vd.

- **Sektörel Otoritelerle İş Birliği:** Diğer AB veya ulusal yasal düzenlemelerin uygulanmasından sorumlu otoritelerle, özellikle veri ve elektronik iletişim hizmetleri alanındaki otoritelerle ve GDPR'ın uygulanmasını denetleyen gözetim otoriteleriyle iş birliği yapmak.
- **Veri İşleme Hizmet Sunucularıyla İlgili İş Birliği:** Veri işleme hizmeti sağlayıcılarına uygulanabilir diğer AB yasaları ve öz düzenlemelerle uyumlu olarak, 23 ila 31. Maddeler ve 34 ve 35. Maddelerin tutarlı bir şekilde uygulanmasını sağlamak için ilgili yetkili otoritelerle iş birliği yapmak.

Otoriteler için getirilen düzenlemelere ilaveten Yasa, veri koordinatörüne ilişkin de ek görevler öngörmektedir. Bu bağlamda;

- **Tek İrtibat Noktası:** Düzenlemenin uygulanmasıyla ilgili tüm konular için tek irtibat noktası olarak hareket etmek.
- **Veri Taleplerinin Yayınlanması:** Kamu sektörünün olağanüstü ihtiyaç durumlarında veri sağlama taleplerini çevrimiçi olarak kamuya sunmak ve kamu sektörü ile veri sahipleri arasında gönüllü veri paylaşım anlaşmalarını teşvik etmek.
- **Raporlama:** Belirli maddeler uyarınca bildirilen retleri yıllık olarak Komisyona bildirmek.

Otoritelerin ayrıca tarafsız olması gerekmektedir. Gerçekten de yetkili otoriteler, görevlerini yerine getirirken her türlü dış etkiden bağımsız olmalı ve herhangi bir kamu otoritesinden veya özel kişilerden talimat almamalıdır. Ayrıca üye devletler, yetkili otoritelerin görevlerini etkili bir şekilde yerine getirebilmeleri için yeterli insan kaynağı, teknik kaynak ve uzmanlıkla donatılmasını sağlamakla yükümlü kılınmaktadır.

Nihayet Veri Yasası, ilgili yükümlülüklere tabi olup da Birlik sınırları dışında mukim olanlar açısından temsilci atama yükümlülüğü öngörmektedir. Bu sayede yetkili otoriteler, ürün ya da hizmeti sunan kişiye ilaveten doğrudan muhatap olabilecekleri bir kişiye başvurabilecektir. Temsilci, otoritelerle yakın bir işbirliği içerisinde bulunacak ve Veri Yasası'nda öngörülen yükümlülüklere riayet edildiğine ilişkin bütün önlemlerin belgelenebilmesi amacıyla gerekli desteği sağlayacaktır. Bir diğer ifade ile temsilci, hesap verilebilirlik ilkesine hizmet etmek amacıyla AB dışında mukim olan üretici ya da hizmet sağlayıcının Birlik içerisindeki yardımcısı olacaktır.

b. Yaptırımlar

AB mevzuatında yürürlükte olan birçok düzenlemenin aksine Veri Yasası, öngörülen yükümlülüklerin ihlali halinde doğrudan herhangi bir yaptırım mekanizması öngörmemektedir. Bunun yerine Art. 40 f.

1 üye devletlere yaptırımları belirleme yükümlülüğü getirmekte, bu bağlamda da söz konusu yaptırımların etkili, orantılı ve caydırıcı olması gerektiğine işaret etmekle yetinmektedir.

Anlaşıldığı kadarıyla Veri Yasası, halihazırda özel hukuk sözleşmelerini, Yasa kapsamında öngörülen amaçlara ulaşabilmek için bir araç olarak değerlendirdiği için yükümlülüklerin ifası noktasında da yine özel hukuk enstrümanları önem kazanacaktır. Şöyle ki Art. 38 ve 39 hükümleri uyarınca Veri Yasası yükümlülüklerine riayet etmeyen aktörlere karşı ilgili kişilerin yetkili otoritelere şikâyette bulunma ve yargı yollarına başvurma imkanları mevcuttur. Dolayısıyla asıl yaptırımlar, devlet-birey arasındaki dikey ilişkiden çok bireyler arasındaki yatay ilişkide önem kazanacak, bu bağlamda ise özellikle haksız rekabet hukuku ve borçlar hukuku önem kazanacaktır. Nitekim Veri Yasası'nda öngörülen yükümlülüklerine riayet etmeyen üreticiler bir yandan haksız ticari uygulamalarda bulunmuş sayılacak, diğer taraftan satış sözleşmesi çerçevesinde ayıplı ürün ya da hizmet sunmaları sebebiyle sorumlu tutulacaktır.

C. AB Veri Yönetişimi Yasası (Data Governance Act)

Verinin önemi gerek ekonomik açıdan gerekse toplumsal açıdan arttıkça veriye erişim de önem kazanmaktadır. Yeteri kadar veriye erişimi olmayan aktörler, veri ekonomisinde dezavantajlı bir konuma sahiptirler[26]. Dolayısıyla özellikle KOBİler ve girişimcilerin de veriye erişim noktasında fırsat eşitliğine sahip olduğu bir düzene ihtiyaç duyulmakla birlikte, aynı zamanda veriye erişim bağlamında tarafsızlığın, veri taşınabilirliğinin ve birlikte çalışabilirliğin güvence altına alınması da gerekmektedir. Bu doğrultuda Veri Yönetişimi Yasası, işlevsel ve rekabetçi bir veri ekonomisi oluşturmayı, buna engel olacak unsurları bertaraf etmeyi ve verinin altruistik saiklerle paylaşımını teşvik etmeyi amaçlamaktadır.

Belirtildiği üzere Veri Yönetişimi Yasası, AB'nin veri stratejisinin önemli bir parçasını oluşturmaktadır. Bu strateji belgesi kapsamında Komisyon, sağlık, mobilite, üretim, finansal hizmetler, enerji, tarım ve iklim gibi alanlarda verilerin ortak kullanımını ve bir araya getirilmesini sağlayacak ortak Avrupa veri alanları oluşturulmasını öngörmektedir. Bu ortak veri alanlarında veriler "bulunabilir, erişilebilir, birlikte çalışabilir ve yeniden kullanılabilir" olmalıdır (İngilizce: "findable, accessible, interoperable and re-usable") – "FAIR ilkeleri"[27].

Genel olarak Veri Yönetişimi Yasası'nın amacı, "bir sınır ötesi dijital iç pazarın gelişimini ve insana odaklı, güvenilir ve güvenli bir veri toplumu ve ekonomisini" teşvik etmektir (Dibace 3). Bu doğrultuda kamu kurumlarının sahip olduğu belirli veri kategorilerinin yeniden kullanımı düzenlenmekte (Bölüm II), veri aracılık hizmetlerinin sunulması için bir yasal çerçeve oluşturulmakta (Bölüm III) ve verileri altruistik amaçlar için sunan kuruluşlara yönelik düzenlemeler getirilmektedir (Bölüm IV). Bunun ötesinde bir Avrupa Veri Inovasyon Kurulu'nun (Bölüm VI) ihdas edilmesi öngörülmekte, ayrıca verilerin uluslararası erişimi ve aktarımına ilişkin düzenlemeler getirmektedir (Bölüm VII).

1. Uygulama Alanı

Veri Yönetişimi Yasası'nın uygulama alanını düzenleyen Art. 1 hükmü çerçevesinde Yasanın amaçlarını dört ana başlık altında toplamak mümkündür. Bunlar;

> -Birlik içerisindeki kamu kurumlarının elinde bulunan belirli veri kategorilerinin yeniden kullanım koşullarını düzenlemek;
>
> -Veri aracılık hizmetlerinin sunulması için bir kayıt ve denetim çerçevesi oluşturmak;

[26] Veri Yönetişimi Yasası, Dibace No. 2.
[27] Veri Yönetişimi Yasası, Dibace No. 2.

-Altruistik amaçlar doğrultusunda sunulan verileri toplayan ve işleyen kuruluşların gönüllülük esasına dayalı olarak kaydolabilecekleri bir çerçeve oluşturmak;

-Avrupa Veri İnovasyon Kurulu'nun kurulması için bir çerçeve oluşturmak.

Her ne kadar veri ekonomisi açısından kamunun elinde bulundurduğu verilerin yeniden kullanımı büyük bir önem arz etse ve Veri Yönetişimi Yasasının temel amaçlarından birisini teşkil etse de, Art. 1 f. 2 hükmü Veri Yönetişimi Yasası'nın kamu kurumlarına verilerin yeniden kullanımına müsaade edilmesi hususunda bir zorunluluk getirmediğini, hatta bu kurumların diğer kanunlardan kaynaklanan gizlilik yükümlülüklerinin saklı kalacağını belirtmektedir. Dolayısıyla Yasa, kamu kurumlarına verilerin paylaşılması noktasında bir yükümlülük getirmemekte, dolayısıyla bireylere de bu doğrultuda bir hak bahşetmemektedir. Ayrıca kişisel verileirn korunmasına ilişkin düzenlemeler ile sektör özelinde veri paylaşımına ilişkin getirilen düzenlemeler de yine saklı tutulmuştur. Bu bağlamda da, tıpkı Veri Yasası'nda olduğu gibi, Veri Yönetişimi Yasası'nın kişisel verilerin işlenmesi için bir yasal dayanak teşkil etmeyeceği ve GVKT, kamu kuruluşlarının kişisel veri işlemesine ilişkin Tüzük ((AB) 2018/1725) ile e-Privacy Direktifi'nden kaynaklanan hak ve yükümlülüklerin saklı olduğu belirtilmektedir. Keza rekabetin korunmasına ilişkin hükümler de saklı tutulmuştur.

Son olarak üye devletlerin kamu güvenliği, ulusal savunma ve ulusal güvenlik alanlarındaki faaliyetleri ile ilgili yetkileri de saklı tutulmuştur.

Veri Yönetişimi Yasası'nda ayrıca birçok tanıma yer verilmektedir. Bu tanımlar Veri Yasası'nda yer verilen tanımlarla da birebir örtüşmemektedir. Söz konusu tanımlar, ilgili bölümlerde etraflıca incelenecektir.

2. Kamunun Elinde Bulundurduğu Verilerin Yeniden Kullanıma Sunulması

a. Art. 3: Yeniden Kullanıma Tabi Olan Veri Kategorileri

Veri Yönetişimi Yasası Bölüm II kapsamında kamunun "sahibi olduğu" belirli veri kategorilerinin yeniden kullanımını düzenlemektedir. Bu bağlamda yeniden kullanım, Art. 2 f. 2 hükmünde, kamu kurumlarının elinde bulundurduğu verilerin gerçek veya tüzel kişiler tarafından ticari veya ticari olmayan amaçlarla, verinin kamusal görev kapsamında elde edilme amacından farklı amaçlarla kullanılmasını ifade etmekle birlikte, farklı kamu kurumlarının münhasıran kendi görevlerini ifa etmek amacıyla aralarında gerçekleştirdikleri veri paylaşımları bu tanım dışında kalmaktadır. Görüldüğü üzere burada esas olan, kamu kuruluşunun veriyi hangi görevi çerçevesinde elde ettiğinin belirlenmesi ve

yeniden kullanımdan bahis açabilmek için bu verinin artık yeni ve ilk amaçtan farklı bir amaç için işlenmesidir.

Belirtildiği üzere Birlik hukukunda halihazırda "açık veri" konusunda düzenlemeler mevcuttur. Zira açık veri, 2003/98/EC sayılı Direktif ile 2013/37/EU sayılı Direktiflerin yerine yürürlüğe giren ve kısaca PSI-Direktifi (public sector information) olarak bilinen EU 2019/1024 sayılı Açık Veri ve Kamusal Verinin Yeniden Kullanımına İlişkin Direktif (Açık Veri Direktifi) ile düzenlenmiştir. Bununla birlikte Açık Veri Direktifi, hukuki açıdan korunan verileri kapsamadığı için yetersiz kalmış, beklenen etkiyi oluşturamamıştır. Buradan hareketle Veri Yönetişimi Yasası, Bölüm II Art. 3 kapsamında öncelikle kamunun elinde bulundurduğu ve farklı hukuki rejimler vesilesiyle korunan verilerin yeniden kullanım amacıyla paylaşılmasını esas almaktadır.

Buradan hareketle kamunun elinde bulundurduğu ve yeniden kullanım amacıyla paylaşıma sunabileceği veriler, işyeri sırrı, mesleki sır ya da şirket sırrı da dahil olmak üzere her türlü ticari sır olarak, istatistiksel sır olarak, üçüncü kişilerin fikri mülkiyet hakları çerçevesinde ve kişisel verilerin korunması hukuku çerçevesinde korunan verilerdir. Nitekim Açık Veri Direktifi'nin uygulanması noktasında özellikle muhtelif hukuki sebeplerle korunan verilerin paylaşılması hususunda sorunlar yaşanmıştır. Buradan hareketle Veri Yönetişimi Yasası, kamunun elinde bulundurduğu ve belirtilen kategoriler dahilinde korunan verilerin yeniden kullanım amacıyla paylaşılması konusunu esas almaktadır[28].

Öncelikle ticari sır, 2016/943 (EU) Ticari Sır Direktifi Art. 1 f. 2 kapsamında know-how da dahil olmak üzere tanımlanan bilgilerdir. Bu tür bilgiler, tıpkı diğer veri kategorilerinde olduğu gibi, PSI-Direktifi kapsamına dahil edilmemişti. İstatistiksel sır ise kamunun istatistik toplama faaliyetleri bağlamında elde edilen ve sır niteliğini haiz olan bilgileri kapsamaktadır. Fikri mülkiyete ilişkin haklar ise üçüncü kişilere ait olan haklardır. Bu bağlamda da yine PSI-Direktifinin aksine fikri hakların da kullanımına müsaade edilmesi amaçlanmakta, bu bağlamda kamunun çeşitli imkanlar dahilinde bu verileri de yeniden kullanıma sunabilmesi için bir çerçeve oluşturulmaya çalışılmaktadır. Bu bağlamda "Edebiyat ve Sanat Eserlerinin Korunmasına İlişkin Bern Sözleşmesi, Ticaretle Bağlantılı Fikri Mülkiyet Anlaşması (TRIPS) ve Dünya Fikri Mülkiyet Örgütü Telif Hakları Anlaşması (WIPO Telif Hakları Anlaşması – WCT) ile Birlik ve ulusal hukuk düzeyindeki mevzuat önem kazanmaktadır. Son olarak kişisel verilerin korunmasına ilişkin mevzuat kapsamında kamunun elinde bulundurduğu kişisel verilerin yeni bir amaç için kullanılması halinde Veri Yönetişimi Yasası'nın ilgili hükümleri dikkate alınacaktır.

[28] Veri Yönetişimi Yasası, Dibace No. 6.

Bununla birlikte Art. 3 f. 2'de önemli istisnalar mevcuttur. Nitekim kamu iştiraki niteliğindeki teşebbüsler, kamuya ait radyo-televizyon kuruluşlar ile kültür ve eğitim amaçlı kamu kuruluşlarının elinde bulundurduğu verileri Veri Yönetişimi Yasası'nın kapsamına dahil edilmemiştir. Aynı şekilde kamu güvenliği, ülke müdafaası ve ulusal güvenlik sebeplerine dayalı olarak korunan kamu verileri ile ilgili kamu kurumunun kamu menfaati amacı çerçevesinde elde ettiği verilerin dışında kalan (örnek olarak kamu kurumunun personeline ilişkin veriler) kapsam dışında kalmıştır.

b. Yeniden Kullanıma İlişkin Usul ve Esaslar

aa. Münhasırlık Sözleşmelerinin Yasaklanması

Kamunun elinde bulundurduğu verilerin herkese açık olması amacından hareketle Art. 4, kamunun elinde bulundurduğu verilerin münhasıran belirli bir kişi tarafından kullanımına ilişkin sözleşmeleri ve bu etkiyi doğuracak diğer her türlü eylemi yasaklamaktadır. Dolayısıyla kamu kurum ve kuruluşları, Art. 3 bağlamında düzenlenen veri kategorilerine yeniden kullanım amacıyla erişim sundukları durumlarda bu verilerin diğer kişilerce de kullanımına müsaade etmeli, bu verilerin münhasıran sınırlı bir çevre tarafından kullanımına ilişkin her türlü eylemden imtina etmelidir. Bu bağlamda sadece sözleşmeler değil, söz konusu etkiye sebebiyet verecek her türlü idari işlem de bu yasak kapsamına dahil edilmektedir.

Bu yasağın istisnası ise ancak kamu menfaatine hizmet eden bir hizmetin ya da bir ürünün sunulması için gerekli olduğu ve münhasırlık sözleşmesine alternatif bir yöntemin bulunmadığı durumlarda söz konusu olacaktır. Ancak söz konusu istisna hallerinde de yine de şeffaflık, eşit davranma ve ayrımcılık yasağı ilkelerinin dikkate alınmalı, ayrıca münhasırlık süresinin 12 ayı geçmemesi gerekmektedir. Ayrıca istisnaya ilişkin gerekçenin internette erişilebilir bir şekilde şeffaf olarak kamuya sunulması gerekmektedir.

Yukarıda belirtilen şartlara aykırılık teşkil eden her türlü sözleşme ve idari işlem geçersiz sayılacaktır.

bb. Yeniden Kullanım Şartları

Kamunun elinde bulundurduğu verilerin yeniden kullanımı için öngörülen şartlar, Art. 5 ve devamındaki hükümlerde genel olarak düzenlenmektedir.

Bu bağlamda öncelikle sürece dahil olan aktörleri tanımlamak gerekecektir. Bunların başında Art. 3 kapsamında öngörülen veri kategorilerini yeniden kullanım amacıyla kişilerin erişimine sunmak isteyen kamu kurum ve kuruluşları gelmektedir. Söz konusu kamu kurum ve kuruluşları, yeniden kullanımın şartları ve sürece ilişkin bilgileri önceden şeffaf bir şekilde ilan etmelidirler. Bu ilan, Art. 8'de

düzenlenen ve "merkezi bilgi noktası" (single information point) olarak nitelendirilen yetkili merci nezdinde gerçekleşecektir.

Merkezi bilgi noktası, Art. 8'e göre yeniden kullanım süreci bağlamında bütün usul ve esaslara ilişkin bilgilerin şeffaf ve kolayca ulaşılabilir bir şekilde bulundurulduğu bir mercidir. Bu bağlamda üye devletler, yeni bir kurum ihdas edebilecekleri gibi halihazırda mevcut bir kurum bünyesinde de böyle bir müesseseyi kurabilecektir. Merkezi bilgi noktası, yeniden kullanıma ilişkin talepleri almak ve bunları Art. 7 çerçevesinde öngörülen yetkili birimlere iletmekle görevlidir. Ayrıca merkezi bilgi noktası, erişime sunulan bütün verileri, veri formatları ve verinin hacmine ilişkin bilgiler de dahil olmak üzere ilgililere sunmalıdır.

Art. 7 bağlamında yetkili kurum ise veriyi yeniden kullanıma sunmak isteyen kamu kurum ve kuruluşlarını bu kapsamda destekleyen kuruluşlar olarak nitelendirilmektedir. Bu bağlamda da yeni bir kurumun ihdas edilmesi ya da mevcut bir ya da birden çok kurumun söz konusu vazife ile yetkilendirilmesi mümkün olacaktır. Destek faaliyeti ise Art. 7 f. 4 bağlamında erişimin mümkün kılınması amacıyla teknik destek, verilerin sınıflandırılması bağlamında teknik destek, verilerin maskelenmesi, anonimleştirme ya da diğer şekilde mahremiyetin korunmasına ilişkin önlemler bağlamında teknik destek, gerektiğinde açık rıza temin edilmesi için destek şeklinde örneklendirilmektedir.

Art. 3 kapsamında öngörülen veri kategorilerini yeniden kullanım amacıyla erişime sunmak isteyen kamu kurumları, yeniden kullanım şartları ve sürece ilişkin bilgileri merkezi bilgi noktası üzerinden ilan ettikten sonra kişiler, öncelikle merkezi bilgi noktası üzerinden taleplerini iletecek, bu talep, Art. 7 bağlamında yetkili kurum tarafından ilgili kamu kurumuna iletilecek, gerekli olduğu takdirde yetkili kurum, ilgili kamu kurumuna destek sağlayacak ve nihayet ilgili kurum talep hakkında karar verecek, olumlu karar halinde verileri ilgili kişiye merkezi bilgi noktası üzerinden sunacak, olumsuz karar verilmesi durumunda ise bu kararını yine talepte bulunan kişiye merkezi bilgi noktası üzerinden iletecektir.

Yeniden kullanıma sunulacak olan veri kategorilerine ilişkin kullanım şartları ise Art. 5 f. 2 hükmünde somutlaştırılmaktadır. İlgili düzenlemeye göre yeniden kullanım şartları, veri kategorileri, yeniden kullanım amaçları ve yeniden kullanımına izin verilen veri türleri bakımından ayrımcılığa sebebiyet vermeyecek, şeffaf, orantılı ve objektif olarak gerekçelendirilmiş olmalıdır. Aynı zamanda söz konusu şartların rekabeti engellememesi gerekmektedir.

Belirtildiği üzere kamu kurum ve kuruluşlarının Art. 3 kapsamında verileri yeniden kullanım amacıyla erişime sunması, onları hukuki koruma yükümlülüklerinden muaf tutmamaktadır. Bilakis ilgili kurum ve kuruluşlar, erişime sundukları verilerin korunmasını erişime sunmaları halinde dahi muhafaza etmekle yükümlüdür. Bu bağlamda ilgili kurum ve kuruluşların Art. 5 f. 3'e göre aşağıdaki önlemleri öngörebilmektedir:

a) Verilerin yeniden kullanımının münhasıran aşağıdaki hallerle sınırlandırılması:

i) Kişisel veriler söz konusu olduğunda veriler anonim hale getirilmeli

ii) Ticari sırlar, ticari gizli bilgiler veya fikri mülkiyet hakları ile korunan içerikler, modifiye etme, birleştirilme ya da işleme gibi çeşitli ifşa kontrolü yöntemleri kullanılarak sunulmalı;

b) Verilere erişim ve yeniden kullanım, kamu kurumu tarafından sağlanan veya kontrol edilen güvenli bir işleme ortamında uzaktan erişim yoluyla gerçekleştirilmeli

c) Uzaktan erişimin üçüncü kişi haklarını tehlikeye atmadan gerçekleştirilmesi mümkün olmadığı durumlarda verilere erişim ve yeniden kullanım, güvenli işleme ortamının bulunduğu fiziksel alanlarda yüksek güvenlik standartlarına uygun olarak sağlanmalıdır.

Öngörülen önlemlere rağmen hale erişime sunulan verilerin amaca aykırı şekilde kullanımı gündeme gelebilecekse kamu kurumu ayrıca ilgili kişilerden "gizlilik taahhüdü" vermelerini şart koşabilecektir. Alınan bütün önlemlere ve gizlilik taahhütlerine rağmen kişisel veriler söz konusu olduğu ve veri işleme sebebinin bulunmadığı durumlarda ise ilgili kamu kurumu ilgili kişilerden açık rıza temin edilmesi için kullanım talebinde bulunan kişileri destekleyebilecektir.

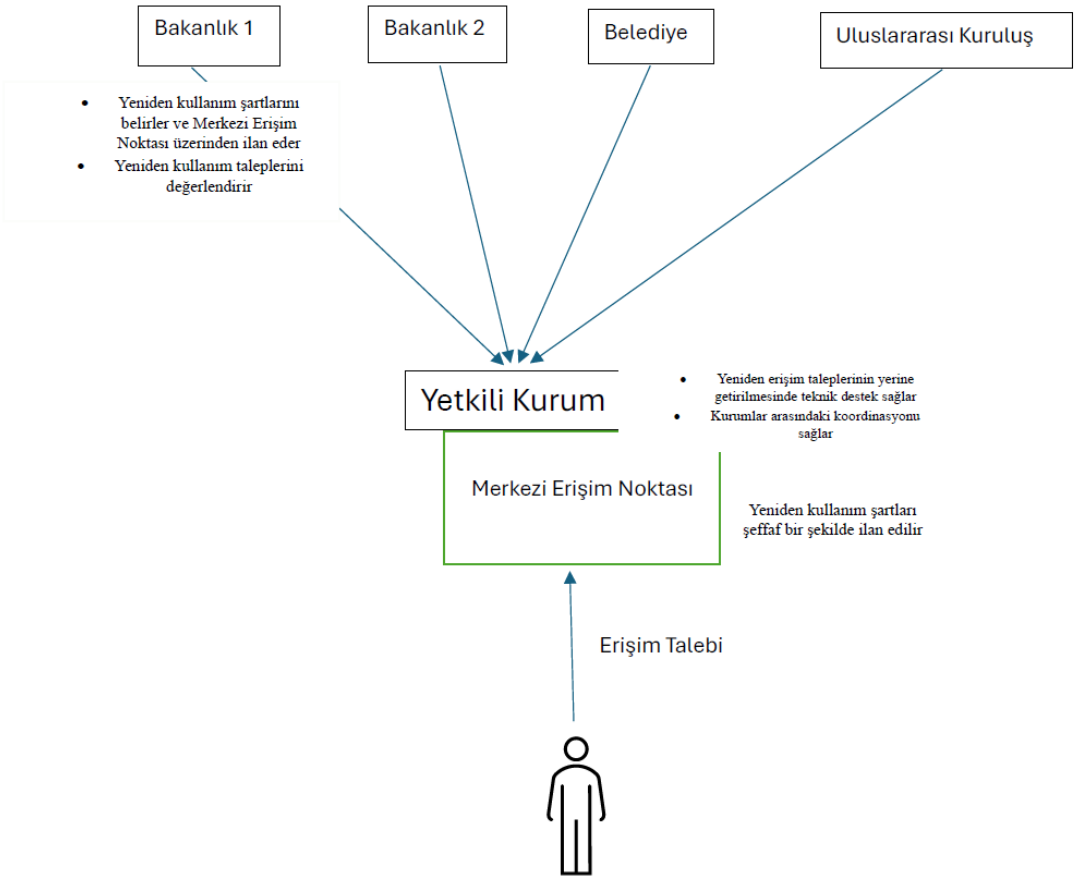
Kamu kurum ve kuruluşları tarafından erişime sunulan verilerin ilgili kişiler tarafından Birlik dışında üçüncü ülkelere aktarımı halinde ise öncelikle erişim talep eden kişinin bu durumu ilgili kamu kurumuna bildirmesi gerekmektedir. Ayrıca söz konusu verilerin üçüncü ülkelere aktarımı için talepte bulunan tarafın bazı sözleşmesel taahhütlerde bulunması gerekmektedir. Her ne kadar bu şartlar, an itibariyle Veri Yönetişimi Yasası Art. 5 f. 10 kapsamında genel hatlarıyla belirtilmiş olsa da, yakın zamanda tıpkı GVKT bağlamında olduğu gibi standart sözleşme hükümlerinin Komisyon tarafından çıkartılması ve bu standart sözleşme hükümlerine göre verilerin üçüncü ülkelere aktarımına müsaade edilmesi gündeme gelecektir.

Kamu kurum ve kuruluşları, ellerinde bulundurdukları verilerin yeniden kullanıma sunulması için belirli bir ücret talep edebilecektir. Söz konusu ücretin, şeffaf, ayrımcılığa sebebiyet vermeyecek

nitelikte, orantılı ve objektif olarak gerekçelendirilebilir nitelikte olması gerekmektedir. Bununla birlikte ticari amaç gütmeyen araştırma kuruluşları ya da KOBİler ve girişim şirketleri için daha düşük ücret öngörülmesi ya da bunların bütünüyle ücret ödemekten muaf tutulması da mümkün kılınmaktadır.

Ücretin belirlenmesi noktasında Art. 6 f. 3'e göre dikkate alınması gereken kıstaslar, başvuru sürecinin yürütülmesi için meydana gelen maliyetlerden müteşekkildir. Bunlar özellikle verilerin çoğaltılması, sağlanması ve paylaşılması için yapılan masraflar, telif ödemelerine ilişkin masraflar, anonimleştirme ve benzer veri işleme süreçlerine ilişkin masraflar, güvenli bir işleme ortamının bakımının sağlanması için yapılan masraflar, gerekli izin ve rızaların alınması için yapılan masraflar şeklindedir.

Nihayet veriye erişim talebinin en geç iki ay içerisinde cevaplandırılması gerekmektedir. Bu süre, talebin kapsamı ve karmaşıklığı dikkate alınmak suretiyle asgari olarak 30 gün daha uzatılabilmektedir.



3. Aracı Veri Hizmeti Sağlayıcılarına İlişkin Düzenlemeler

Veri Yönetişimi Yasası Bölüm III kapsamında aracı veri hizmeti sağlayıcılarına ilişkin düzenlemeler bulunmaktadır. Bu aktörler, verinin birden fazla kişi tarafından kullanılabilmesi açısından önemli bir konuma sahiptirler. Nitekim aracı veri hizmeti sağlayıcıları, veriyi kullandırmak isteyen ile veriyi kullanmak isteyen taraflar arasındaki ilişkiyi kuran, bu sayede veriye tedavül niteliği kazandıran aktörlerdir. Bu sebeple söz konusu müessesenin özel olarak düzenlenmesi, bu vesileyle aracı veri hizmeti sağlayıcılarına ilişkin güvenin tesis edilmesi ve veri paylaşımının öngörülen güvenli ortamda teşvik edilmesi amaçlanmaktadır.

Bölüm III, öncelikle aracı veri hizmet sağlayıcılarını tanımlamakta, ardından bu aktörlere ilişkin bir bildirim mekanizması öngörmektedir. Akabinde aracı veri hizmeti sağlayıcılarının uyması gereken yükümlülükler düzenlenmekte ve nihayet bunların denetimine ilişkin hükümlere yer verilmektedir.

Sistematik açıdan dikkat edilmesi gereken ve hemen bu aşamada belirtilmesi lazım gelen husus, aktörlerin bildirim yükümlülüğü esnasında Veri Yönetişimi Yasasında öngörülen faaliyet şartlarının yerine getirilip getirilmediğine ilişkin herhangi bir denetim yapılmamasına ilişkindir. Bu aşamada risk temelli yaklaşım ve hesap verilebilirlik ilkelerinin tezahürünü görmek mümkündür. Bu husus ilerleyen aşamalarda daha etraflıca açıklanacaktır.

a. Aracı Veri Hizmeti Sağlayıcıları Kavramı ve Örnekler

Aracı veri hizmeti sağlayıcı kavramı öncelikle Art. 2 Nr. 11 bağlamında tanımlanmaktadır. Bu tanımdan hareketle de Art. 10 kapsamında aracı veri hizmeti sağlayıcılarının hangi faaliyetleri bağlamında Bölüm III hükümlerine tabi olacakları düzenlenmektedir.

Öncelikle Art. 2 Nr. 11 çerçevesinde verilen tanıma bakıldığında aracı veri hizmet sağlayıcısı, bir yanda belirsiz sayıda ilgili kişi veya veri sahibi ile diğer tarafta veri kullanıcıları arasında ticari ilişki kurmasına olanak tanıyan; teknik, hukuki veya diğer araçlar vesilesiyle ortak veri kullanımını, özellikle kişisel verilerle ilgili olarak ilgili kişilerin haklarını kullanmalarını sağlamak amacıyla anılan ticari ilişkinin kurulmasını sağlayan bir hizmet olarak tanımlanmaktadır. Bununla birlikte tanım aynı madde içerisinde daraltılmaktadır. Nitekim aracı veri hizmeti sağlayıcısı tanımına aşağıdaki faaliyetler dahil edilmemektedir:

> a) Taraflar arasında herhangi bir ticari ilişki kurmaksızın, verilerin veri sahiplerinden alınıp toplanması, zenginleştirilmesi veya dönüştürülmesi yoluyla değerinin önemli ölçüde artırılması ve sonucunda oluşan verilerin kullanım lisanslarının veri kullanıcılarına verilmesi;

b) Odak noktası telif hakkıyla korunan içeriklerin aracılığını yapan hizmetler;

c) Yalnızca bir veri sahibi tarafından, kendisine ait verilerin kullanımını sağlamak amacıyla kullanılan veya tedarikçi-müşteri ilişkileri veya sözleşmeye dayalı işbirlikleri de dâhil olmak üzere, kapalı bir grup içindeki birden fazla tüzel kişi tarafından kullanılan hizmetler; özellikle Nesnelerin İnterneti (IoT) ile ilgili nesne ve cihazların işlevlerini güvence altına almayı amaçlayan hizmetler;

d) Kamu kurumları tarafından iş ilişkisi kurma amacı olmaksızın sunulan veri aracı hizmetleri.

Görüldüğü üzere tanım son derece geniştir. Bununla birlikte halihazırda Yasa içerisinde belirli sınırlamalara yer verilmiştir. Örnek olarak Dibace No. 28 kapsamında bulut bilişim hizmetleri, analiz hizmetleri, ortak kullanım amaçlı yazılımlar, web tarayıcıları, e-mail hizmetleri, kullanıcılar arasında ticari ilişki kurmaya yönelik olmadıkları için kapsam dışında olarak değerlendirilmektedir.

Ayrıca verilen tanımda yine tanımlamaya muhtaç başka kavramlar da mevcuttur. Bu bağlamda özellikle veri sahibi ile veri kullanıcısı kavramlarının açıklığa kavuşturulması gerekmektedir. Art. 2 Nr. 8'e göre veri sahibi, "erişim ya da paylaşıma konu olan veriler açısından ilgili kişi olmayan, Birlik hukuku ve ulusal mevzuat uyarınca belirli kişisel veya kişisel olmayan verilere erişim sağlama veya bu verileri paylaşma yetkisini haiz olan tüzel kişi, kamu kurumları, uluslararası organizasyonlar ya da gerçek kişiler olarak tanımlanmaktadır. Veri kullanıcısı ise Art. 2 Nr. 9'a göre belirli kişisel veya kişisel olmayan verilere hukuki erişim yetkisi olan ve kişisel verilerin söz konusu olduğu hallerde özellikle GVKT uyarınca bu verileri ticari veya ticari olmayan amaçlarla kullanma yetkisine sahip gerçek veya tüzel kişiler olarak tanımlanmaktadır. Her iki tanımda da dikkat çeken nokta erişim ve paylaşım yetkisinin hukuki bir zemine dayanmasıdır. Bir diğer ifade ile Bölüm III kapsamında yükümlülük altında olan veri hizmeti sağlayıcıları, ancak hukuka uygun veriye erişim ve paylaşım hallerini kapsamakta, buna karşılık hukuka aykırı veriye erişim ve paylaşım halleri kapsam dışında kalmaktadır. Bu durum ise ciddi bir eksiklik olarak eleştirilmektedir[29].

Veri sahibi ve veri alıcısı tanımlarından hareketle Veri Yasası Art. 10, her türlü aracı veri hizmeti sağlayıcısı faaliyetini değil, bunların belirli faaliyetlerini esas almaktadır. Bu hizmetler şu şekilde tanımlanmaktadır:

a) Veri sahipleri ile potansiyel veri kullanıcıları arasında, söz konusu hizmetlerin sağlanabilmesi için gerekli teknik veya diğer araçların sağlanması da dâhil olmak üzere, aracılık hizmetleri; bu

[29] Borges, Borges/Keil, Big Data, 2024, § 5 Rn. 218.

hizmetlere ayrıca verilerin iki veya çok taraflı değişimi, veri değişimi veya ortak kullanımı sağlamak üzere platform veya veri tabanlarının oluşturulması, ayrıca veri sahipleri ile veri kullanıcılarının birbirine bağlanması için özel altyapıların kurulması da dâhildir;

b) Kendi kişisel verilerini erişilebilir kılmak isteyen ilgili kişiler veya kişisel olmayan verileri erişilebilir kılmak isteyen gerçek kişiler ile potansiyel veri kullanıcıları arasında, söz konusu hizmetlerin sağlanabilmesi için gerekli teknik veya diğer araçların sağlanması da dâhil olmak üzere, aracılık hizmetleri; özellikle, ilgili kişilerin GVKT bağlamında tanınan haklarını kullanmalarının sağlanması;

c) Veri kooperatiflerinin hizmetleri.

Görüldüğü üzere aracı veri hizmeti sağlayıcının iki taraf arasında ticari bir ilişki kurmayı amaçlaması gerekmektedir. Buradan hareketle verileri toplayıp gerektiğinde işleyen, bunları başka verilerle eşleştiren ya da zenginleştiren ve akabinde üçüncü kişilere kendi adı altında sunan veri brokırları bu tanımın dışındadır. Buna karşılık çeşitli taraflar arasında aracılık hizmeti sunan, verilerin satışa sunulduğu ve alıcıların da buradan veri temin edebildiği veri pazar yerleri uygulama alanına dahildir. Veri sahipleri ile veri alıcıları arasında koordinasyon sağlamayı amaçlayan müesseseler de uygulama alanına dahildir. Bunlar özellikle Mobility Data Space[30], Gaia-X projesi ve bu bağlamda otomotiv sektörüne mahsus olan Catena-X projeleri[31] olarak örneklendirilebilecektir. Veri kooperatiflerinden kasıt ise farklı kişilerin bir araya gelip ellerinde bulundurdukları veriden gelir elde etmek amacıyla kurdukları veri kooperatiflerini esas almakla birlikte, bunların henüz uygulamada yaygın bir örneği bulunmamaktadır.

b. Aracı Veri Hizmeti Sağlayıcılarının Kayıt Süreci

Veri Yönetişim Yasası Art. 11'e göre Art. 10 çerçevesinde tanımlanan faaliyetlerde bulunmak isteyen her aracı veri hizmeti sağlayıcı, aracı hizmetler açısından yetkili kılınan kurum nezdinde kaydolmakla yükümlü kılınmaktadır. Hizmet sağlayıcının birden fazla ülkede faaliyet göstermesi halinde kurulu olduğu yerdeki otorite nezdinde kaydolması öngörülmektedir. Hizmet sağlayıcının Birlik sınırları dışında bulunması halinde ise bir temsilci ataması gerekmektedir.

Aracı veri hizmeti sağlayıcı, kayıt işlemini gerçekleştirdikten sonra Birlik içerisinde faaliyetlerine başlayabilecektir. Bununla birlikte belirtildiği üzere kayıt aşamasında münhasıran Art. 11 f. 6

[30] https://mobility-dataspace.eu/.
[31] Diğer projeler için özellikle bkz. https://gaia-x.eu/who-we-are/lighthouse-projects/.

çerçevesinde öngörülen bilgilerin iletilmesi gerekmektedir. Bir diğer ifade ile ilgili kurum, Art. 12 kapsamında öngörülen gerekliliklerin yerine getirilip getirilmediğini denetlemez. Bilakis kayıt aşamasındaki denetimin kapsamı münhasıran Art. 11 f. 6'da belirtilen bilgilerin sunulmasından ibarettir. Bununla birlikte aracı veri hizmeti sağlayıcı, Veri Yönetişimi Yasası Art. 12'de aracı veri hizmeti sağlayıcıları açısından öngörülen yükümlülüklerin yerine getirildiğini tasdik etmesi amacıyla ilgili kuruma başvurabilecektir. Bu başvuru neticesinde ilgili kurum şartların sağlandığı kanaatine ulaştığı takdirde aracı veri hizmeti sağlayıcıya "Birlik içerisinde tanınan aracı veri hizmeti sağlayıcısı" belgesini sunabilecektir. Ayrıca Komisyona bütün Birlik içerisinde tasdik edilmiş olan aracı veri hizmet sağlayıcılarının kolayca tanınabilmeleri için bir logo çalışması yapacaktır. Kayıt sürecinde ayrıca ilgili kurumların ücret talep edebileceği, ancak söz konusu ücretin de ayrımcılığa sebebiyet vermeyecek şekilde olması gerektiği belirtilmektedir.

Kayıt aşamasında talep edilen ve Art. 11 f. 6 çerçevesinde öngörülen bilgileri ise şu şekildedir:

> a) Veri aracı hizmeti sağlayıcısının adı,
>
> b) Hukuki statüsü, hukuki yapısı, pay sahipleri yapısı, ilgili bağlı kuruluşlar ve veri aracı hizmeti sağlayıcısının bir ticaret sicilinde veya diğer benzer bir kamuya açık ulusal sicilde kayıtlı olması durumunda veri aracı hizmeti sağlayıcısının sicil numarası,
>
> c) Birlik içindeki ana merkez adresi (uygulanabilir ise) ve diğer bir üye devletteki herhangi bir şube veya yasal temsilci adresi,
>
> d) Veri aracı hizmeti sağlayıcısının ve faaliyetlerinin güncel ve tam bilgilerini içeren, en azından a, b, c ve f bentlerinde belirtilen bilgileri kapsayan halka açık bir web sitesi,
>
> e) Veri aracı hizmeti sağlayıcısının iletişim kişileri ve iletişim bilgileri,
>
> f) Veri aracı hizmeti sağlayıcısının sunmayı amaçladığı veri aracı hizmetinin tanımı ve bu veri aracı hizmetinin Madde 10'da belirtilen kategorilerden hangisine girdiğine dair bilgi,
>
> g) Faaliyetin başlama günü kayıttan farklı bir gün ise, tahmini başlama tarihi.

c. Aracı Veri Hizmet Sağlayıcısının Yükümlülükleri

Art. 12 çerçevesinde aracı veri hizmet sağlayıcılarının uyması gereken yükümlülükler detaylı bir şekilde düzenlenmiştir. Bunlardan belki de en önemlisi kuşkusuz lit. a)'ya göre amaca bağlılık ilkesiyle alakalıdır. Buna göre aracı veri hizmeti sağlayıcısı, sunduğu veri aracı hizmetleri için elde ettiği verileri veri kullanıcılarına sunmak dışında başka bir amaç için kullanmaz. Ayrıca hizmet sağlayıcı söz konusu

hizmeti, münhasıran bu amaç için kurulmuş olan bir tüzel kişilik vesilesiyle sağlamalıdır. Lock-in etkilerini önlemek amacıyla ayrıca fiyatlandırma noktasında eşit davranılması, özellikle aynı sağlayıcının başka hizmetlerinden istifade edilmesi halinde daha düşük ücret talep edilmesi gibi uygulamalar yasaklanmaktadır.

Aracı veri hizmet sağlayıcının elde ettiği kullanıcı verileri ise ancak sunulan hizmetin sunulması ve geliştirilmesi amaçlarıyla kullanılabilecek, bu bağlamda özellikle dolandırıcılık tespiti veya siber güvenlik amacıyla veri kullanımını gündeme gelecektir. Elde edilen verinin farklı formatlara dönüştürülmesi ise ancak birlikte çalışılabilirlik açısından gerekli olduğu takdirde gündeme gelecektir. Genel olarak aracı veri hizmeti sağlayıcının birlikte çalışabilirliği sağlayabilmek için gerekli önlemleri alması da öngörülmektedir. Ayrıca birlikte çalışılabilirlik sebebiyle aracı veri hizmeti sağlayıcının, özellikle geçici depolama, bakım, dönüştürme, anonimleştirme ve takma adlandırma gibi hizmetleri sunması da mümkündür. Ancak bunun için veri sahibi veya ilgili kişinin açık talebi ya da rızası gerekmektedir. Ayrıca fiyatlar ve ticari koşullar da dahil olmak üzere sunulan hizmete erişim şartları, ilgili kişiler, veri sahipleri ve veri kullanıcıları açısından hem ilgili kişiler hem veri sahipleri hem de veri kullanıcıları açısından adil, şeffaf ve ayrımcılığa sebebiyet vermeyecek nitelikte olmalıdır. Yasa bunun dışında çeşitli teknik ve idari tedbirlere de yer vermektedir.

ç. Aracı Veri Hizmeti Sağlayıcılarının Denetimi

Aracı veri hizmeti sağlayıcılarının kayıt ve diğer yükümlülüklerinin denetimi noktasında üye ülkeler, yetkili bir kurum belirlemelidirler. Ancak bu denetim yetkisi, diğer kurumların yetkilerini etkilemeyecektir. Yetkili kurumun görevleri ve denetimin kapsamı, Art. 14 kapsamında düzenlenmiştir. Art. 14 f. 1'e göre kurumun görevi, veri aracı hizmetlerinin Art. 11 ve 12 kapsamında öngörülen gerekliliklere uyumunu denetlemek ve gözetmektir. Bu bağlamda kurum, denetim görevini yerine getirebilmesi için hizmet sağlayıcılardan gerekli tüm bilgileri talep edebilecektir (Art. 14 f. 2 c. 1). Veri Yönetişi Yasası'na aykırılık tespit eden kurum, bu durumu hizmet sağlayıcısına Art. 14 f. 3'e göre bildirmek ve 30 gün içinde görüş bildirme fırsatı vermek zorundadır. İhlalin tespit edilmesi halinde Art. 14 f. 4'e göre yetkili kurumun önlem alma, özellikle ihlalin giderilmesini talep etme yetkisi öngörülmektedir. Kurumun uygulayacağı yaptırımlar ise her ne kadar sınırları Veri Yönetişimi Yasası'nda belirlenmemiş olsa da para cezası, hizmetin askıya alınması ya da ciddi eksikliklerin giderilmemesi durumunda hizmetin durdurulmasını şeklinde olabilecektir.

d. Gaia-X Projesine Dair Bilgiler

aa. Genel Bakış:

Gaia-X, Avrupa'da veri ekonomisini güçlendirmeyi hedefleyen bir proje olarak ön plana çıkmaktadır. Veri, günümüz ekonomilerinde temel bir kaynak ve rekabet avantajı sağlamaktadır. Ancak, veri paylaşımı ve kullanımı önünde teknik, hukuki ve ekonomik zorluklar bulunmaktadır. Gaia-X, bu engelleri aşmak ve Avrupa'nın dijital egemenliğini artırmak için bir altyapı sunmayı amaçlamaktadır.

Bu bağlamda hukuki engellerin aşılması görevi, Komisyon tarafından çıkartılan yasalar şeklinde ifa edilmektedir. Buna karşılık teknik altyapının ve bilhassa standartizasyon süreçlerinin yürütülmesi görevi ise ilk olarak Almanya ve Fransa'nın teşebbüsleriyle hayata geçirilen, ardından yönetimi özel sektöre bırakılan Gaia-X projesi vesilesiyle gerçekleştirilmektedir.

AB, veri hacminin 2018 yılında 33 ZettaB'den 2025 yılında 175 ZettaB'ye artmasını ve Birlik içerisindeki veri ekonomisinin 301 milyar €'dan 829 milyar €'ya çıkmasını öngörmektedir. Söz konusu öneme binaen veri paylaşımını kolaylaştırmak için bir taraftan hukuki çerçeve sağlanacak, diğer yandan standartlar belirlenecek ve güvenilir bir altyapı oluşturulacaktır. Bu kapsamda özellikle farklı standartların ve eksik altyapının, veri paylaşımı önünde ciddi bir engel teşkil ettiğine işaret edilmekte, hukuki belirsizlikler ile verinin kötüye kullanılmasına dair endişelerin de ilaveten veri paylaşımını olumsuz etkilediği belirtilmektedir.

Bir diğer önemli husus, AB'nin ABD ve Asya merkezli teknoloji devlerine dair bağımlılığını azaltmak ve Avrupa'nın kendi altyapısını oluşturmak suretiyle dijital egemenliğini tesis etmek şeklinde ifade edilmektedir.

bb. Projenin Yapısı ve İşleyişi

Gaia-X projesi hem merkezi bir koordinasyona, hem de yerel ve sektörel bazda oluşturulmuş hublara dayanmaktadır. Projenin koordinasyonu ise Gaia-X European Association for Data and Cloud AISBL tarafından sağlanmaktadır. Altyapı noktasında ise açık kaynak temelli standartların geliştirilmesi, bu sayede şeffaflık ve güven sağlanması amaçlanmakta, katılımcıların söz konusu veri ve veri hizmetlerini önceden belirlenen Avrupa değerlerine uygun şekilde sunmaları öngörülmektedir. Söz konusu ilkeler, AB değerlerine bağlılık, güven ve şeffaflık, birlikte çalışabilirlik, dijital egemenlik ve veri üzerinde hakimiyet olarak tanımlanabilecektir.

cc. Uygulama ve Süreçlerin Ayrıntılı Açıklaması

Gaia-X, Avrupa'nın veri ekonomisini şekillendirmek için bir ekosistem olarak tasarlanmıştır. Projenin uygulama kısmı, federasyonların oluşturulmasından teknik altyapıların uygulanmasına, etik kurallardan standartlaşmaya kadar geniş bir yelpazeyi kapsamaktadır.

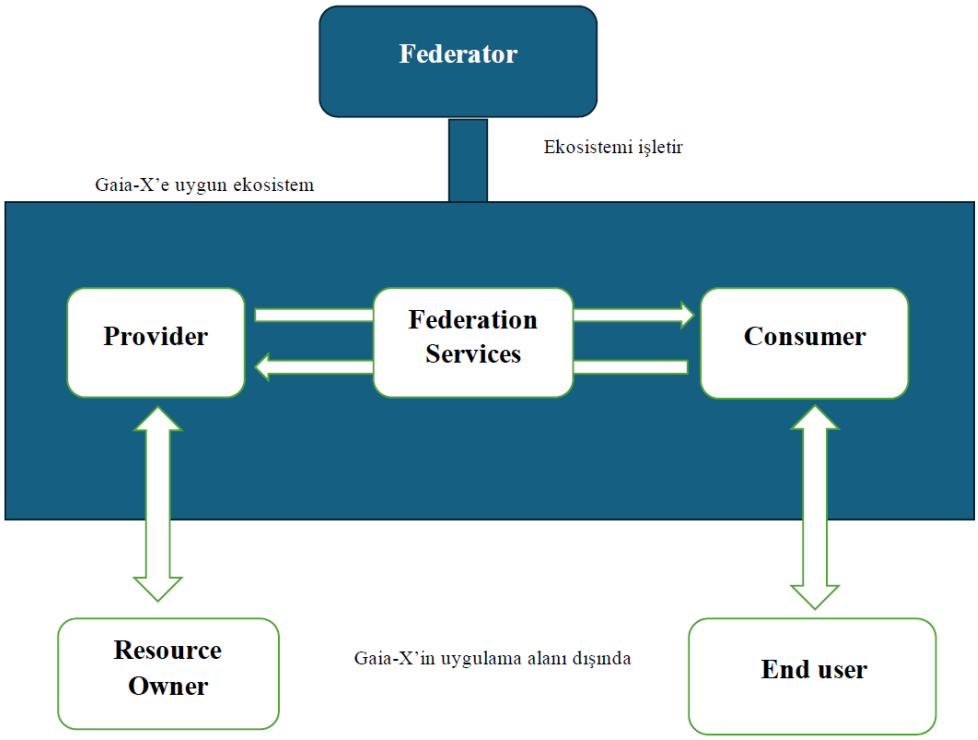
(1) Federasyonların Oluşturulması

Gaia-X'in temel yapısı, federasyonlar olarak adlandırılan işbirliği gruplarına dayanır. Bu federasyonlar, belirli sektörlerde veya veri türlerinde faaliyet göstermek üzere katılımcılar tarafından kurulur.

Federasyondaki aktörler, sağlayıcı (Provider), tüketici (Consumer) ve federasyon yöneticisi (Federator) olarak nitelendirilmektedir. Bu bağlamda sağlayıcı, altyapı, veri ya da hizmet sunan tarafları, tüketici, sağlanan hizmetleri ya da verileri kullanan tarafları ve yönetici ise federasyonun teknik altyapısını yöneten, güvenliği ve kurallara uygunluğu sağlayan aktörler olarak tanımlanabilecektir.

Bu şekilde oluşturulan federasyonda katılımcılar, ortak kurallar çerçevesinde işbirliği yapmaktadır. Öngörülen teknik standartlar, katılımcıların sorunsuz bir şekilde veri alışverişi yapmasını sağlamayı amaçlamaktadır. Her bir federasyon, Gaia-X'in genel kurallarına bağlı kalarak özerk bir şekilde organize edilir.

Söz konusu federasyon projelerine örnek olarak Catena-X, otomotiv sektöründe tedarik zinciri verilerinin paylaşımını standartlaştırır. Bu sayede üreticiler ve tedarikçiler arasında veri alışverişi yapılırken güven ve şeffaflık sağlanır. Bir diğer örnek olarak EuroDaT projesi bağmalında finans sektörü için veri yönetimi ve güvenliğini sağlayan, Avrupa'ya özgü bir altyapı oluşturulmaktadır.

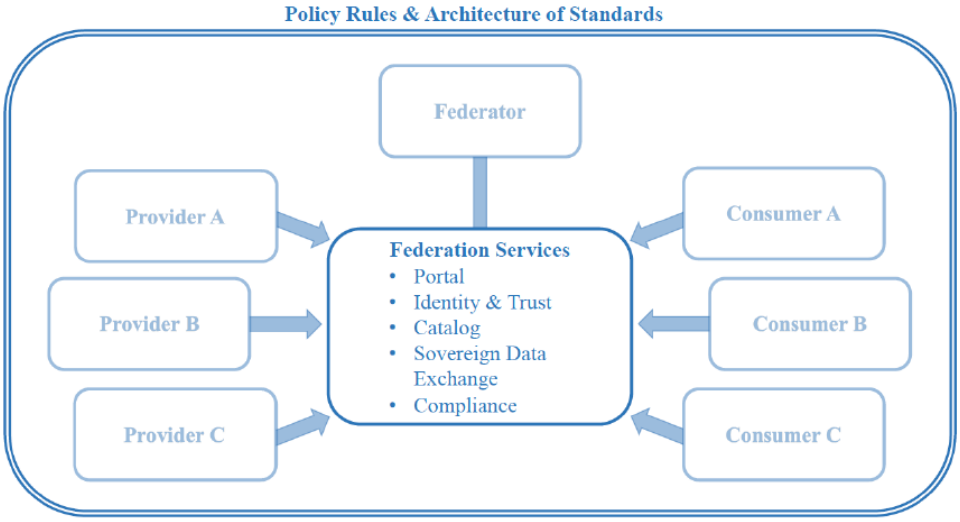


Kaynak: Schütrumpf/Person: Gaia-X: VernetzteInfrastrukturen für eine europäisch geprägteDatenwirtschaft, RDi 2022, s. 281 vd.

(2) Teknik Altyapı: Gaia-X Federasyon Servisleri

Federasyonların çalışabilmesi için bir dizi teknik araç ve altyapı sunulur. Bunlar, Gaia-X'in "Federation Services" adı verilen hizmetler setiyle sağlanır. Bu çerçevede kimlik ve güven, verinin takip edilebilirliği ve uyumluluk kontrolleri şeklinde hizmetler sunulmaktadır. Şöyle ki katılımcıların kimlik doğrulaması, Self-Sovereign Identity (SSI) yöntemiyle yapılır. Bu yöntem, merkezi bir veri tabanı olmaksızın katılımcıların dijital kimliklerini yönetmesini sağlar. Verilerin paylaşımı sırasında her aşama kaydedilir (Data Logging Service). Böylece veri sahibi, verilerinin ne zaman, kim tarafından ve ne amaçla kullanıldığını görebilir. Ayrıca her federasyon, katılımcıların kurallara uygun hareket edip etmediğini kontrol eder. Teknik standartlar ve protokoller, veri güvenliğini ve düzenlemelere uygunluğu sağlar.

Bu bağlamda veri paylaşımına ilişkin tarafların hak ve yükümlülükleri, akıllı sözleşmeler (smart contracts) vasıtasıyla belirlenebilir. Bu sözleşmeler, veri paylaşımının otomatik yönetimini ve gerektiğinde yaptırımların uygulanmasını mümkün kılar.



Kaynak: Schütrumpf/Person: Gaia-X: VernetzteInfrastrukturen für eine europäisch geprägteDatenwirtschaft, RDi 2022, s. 281 vd.

(3) Etiketleme ve Sertifikasyon Süreci

Gaia-X çerçevesinde güvenilirlik ve şeffaflık ilkesi doğrultusunda tüm hizmetler, belirli bir sertifikasyon sürecinden geçirilir. Buna göre hizmetler, veri güvenliği, yasal uyumluluk ve kullanıcı gizliliği gibi kriterlere göre etiketlenir (örneğin, yüksek gizlilik seviyesi için özel etiket). Sertifikasyon süreci ise bağımsız bir denetim mekanizması tarafından yönetilir. Katılımcılar, standartlara uyum sağladıklarını gösteren etiketleri alır ve bu sayede kullanıcıların hizmet seçimini kolaylaştırır.

(4) Yönetim ve Koordinasyon

Gaia-X'in merkezi organizasyonu olan **Gaia-X AISBL**, stratejik kararlar almakla birlikte genel yönetişimi sağlar. Ancak federasyonlar bağımsız olarak faaliyet gösterir. AISBL ayrıca teknik standartları ve referans mimariyi geliştirir. Tüm katılımcılar bu standartlara uymak zorundadır.

Federasyonlar ise yerel ve sektörel bazda organize edilir. Her hub, kendi sektörüne özgü veri paylaşım senaryoları geliştirir. Örnek olarak sağlık sektörü için güvenli tıbbi veri paylaşımı sağlayan bir federasyon, otomotiv sektöründen tamamen farklı önceliklere sahip olabilir.

(5) Süreçlerin Çalışma Modeli

Süreç, öncelikle bir federasyonun kurulmasıyla başlar. Bu federasyon, Gaia-X tarafından belirlenen teknik altyapıyı baz alır ve bunun teknik standartlarına uyumluluk sağlar. Ardından sağlayıcılar, tüketiciler ve yöneticiler sisteme dahil olur. Sürecin işleyişi aşamasında artık katılımcılar arasında veri paylaşımı başlar. Söz konusu veriler, belirlenen kurallara uygun şekilde işlenir ve kullanılır. Federasyonlar büyüdükçe, yeni iş modelleri ve kullanım senaryoları da ortaya çıkar.

Bu kurguya örnek olarak Catena-X projesi gösterilebilir. Buna göre öncelikle Catena-X federasyonu, otomobil üreticileri ve tedarikçileri arasında bir işbirliği platformu kurar. Ardından üretim süreçleriyle ilgili veriler, taraflar arasında güvenli bir şekilde paylaşılır. Bu verilere örnek olarak bir tedarikçinin ürün teslim sürelerini gerçek zamanlı olarak üreticiyle paylaşması hali gösterilebilir. Verinin taraflar arasında paylaşılması aşamasında SSI ile kimlik doğrulama yapılır, veri paylaşımı sırasında akıllı sözleşmeler uygulanır ve her işlem kaydedilir. Ayrıca bağımsız bir denetim, tüm süreçlerin kurallara uygun olduğunu doğrular ve etiketleme sistemiyle güvence sağlar.

4. İdari Yapı ve Yaptırımlar

a. Aracı Veri Hizmeti Sağlayıcıları Açısından

Aracı veri hizmeti sağlayıcılarının kayıt süreçleri açısından her üye devlet, Madde 13(1) DGA uyarınca bir veya birden fazla "yetkili otorite" atayacak ve bu otoritelerin isimlerini en geç 24 Eylül 2023 tarihine kadar Komisyona bildirecektir. Söz konusu otoriteler açısından aranan kriterler, fonksiyonel olarak bağımsız olmaları (Madde 26(1)) ve görevlerini tarafsız, şeffaf, tutarlı ve zamanında yerine getirmeleri şeklindedir (Madde 26(2)). Madde 13(3) DGA uyarınca, veri koruma otoritelerinin, ulusal rekabet otoritelerinin, siber güvenlikten sorumlu otoritelerin ve diğer uzman otoritelerin yetkileri saklı tutulmaktadır.

Madde 14(1) DGA'ya göre, aracı veri hizmet sağlayıcılarından sorumlu yetkili otoriteler, belirli durumlarda bir gerçek veya tüzel kişinin talebi üzerine, Bölüm III gerekliliklerine uyumu denetlemek ve gözetmekle yükümlüdür. Yetkili otorite, Madde 14(3) DGA uyarınca Bölüm III hükümlerine aykırılık tespit ederse, ilgili aracı veri hizmeti sağlayıcısından görüş almasının ardından ihlalin sona erdirilmesini talep edebilir. Madde 14(4) DGA'ya göre, bu amaçla yetkili otorite, ulusal yasal düzenlemeler temelinde caydırıcı para cezaları uygulayabilir ve/veya veri aracılık hizmetinin başlangıcını erteleyebilir, askıya alabilir ya da tamamen durdurabilir.

b. Veri Hayırseverliği Açısından

Her üye devlet, Art. 23 f. 1uyarınca, Art. 26 hükmündeki gerekliliklere uygun olarak, tanınmış veri hayırseverliği kuruluşlarının ulusal kamu sicilinden sorumlu bir veya birden fazla "yetkili otorite" atamak ve bu otoritelerin isimlerini en geç 24 Eylül 2023 tarihine kadar Komisyona bildirmekle yükümlüdür. Art. 23 f. 3'e göre, veri hayırseverliği kuruluşlarının kaydından sorumlu yetkili otorite, kişisel verilerin işlenmesiyle ilgili görevlerini, ilgili veri koruma otoritesi ve aynı üye devletteki ilgili sektörel otoritelerle iş birliği içinde yerine getirir. Her ne kadar veri hayırseverliği açısından veri koruma otoritelerinin yetkilerine ilişkin (Art. 13 f. 3 hükmüne benzer şekilde) bir düzenleme bulunmasa da, Genel Veri Koruma Tüzüğü hükümlerinin (GDPR) ve özellikle "denetim otoritelerinin yetkilerinin" saklı olduğu dikkate alındığında bu bağlamda da aynı sonuca varmak mümkündür.

Yetkili otoriteler, belirli durumlarda bir gerçek veya tüzel kişinin talebi üzerine, Bölüm IV DGA'da belirtilen gerekliliklere uyumu denetlemekle yetkili kılınmıştır (Art. 24 f. 1). Eğer yetkili otorite, Bölüm IV DGA'ya aykırılık tespit ederse, Madde 24(3) ve (4) DGA uyarınca, ilgili tarafın görüşünü aldıktan sonra ihlalin sona erdirilmesini talep edebilir ve Bölüm IV DGA'ya uyumu sağlamak için uygun ve orantılı önlemler alır. Eğer ihlal devam ederse, söz konusu tanınmış veri hayırseverliği kuruluşu, "AB'de tanınmış veri hayırseverliği kuruluşu" unvanını kullanma hakkını kaybeder ve ilgili ulusal kamu sicilinden çıkarılır. Bu karar kamuya açık bir şekilde duyurulur (Art. 24 f. 5). Ancak, veri hayırseverliği kuruluşlarının kayıt olmadan da faaliyet gösterebilmesi nedeniyle daha ileri düzeyde yaptırım olanakları öngörülmemiştir.

c. AB Veri İnovasyonu Kurulu

Veri Yönetişimi Yasası Art. 29'a göre Avrupa Birliği nezdinde bir Veri İnovasyonu kurulu ihdas edilmektedir. Bu Kurul, aşağıdaki kişi ve kuruluşlardan müteşekkildir:

Üye devletlerin aracı veri hizmeti sağlayıcılarına ilişkin yetkili otoriteleri,

Üye devletlerin veri hayırseverliği ile ilgili yetkili otoriteleri,

Avrupa Veri Koruma Kurulu (EDPB),

Avrupa Veri Koruma Denetçisi (EDPS),

Avrupa Birliği Siber Güvenlik Ajansı (ENISA),

Avrupa Komisyonu,

KOBİ'lerden sorumlu ağ tarafından atanmış olan AB KOBİ temsilcisi,

Komisyon tarafından bir uzman çağrısı çerçevesinde seçilen diğer ilgili kuruluşların temsilcileri.

Kurul, özellikle birlikte çalışabilir ortak Avrupa veri alanları için yönergeler önerecek, ayrıca Komisyon'a danışmanlık faaliyetlerinde bulunacaktır.

ç. Yaptırımlar

Tıpkı Veri Yasası'nda olduğu gibi Veri Yönetişimi Yasası da yaptırımlar noktasında belirli miktarlar öngörmemektedir. Bunun yerine Art. 34 hükmünde aracı veri hizmeti sağlayıcıları, veri hayırseverliği kuruluşları ve uluslararası veri aktarımlarına ilişkin yükümlülüklere aykırı davranılması halinde yaptırım uygulanması öngörülmekte, ayrıca bu yaptırımların uygulanmasına dikkate alınması gereken kriterler düzenlenmektedir. Bu kriterler, ihlalin niteliği, ağırlığı, kapsamı ve süresi, ihlalin telafisi için alınan önlemler, önceden yaşanmış ihlallerin varlığı, ihlal sebebiyle elde edilen gelirler ya da uğranılan kayıplar ile diğer somut olay şartları olarak düzenlenmiştir.

Ç. Ürün Sorumluluğu Direktifi

Her ne kadar doğrudan veriye ilişkin düzenlemeleri sadece kısmen içerse de, AB pazarını hedefleyen Türk ürün ve hizmet sağlayıcılar açısından önem arz eden bir diğer düzenleme, 18 Ekim 2024 tarihli AB Resmi Gazetesinde yayımlanan (EU) 2024/2853 no.lu Ürün Sorumluluğu Direktifi'dir. Söz konusu Direktif, aynı zamanda 40 yıldır yürürlükte olan 85/374 no.lu eski Ürün Sorumluluğu Direktifini de yürürlükten kaldırmaktadır.

1. Neden Yeni Direktife İhtiyaç Duyuldu?

Eski ürün sorumluluğu Direktifinin (85/374/EEC), bilhassa yapay zeka ve diğer yeni teknolojiler, döngüsel ekonomiye ilişkin yeni iş modelleri ve küresel tedarik zincirleri bağlamında yaşanan gelişmeler sebebiyle yeniden gözden geçirilmesi icap etmiştir.

Ürün kavramı artık ihtiyaçları karşılamıyor

Teknik ve bilimsel gelişmeler, ispat noktasında karmaşıklığa ve mağdurlar açısından zorluluklara sebebiyet veriyor

Bu gelişmeler dikkate alınarak Direktif gözden geçirildi, yapay zeka da dahil olmak üzere yeni teknolojilerin üretilmesi, geliştirilmesi ve kullanımı teşvik edilirken, koruma düzeyinin muhafaza edilmesi ve teşebbüsler açısından daha fazla hukuki güvenlik ve eşit rekabet koşullarının sağlanması amaçlandı! (Rec. 3)

2. Yazılımların Ürün Sorumluluğuna Dahil Edilmesi

Yeni Direktif'in en önemli yeniliği belki de yazılımların da artık ürün kavramına dahil edilmesidir. Bu bağlamda Dibace No. 6'da açıkça yazılımların da artık ürün sorumluluğunun kusursuz sorumluluk rejimine tabi olacağı belirtilmektedir. Aynı doğrultuda tanımlar başlığını taşıyan Art. 4 No. 1 hükmünde de ürün, "başka bir taşınır veya taşınmazla entegre edilmiş ya da birbirine bağlı olsa bile tüm taşınır eşyaları ifade eder; bu tanım elektriği, dijital üretim dosyalarını, hammaddeleri ve yazılımı da kapsar".

Buna göre ürün sorumluluğu hükümleri bütün taşınırlara uygulanacak, bu taşınırlara, başka taşınırlara dahil edilen ve taşınmazlara uygulananlar da dahil olmak üzere yazılımlar da dahil edilmektedir. Dolayısıyla yazılım başlı başına ürün olarak kabul edilecektir. Yazılımın taşınır ya da taşınmaz bir eşyaya dahil edilmesi halinde de yine yazılımın kendisi ürün olarak değerlendirilebilecektir.

Bununla birlikte ücretsiz ve açık kaynak kodlu yazılımlar, ticari faaliyet dışında geliştirilip sunulduğu takdirde kapsam dışı bırakılmaktadır. Bu sayede inovasyonun engellenmemesi amaçlanmaktadır.

Yazılımlara ilişkin değerlendirmeler, Dibace No. 13'te detaylandırılmaktadır. Buna göre dijital çağda ürünlerin cismani ya da gayri cismani olabileceği hususuna dikkat çekilmektedir. Bu bağlamda yazılımlara işletim sistemleri, donanım yazılımları, bilgisayar programları, uygulamalar ve yapay zeka sistemleri örnek gösterilmekte, bunların piyasadaki yaygın kullanışına dikkat çekilmektedir. Yazılımın hem kendi başına bağımsız bir ürün olarak piyasaya sürülebilmesi, hem de bir bileşen olarak diğer ürünlere entegre edilebilmesinden hareketle Direktif, her iki senaryo açısından da zararların meydana gelebileceğine işaret etmektedir. Hukuki belirlilik açısından yazılımın tedarik ve kullanım şekline bakılmaksızın ürün olarak kabul edilmesi, bu vesileyle kusursuz sorumluluk rejimine tabi tutulması öngörülmektedir. "Bu nedenle, yazılımın bir cihazda depolanıp depolanmadığı, bir iletişim ağı veya bulut teknolojileri üzerinden erişilip erişilmediği ya da bir hizmet olarak yazılım (SaaS) modeliyle sunulup sunulmadığı fark etmeksizin, yazılım bir ürün olarak değerlendirilmelidir."

Her ne kadar yazılımın kendisi bir ürün olarak kabul edilse de, bilginin ürün niteliği açıkça reddedilmektedir. Dolayısıyla dijital dosyanın içeriğinden kaynaklı bir ürün sorumluluğu söz konusu değildir. Bu takdirde dijital içeriklere ilişkin özel düzenlemeler uygulama alanı bulabilecektir, ancak bu içerik, ürün sorumluluğunun konusu değildir. Ayrıca 2024/1689 no.lu AI Act kapsamındaki sağlayıcılar da dahil olmak üzere yazılım geliştirici ve üreticiler de bu Direktif kapsamında üretici olarak değerlendirilecektir.

Buna karşılık ürün tanımından da anlaşılacağı üzere dijital üretim dosyaları, dijital bilgi niteliğini haiz olsa da, ürün sorumluluğu kurallarına tabi tutulacaktır. Art. 4 No. 2'ye göre dijital üretim dosyası, "bir

taşınırın dijital versiyonunu veya dijital şablonunu ifade eder ve bu dosya, makine veya araçların otomatik kontrolünü sağlayarak somut bir eşyanın üretilmesi için gerekli işlevsel bilgileri içerir". Dijital ürün dosyalarına örnek olarak Dibace No. 16'da matkap, torna, freze makineleri ile 3D yazıcıların otomatik kontrolünü sağlayarak somut bir eşyanın üretilmesi için gerekli işlevsel bilgileri içeren dijital tasarım belgeleri gösterilmektedir. Bu bağlamda üç boyutlu yazıcı ürünlerinin üretiminde kullanılan ve zarar veren hatalı bir bilgisayar destekli tasarım (computer-assisted-design - CAD) dosyası, eğer bu tür bir dosya ticari bir faaliyet kapsamında geliştirilmiş veya sağlanmışsa, ilgili Direktif çerçevesinde sorumluluğa yol açmalıdır.

3. Bağlantılı Hizmetlerin Dahil Edilmesi

Her ne kadar ürün sorumluluğu hizmetleri kapsamamaktaysa da, bir ürüne entegre edilip ürünle bağlantılı hale gelen, ürünün bu hizmet olmaksızın işlevsiz hale geldiği bağlantılı hizmetler açısından farklı bir değerlendirme yapılmaktadır.

Her ne kadar Veri Yasası kapsamında da bağlantılı hizmet düzenlemeye tabi tutulmuş ve tanımlanmış[32] olsa da, ürün sorumluluğu bağlamında yer verilen tanım daha sadedir. Buna göre bağlantılı hizmet, ürüne entegre edilmiş ya da ürünle bağlantılı hale gelmiş öyle bir dijital hizmettir ki bu hizmetin yokluğunda ürünün bir ya da daha fazla işlevini yerine getirmesi mümkün olmayacaktır. Söz konusu bağlı hizmetler, ayrıca "ürünün üreticisinin kontrolü altında olmaları durumunda, entegre edildikleri veya bağlantılı oldukları ürünün bir bileşeni olarak değerlendirilmelidir. Bağlı hizmetlere örnek olarak, bir navigasyon sisteminde sürekli trafik verilerinin sağlanması, fiziksel bir ürünün sensörlerine dayanarak kullanıcının fiziksel aktivitelerini veya sağlık parametrelerini izleyen bir sağlık izleme hizmeti, bir akıllı buzdolabının sıcaklığını izleyen ve düzenleyen bir sıcaklık izleme hizmeti ya da bir veya birden fazla ürünü sesli komutlarla kontrol etmeyi sağlayan bir sesli asistan verilebilir"[33]. Bununla

---

[32] Veri Yasası Art. 2 f. 6.

'related service' means a digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product;

[33] Veri Yönetişimi Yasası, Dibace No. 17.

birlikte internet erişim hizmetleri bağlı hizmet olarak değerlendirilmemekte, dolayısıyla kapsam dışı bırakılmaktadır.

Bağlantılı hizmetin hangi şartlar altında üreticinin kontrolü altında olduğu ve dolayısıyla ürün sorumluluğu kurallarının uygulanmasını haklı kılacağı hususunda ise Direktif, üreticinin belirli faaliyetlerini esas almaktadır. Buna göre bağlantılı hizmet ve diğer bileşenler, ki bunlara yazılım güncellemeleri ve yükseltmeleri de dahil edilmektedir, üretici tarafından bir ürüne yerleştirildiğinde, bağlantılı hale getirildiğinde, sunulduğunda ya da söz konusu faaliyetlerin üçüncü kişilerce gerçekleştirilmesine müsaade edildiğinde ürün, üreticinin kontrolü altında olarak kabul edilmektedir. Hatta ürün piyasaya sürüldükten sonra, üreticinin hala yazılım güncellemeleri veya yükseltmeleri sağlayabilmesi ya da bunların bir üçüncü tarafça sağlanmasını mümkün kılabilmesi durumunda, ürün üreticinin kontrolü altında olmaya devam ediyor olarak kabul edilmelidir[34].

4. Verinin Ürün Sorumluluğu Kapsamında Korunması

Ürün sorumluluğu kapsamında kural olarak tazmin edilecek olan zarar kalemlerine can ve beden bütünlüğü ile eşyaya ilişkin zararlar dahil edilmekteyken, yeni Direktif ile birlikte gayri cismani bir varlık olarak veriler de dahil edilmiştir.

Buna gerekçe olarak özellikle verilerin artan önemi ve ekonomik değeri gösterilmektedir. Dolayısıyla örnek olarak bir sabit diskten silinen dijital dosyaların yok edilmesi ya da bozulması da hukuk düzenince korunmaya layık bir menfaat olarak değerlendirilmektedir. Ürün sorumluluğunun amacı bu doğrultuda münhasıran ölüm ya da yaralanma ve mülkiyet hakkına ilişkin müdahalelerden meydana gelen zararlarla sınırlı kalmamalı, "aynı zamanda verilerin yok edilmesi veya bozulmasından kaynaklanan maddi kayıplar için de tazminat" hakkı tanınmalıdır[35]. Söz konusu tazminatın kapsamı noktasında Direktif, verilerin kurtarılması veya geri yüklenmesi için yapılan masrafları da kapsayacağına işaret etmekteyse de, verinin silinmesinden dolayı meydana gelecek olan salt malvarlığı zararlarının da bu kapsama dahil edilip edilmeyeceğine ilişkin herhangi bir bilgi içermemektedir. Ancak zarar görenin verileri yedekleme ya da başka yöntemlerle yeniden elde etme, kurtarma imkanları mevcutsa artık tazminata gerek olmayacaktır. Ayrıca münhasıran olmasa da eş zamanlı olarak ticari amaçlar için de kullanılan veriler kapsam dışı bırakılmaktadır (Dibace No. 22). Ayrıca ürün sorumluluğu bağlamında öngörülen tazminat yükümlülüğünün, bilhassa kişisel veri ihlali sebebiyle doğması muhtemel olan tazminat taleplerinden de ayırt edilmesi gerekmektedir.

[34] Veri Yönetişimi Yasası, Dibace No. 18-19.
[35] Veri Yönetişimi Yasası, Dibace 20.

5. Tazminatın Kapsamına Dair Sınırlamalar

Direktif çerçevesinde tazminat hakkının kapsamına ilişkin sınırlandırmalar mevcuttur. Nitekim münhasıran ticari amaçlar için kullanılan ürünler için Direktif uygulama alanı bulmayacaktır. Belirtildiği üzere kısmen de olsa ticari amaçlar için kullanılan verilerin silinmesi ya da bozulması halinde de Direktif uygulama alanı bulmayacaktır. Dibacelerde ayrıca salt malvarlığı zararlarının da kural olarak ürün sorumluluğu kapsamında tazmin edilmeyeceği belirtilmektedir (Dibace No. 24). Yine Direktif'in esas aldığı ürün kavramı, bir ticari faaliyet kapsamında ivazlı ya da ivazsız şekilde piyasaya arz edilen ürünleri kapsamaktadır.

6. Ürünün Hatalı Olmasına İlişkin Kıstaslar

Direktif kapsamında ürünün hatalı olup olmadığını değerlendirirken Art. 7 f. 1'e göre üründen bir kişinin bekleyebileceği ya da Birlik ya da ulusal hukuk çerçevesinde öngörülen güvenliğin mevcut olup olmadığı esas alınmaktadır. Bir diğer ifade ile ürün, yürürlükteki mevzuat ya da ortalama kişinin ondan bekleyebileceği makul bir güvenlik seviyesine sahip değilse hatalı ürün olarak nitelendirilecektir. Bu çerçevede özellikle ürünün kullanıma elverişli olup olmadığı değil, güvenlikli olup olmadığı kıstası esas alınmaktadır[36].

Ürünün hatalı olup olmadığını değerlendirirken ürünün kullanıma elverişliliği değil, bir kişinin üründen haklı olarak bekleyeceği güvenliğin eksik olması esas alınacaktır. Ürünün hatalı olup olmadığını değerlendirirken genel olarak kamuoyunun haklı olarak beklediği güvenliğin nesnel bir analizi yapılmalıdır. Bir diğer ifade ile belirli bir kişinin sübjektif beklentisi değil, genel, makul ve ortalama kişinin objektif beklentisi esas alınacaktır. Bu bağlamda esas alınacak güvenlik kıstası, ortalama kişinin güvenlik, ürünün amaçlanan kullanım amacı, makul ölçüde öngörülebilir kullanımı, sunumu, nesnel özellikleri ve nitelikleri, beklenen ömrü gibi kriterlerden oluşan makul beklentisini esas almaktadır. Bunun yanında ürünün hedeflendiği kullanıcı grubunun özel gereklilikleri de dikkate alınabilecektir (Dibace No. 30).

Direktifin güncel teknolojik gelişmeleri dikkate alarak öngördüğü önemli bir diğer husus, bağlantılı ürünlere (burada kastedilen muhtemelen nesnelerin interneti cihazları -IoT) ilişkindir. Şöyle ki bu tür ürünlerin yaygınlaşması, aynı zamanda güvenlik açısından sorunları da beraberinde getirmektedir. Bu bağlamda örnek olarak bir akıllı ev sistemi içerisinde, diğer ürünlerin söz konusu ürün üzerindeki makul ölçüde öngörülebilir etkileri gösterilmekte, bu etkilerin de güvenlik değerlendirilmesi yaparken dikkate

[36] Bkz. Veri Yönetişimi Yasası, Dibace No. 30.

alınması gerektiğine dikkat çekilmektedir[37]. Direktif bu bağlamda özellikle makine öğrenmesi tabanlı çalışan yapay zeka sistemleri açısından önem arz eden düzenlemeler de içermektedir. Zira piyasaya sürüldükten veya kullanıma sunulduktan sonra öğrenme yeteneğine veya yeni özellikler kazanma kabiliyetine sahip ürünlerin, bu özelliklerinden kaynaklanan güvenlik risklerinin de dikkate alınması gerektiğine işaret edilmektedir[38]. Bunun arkasında yatan sebep ise, söz konusu ürünlerin yazılımının ve temel algoritmalarının, tehlikeli ürün davranışlarını önleyecek şekilde tasarlanması gerektiği yönündeki haklı beklentidir. Bu sebeple "beklenmedik davranışlar geliştirme yeteneğiyle tasarlanmış bir ürünü üreten bir üretici, zarar veren davranışlardan sorumlu olmaya devam etmelidir. Dijital çağda birçok ürünün piyasaya sürüldükten sonra dahi üreticinin kontrolü altında kalmaya devam ettiği gerçeğini yansıtmak amacıyla, bir ürünün üreticinin kontrolünden çıktığı anın, ürün güvenliği değerlendirmesinde dikkate alınması gerekmektedir"[39]. Direktif ayrıca bir ürünün siber güvenlik açığını da ürün sorumluluğu bağlamında önem arz edecek bir güvenlik unsuru olarak esas almaktadır.

7. Uygunluk Değerlendirmesi İçin Esas Alınacak Zaman

Bir ürünün güvenli olup olmadığını ve dolayısıyla üreticinin güvenlik eksikliği sebebiyle sorumlu tutulup tutulmayacağını belirlerken kural olarak ürünün piyasaya sunulma ya da hizmete sunulma anı esas alınmaktadır. Zira bu andan itibaren artık ürün üreticinin ya da distribütörün hakimiyetinden çıkmıştır. Dolayısıyla üretici üründeki güvenlik eksikliğinin, ürünün piyasaya sürüldüğü anda mevcut olmadığını ispat ederek mesuliyetten kurtulabilmektedir. Bununla birlikte dijital ürünler ve bağlantılı hizmetler açısından farklı bir değerlendirme yapmak gerekmektedir. Nitekim Direktif, ürünün piyasaya sürülmesi ya da hizmete alınmasından sonra da üreticinin yazılım güncellemeleri ya da makine öğrenimi tabanlı algoritmalar vesilesiyle ürün üzerinde hakimiyetinin devam edebilmesine dikkat çekmektedir. Şayet üreticinin ürün üzerinde hala bir hakimiyeti söz konusuysa, söz konusu yazılım veya hizmetlerden kaynaklanan güvenlik eksiklikleri nedeniyle üreticiler sorumlu olmaya devam etmelidir. "Bu tür yazılım veya ilişkili hizmetler, üretici tarafından sağlandığında veya üretici bu hizmetlerin üçüncü bir tarafça sağlanmasına izin verdiğinde ya da onayladığında üreticinin kontrolü altında kabul edilir. Örneğin, bir akıllı televizyon, bir video uygulaması içerdiği şekilde sunulmuşsa ancak kullanıcı televizyonu satın aldıktan sonra bu uygulamayı üçüncü bir tarafın web sitesinden indirmek zorundaysa, televizyon üreticisi, video uygulamasının piyasaya sürüldükten sonra ortaya çıkan eksiklikleri nedeniyle oluşan zarardan, video uygulaması üreticisiyle birlikte sorumlu olmalıdır.[40]" Özellikle üründeki eksiklik,

[37] Veri Yönetişimi Yasası, Dibace No. 32.
[38] Veri Yönetişimi Yasası, Dibace No. 32.
[39] Veri Yönetişimi Yasası, Dibace No. 32.
[40] Veri Yönetişimi Yasası, Dibace No. 50.

gerekli yazılım güncellemeleri ya da yükseltmelerinin yapılmaması ve bundan kaynaklı siber güvenlik sorunlarının meydana gelmesine dayanıyorsa, bu gibi durumlarda üretici, eksikliğin ürünün piyasaya sürüldüğü andan sonra meydana geldiği şeklindeki savunmaları dikkate alınmayacak ve sorumlulukları buna rağmen kabul edilecektir. Keza üretici, ürünün yaşam döngüsü boyunca meydana gelebilecek açıkları tespit etmeli ve bunlara karşı gerekli tedbirleri, yazılım güncellemesi ya da yükseltmesi gibi yöntemlerle almalıdır[41].

[41] Veri Yönetişimi Yasası, Dibace No. 51.

II. Türk Hukukundaki Mevcut Durum

Etki analizi raporunun bir sonraki aşamasında Türk hukukundaki durum incelenecektir. Bu bağlamda öncelikle verilere ilişkin düzenlemelerin genel çerçevesi çizilecek, ardından verilere erişime ilişkin mevzuat hükümleri, veri yönetişimine ilişkin mevzuat hükümleri ve nihayet siber güvenliğe ilişkin mevzuat hükümlerine yer verilecektir.

A. Veriye İlişkin Düzenlemelerin Genel Niteliği: Koruyucu Düzenlemeler

Türk hukukunda kişisel ve kişisel olmayan verilere ilişkin düzenlemelerin çoğu, doğrudan ya da dolaylı olarak koruyucu niteliktedir.

Kişisel veriler, gerek Anayasa md. 20 f. 3 hükmü, gerekse bu çerçevede çıkartılan 6698 sayılı Kanun uyarınca koruma boyutuyla düzenlemeye tabi tutulmaktadır. Benzer şekilde 5237 sayılı TCK md. 135-138 hükümleri arasında kişisel verilerin hukuka aykırı şekilde kaydedilmesi, verilmesi veya ele geçirilmesi ile yok edilmemesi halleri suç olarak nitelendirilmiş ve cezai yaptırımlar öngörülmüştür.

Kişisel veri niteliğinden bağımsız olarak bir bilişim sistemi içerisinde bulunan verilerin bozulması, yok edilmesi veya değiştirilmesi de TCK md. 244 kapsamında suç olarak düzenlenmiştir.

Benzer şekilde ticari sırlara ilişkin TCK md. 239 kapsamında cezai müeyyideler öngörülmüş, 6102 sayılı TTK bağlamında da çeşitli yerlerde (bilhassa haksız rekabete ilişkin md. 55 hükmünde olmak üzere) düzenlemelere yer verilmiştir.

Verinin fikri ve sınai hak niteliğini haiz olması halinde de 5846 sayılı Fikir ve Sanat Eserleri Kanunu ile 6769 sayılı Sınai Mülkiyet Kanunu çerçevesinde korunması gündeme gelecektir.

Bununla birlikte verilerin taraflar arasında değişime konu olacağını öngören belirli hükümler de, her ne kadar istisnai nitelikte olsa da, mevcuttur.

B. Bireyler Arasında Verilere Erişime İlişkin (İstisnai Nitelikteki) Düzenlemeler

Türk hukukunda bir cihaz ya da hizmet tarafından elde edilen verilere, kullanıcı tarafından erişilebilmesine ilişkin doğrudan bir düzenleme bulunmamaktadır. Özellikle Veri Yasası'nda olduğu gibi nesnelerin interneti olarak nitelendirilen ürün ve bunlarla bağlantılı hizmetler vesilesiyle üretilen verilerin kullanıcılar tarafından talep edilebilmesini öngören herhangi bir kanuni düzenleme mevcut değildir.

Bununla birlikte verilerin talep konusu edilebileceği, kanunun yasal bir dayanak sunduğu örnekler hukukumuzda mevcuttur. Şöyle ki kişisel verilerin işlenmesi halinde 6698 sayılı Kanun md. 11 f. 1 b.

b) çerçevesinde kişisel verisi işlenen ilgili kişi, veri sorumlusundan bilgi talebinde bulunabilecek, kişisel verileri veri sorumlusu tarafından işlendiği takdirde bu işleme sürecine ilişkin bilgi talep edebilecektir. Bununla birlikte Türk hukukunda, GVKT'ne kıyasla bazı eksiklikler bulunmaktadır. Şöyle ki GVKT Art. 15 f. 3'e göre ilgili kişi, veri sorumlusu tarafından işlenen kişisel verilerinin bir nüshasını talep etme hakkını haizdir. "Veri Taşınabilirliği Hakkı" başlığını taşıyan Art. 20 hükmüne göre ise ilgili kişi, kendisine ilişkin kişisel verileri veri sorumlusundan talep etme yetkisini haizdir. Bu veriler, yapılandırılmış, yaygın kullanılan bir formata uygun halde ve makineler tarafından okunabilir bir şekilde ilgili kişiye sunulacaktır. İlgili kişinin bu verileri başka bir veri sorumlusuna taşıma imkanına bulunmakla birlikte ilk veri sorumlusu, veri taşınabilirliği çerçevesinde herhangi bir engel oluşturmamalıdır. Buna karşılık Türk hukukunda veri taşınabilirliğine ilişkin 6698 sayılı Kanun kapsamında herhangi bir düzenleme mevcut değildir. Dolayısıyla KVKK'nın bu bağlamda gerçek bir veri taşınabilirliği hakkı getirdiğini söylemek mümkün değildir.

Veri taşınabilirliği hakkına ilişkin açık bir düzenleme buna karşılık 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Ek madde 2 f. 2 b) çerçevesinde öngörülmüştür. Bu bağlamda elektronik ticaret aracı hizmet sağlayıcıları, "Elektronik ticaret hizmet sağlayıcının satışları dolayısıyla elde ettiği verileri bedelsiz taşımasına ve bu veriler ile bunlardan elde ettiği işlenmiş verilere bedelsiz ve etkin şekilde erişim sağlamasına teknik imkân" sunmakla yükümlü kılınmaktadır. Bununla birlikte söz konusu hüküm, münhasıran bir takvim yılındaki net işlem hacmi on milyar Türk lirasının üzerinde olan elektronik ticaret aracı hizmet sağlayıcılarını kapsamaktadır ve dolayısıyla genel bir erişim yetkisi öngörmemektedir.

Bu açıklamalardan anlaşılacağı üzere Türk hukukunda veriye ilişkin düzenlemeler kural olarak koruyucu niteliktedir. Bir diğer ifade ile veri ekonomisi açısından veriye tedavül niteliği kazandırmayı amaçlayan hükümler ancak istisnai nitelikte mevcuttur.

C. Devlet-Birey İlişkisinde Verilere Erişim Yetkisine İlişkin Düzenlemeler

Devlet-birey arasındaki yatay ilişki çerçevesinde bireylere kamunun elinde bulundurduğu verilere erişim yetkisi tanıyan çeşitli düzenlemeler bulunmakla birlikte, bu düzenlemelerin genel bir yasal çerçeve içerisinde ele alınmadığı, bilakis münferit düzenlemeler çerçevesinde ve çoğu zaman yeknesak olmayan şekillerle gerçekleştiğini söylemek isabetli olacaktır.

Bu bağlamda öncelikle 4982 sayılı Bilgi Edinme Hakkı Kanunu belirtilmelidir. Ancak hemen vurgulamakta fayda olacaktır ki söz konusu kanunun amacı veriye tedavül niteliği kazandırmak değildir. İlgili kanun, bireyin temel hak ve özgürlüklerini kullanabilmesi için gerekli bilgilere erişimini

öngörmekle birlikte, veri ekonomisini dikkate alarak kaleme alınmış bir düzenleme niteliğini haiz değildir.

Diğer taraftan kamunun elinde bulundurduğu belirli veri kategorilerinin paylaşımına ilişkin düzenlemelere rastlamak mümkündür. Örnek olarak 10.03.2015 tarihli Tapu ve Kadastro Verilerinin Paylaşımı Hakkında Yönetmelik, tapu ve kadastro verilerinin paylaşımına ilişkin usul ve esasları düzenlemektedir. Bu çerçevede TAKPAS (Tapu ve Kadastro Paylaşım Sistemi) Sisteminden istifade etmek isteyen kurumlar ve kişiler, Tapu ve Kadastro Genel Müdürlüğü'ne başvurup sözleşme akdetmek suretiyle belirli amaçlar doğrultusunda söz konusu verilerden istifade edebilmektedir. Benzer şekilde Coğrafi Veri Lisans Yönetmeliği kapsamında Coğrafi Bilgi Sistemi konularında faaliyet gösteren yerli veya yabancı gerçek ve özel hukuk tüzel kişileri, kamu ile akdettikleri lisans sözleşmesi ile ilgili coğrafi verileri işleyebilecektir.

Ne var ki anılan düzenlemelerin amacının, söz konusu verilere tedavül niteliği kazandırmak olduğunu söylemek bir hayli güçtür. Kaldı ki belirtildiği üzere genel olarak kamunun elinde bulundurduğu verilere bireyler tarafından erişilebilmesi, bunların farklı amaçlarla yeniden kullanılabilmesi ve bu verilerden katma değer üretilmesi gibi bir amaç da söz konusu değildir.

Ç. Ürün Sorumluluğuna İlişkin Değerlendirmeler

Türk hukukunda ürün sorumluluğuna ilişkin güncel düzenleme, 7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanunu'dur. İlgili düzenleme, her ne kadar 2021 yılında yürürlüğe girse de ürün olarak hala "her türlü madde, müstahzar veya eşya" tanımına yer vermekte, dolayısıyla yazılımları kapsamamaktadır. Özellikle siber güvenliğe ilişkin hiçbir düzenleme mevcut değildir. Türk doktrininde ürün kavramının geniş yorumlanması gerektiğine ilişkin görüşler olmakla birlikte kanaatimizce kanunun açık lafzı, uygulamada yaşanan sorunlar ve teknolojik gelişmeler dikkate alındığında kanun koyucunun yazılımları gözden kaçırmış olması ve dolayısıyla kanunun daha geniş yorumlanması gerektiği şeklinde bir yorum imkân dahilinde gözükmemektedir. Kaldı ki dijital ürünlerin siber güvenliğine ilişkin hiçbir düzenleme mevcut değildir.

D. Ara Sonuç

Ülkemizde veriye ilişkin düzenlemelere bakıldığında Birlik hukukuna kıyasla daha korumacı bir yaklaşımın söz konusu olduğunu söylemek mümkün olacaktır. Nitekim Türk hukuk düzeninde verilere ilişkin düzenlemelerin büyük bir çoğunluğu, bunların çeşitli ihtimaller doğrultusunda korunmasını esas alırken, Avrupa Birliği'nin son dönemde hayata geçirdiği düzenlemeler, koruma yaklaşımını terk edip veriye tedavül niteliği kazandırma ve bu sayede veriden toplumun en geniş şekilde katma değer elde

etmesini mümkün kılmaya yöneliktir. Bu amaç doğrultusunda hem yatay eksende bireyler arasındaki ilişkiler, hem de dikey eksende birey-devlet arasındaki ilişkiler düzenlemeye konu edinilmektedir. Türk hukukunda ise veriye tedavül niteliği kazandırmayı amaçlayan hükümler son derece sınırlı sayıdadır. Ürün sorumluluğu bağlamında ise veri, siber güvenlik gibi hususlara ilişkin bir düzenleme mevcut değildir.

III. Riskler ve Fırsatlar

Bir sonraki aşamada AB düzenlemelerine uyum sağlamanın riskleri ve fırsatları ele alınacaktır.

A. Riskler

1. AB Mevzuatına Yönelik Eleştiriler

Öncelikle AB mevzuatına tam uyumun belirli riskleri de barındıracağı noktasında tereddüt etmemek gerekecektir. Nitekim Veri Yasası ve Veri Yönetişimi Yasası, yasama süreçlerinde birçok eleştiriye maruz kalmış ve hala eleştirilmektedir. Bu yasaların Türk hukukuna aktarılması, bu çerçevede yaşanan belirsizliklerin de aynı şekilde ülkemiz hukukuna aktarılması sonucunu beraberinde getirecektir.

Bu bağlamda Veri Yasasına ilişkin getirilen eleştirilerin başında düzenlemenin bütüncül nitelikte olmadığı, veri ekonomisini bir bütün olarak değil, sadece belirli noktalar açısından ele aldığına

ilişkindir. Gerçekten de Veri Yasası, veri ekonomisinde veri paylaşımını IoT cihazları ve veri hizmetleri düzleminde ele almaktadır. Ayrıca bu bağlamda aksiyon alması gereken aktörler bireyler olarak tanımlanmaktadır. Zira Veri Yasasında öngörülen veri paylaşımının gerçekleşebilmesi ve verilerin serbestçe dolaşıma kazandırılabilmesi için öncelikle kullanıcının aksiyon alması, harekete geçmesi lazımdır. Kullanıcının harekete geçmediği takdirde herhangi bir veri paylaşımı da olmayacaktır. Bunun için ise piyasa aktörlerinin farklı teşvik mekanizmaları geliştirmesi gerekecektir. Örnek olarak sigorta şirketi, trafik poliçesi yapmadan önce kullanıcıdan araç verilerini talep edecek, bu verilere göre sigorta bedelini hesaplayacak, daha düşük ya da daha yüksek bir poliçe bedeli öngörecektir. Ancak birey bu verileri talep etmeden kanunda öngörülen düzenlemeler işlevsiz kalacaktır. Öte yandan veri hizmetlerine ilişkin düzenlemelerde de standartların oluşturulması ve bu sürecin bilhassa akreditasyon ve standartizasyon kuruluşlarınca teşvik edilmesi gerekecektir. Aksi takdirde bu hükümler de işlevsiz kalacaktır.

Veri Yönetişimi Yasası'na getirilen en önemli eleştiri ise sürecin bütünüyle kamunun inisiyatifinde olmasına ilişkindir. Şöyle ki Yasa, kamuya veri paylaşımı yükümlülüğü getirmemekte, ancak elinde bulundurduğu verileri paylaşmak isteyen kamu kuruluşlarına ise karmaşık yükümlülükler getirmektedir. Hal böyle olunca birçok kamu otoritesinin veri paylaşımından imtina etmesi, elinde bulundurduğu verileri kullanıma sunmaması daha çok tercih edilecek bir yöntem olacaktır. Bu durum ise verinin paylaşımının teşvik edilmesi noktasında tam tersine bir etki doğurmaya elverişlidir.

Aracı veri hizmeti sağlayıcılarına ilişkin düzenlemeler de teşvik sağlamaktan çok bürokratik engeller içerdiği için eleştirilmektedir. Hizmet sağlayıcıların bu karmaşık yapı karşısında AB pazarına hizmet sunmaktan bütünüyle imtina etmesi ve daha düşük maliyetlerle farklı pazarlara yönelmesi de ihtimal dahilindedir.

Bütün düzenlemeler açısından son derece önem arz eden bir diğer sorun, kişisel verilere ilişkindir. Nitekim düzenlemeler, GVKT hükümlerinin saklı olduğuna, ihtilaf halinde GVKT hükümlerinin öncelikli olarak uygulanması gerektiğine işaret etmektedir. Oysa AB hukukunda "kişisel veri" kavramı halen son derece tartışmalı bir konudur. Avrupa Birliği Adalet Divanı, 2024 yılında kişisel veri tanımına ilişkin iki adet karar vermiş olmakla birlikte, yakın zamanda da yeni bir kararın yayımlanması beklenmektedir. Bütün bu belirsizliklere rağmen Veri Yasası ve Veri Yönetişimi Yasası, kendi karmaşık düzenlemelerine ilaveten muhataplara kişisel verileri kişisel olmayan verilerden ayrıştırma yükümlülüğü getirmekte, kişisel verinin söz konusu olduğu durumlarda ilaveten GVKT hükümlerine de riayet edilmesi gerektiğini vurgulamaktadır. Ancak Avrupa Adalet Divanı'nın dahi tam olarak

çözemediği kişisel veri kavramının belirsizliği dikkate alındığında söz konusu düzenlemelerin açıklık getirmek yerine daha da karmaşık bir düzene yol açacağı hususunda tereddüt yoktur.

2. Türkiye'deki Mevzuata Uyum

AB mevzuatına ilişkin gerçekleştirilecek her türlü uyum çalışmasının, Türk hukukundaki mevcut düzenlemelerle de uyumlu olması gerekecektir. Özellikle Türk hukukunda veriye ilişkin bütün mevzuat koruma temelli kaleme alınmıştır. Hal böyle olunca mevcut mevzuat ile çelişmeyen, onunla uyumlu düzenlemeler getirmek gerekecektir. Bu bağlamda AB'de olduğu gibi kişisel verilerin korunmasına ilişkin mevzuat hükümlerinin öncelikli olduğu belirtilip topu tamamen uygulamaya atmak düşünülebilecekse de, bu uygulama açısından halihazırda mevcut olan belirsizliği daha da artıracaktır. Böyle bir düzenlemenin piyasada 6698 sayılı Kanun kapsamında yaşanan sorunlara ilaveten bir yük getireceği hususunda tereddüt yoktur. Dolayısıyla Türk hukukundaki mevcut düzenlemeler ile uyum çalışması kapsamında öngörülen düzenlemelerin uyum içerisinde olması, gerektiğinde mevcut düzenlemelere açık istisnaların getirilmesi isabetli bir yaklaşım olarak değerlendirilmektedir.

3. Overregulation

AB'nin dijital alanda son dönemde gerçekleştirdiği yasama faaliyetlerine ilişkin getirilen en önemli eleştirilerden birisi de "overregluation" sorunudur. Draghi[42] raporunda da belirtildiği üzere Birlik içerisinde dijital alana ilişkin çok fazla regülasyon, çok fazla denetleyici ve düzenleyici otorite mevcuttur. Dijital alanda faaliyet göstermek isteyen şirketler aynı zamanda birden fazla regülasyona tabi tutulmakta, birden çok otoriteyle muhatap olmaktadır. Türkiye'de de aynı sonuç ortaya çıkabilecektir. Dolayısıyla dijital alanda gerçekleştirilecek her türlü regülasyon faaliyeti açısından hem özel sektör, hem de kamu nezdinde çok uyumlu bir çalışma gerekmektedir. Nitekim birden fazla mevzuata tabi olan özel sektör, bu düzenlemeler arasındaki uyumu sağlamalıdır. Bu da insan, para ve zaman açısından maliyet demektir. Aynı zamanda regülasyonların uyumlu olmaması halinde hukuki belirsizlikler de ortaya çıkacaktır.

Kamu otoriteleri açısında bakıldığında ise yine bunların diğer otoritelerle işbirliği içerisinde olması gerekmektedir. Türkiye'deki eğilim, aynı fiilin birden çok mevzuata aykırılık teşkil etmesi halinde her otoritenin kendi görev alanı açısından yaptırım uygulamasına ilişkin. Dolayısıyla mevzuat arttıkça, idari yaptırımın sadece niteliği değil, niceliği de artacaktır. Bu takdirde Türkiye pazarında faaliyet göstermek

[42] Mario Draghi tarafından hazırlanan ve AB'nin rekabet edebilirliğine ilişkin rapor: The future of European competitiveness – A competitiveness strategy for Europe, https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en#paragraph_47059.

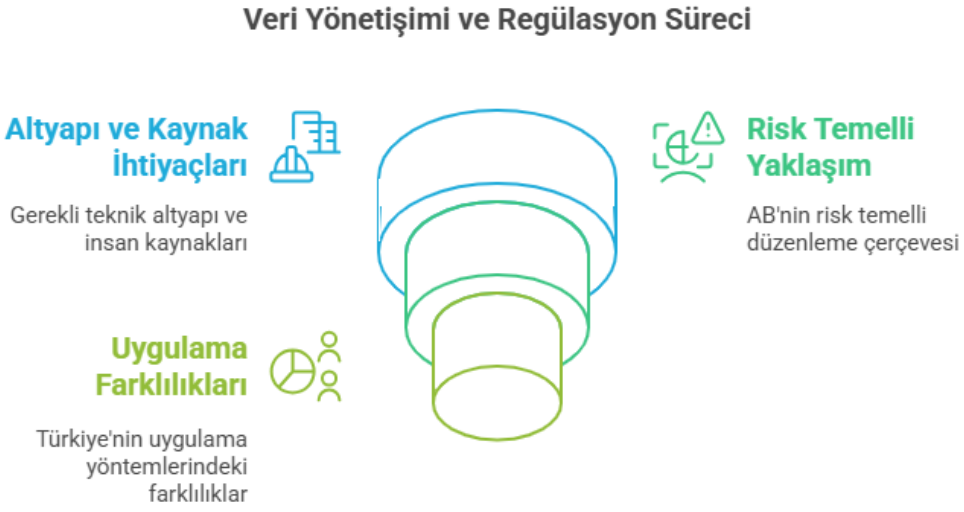
imkânsız hale gelecek, teşebbüsler başka ülkeleri tercih edecektir. Ayrıca Türk idaresinde risk temelli yaklaşım tam olarak benimsenemediği için otoriteler, yol göstermek yerine öncelikli olarak cezalandırmayı tercih etmektedir. Ancak dijital regülasyonların karmaşıklığı ve içerdiği hukuki belirsizlikler dikkate alındığında bu yöntemin dijital alanda son derece olumsuz sonuçlar doğuracağı aşikardır. Şayet otoriteler düzenleyici faaliyetlerini artırmak yerine münhasıran cezalandırma yolunu tercih ederse, Türkiye'de dijital alanda faaliyet gösteren teşebbüsler azalacak, Türkiye pazarı cazibesini bütünüyle yitirecektir.

4. Kamu ve Özel Sektör Nezdinde Süreçleri Yönetecek İnsan Kaynağı ve Know-How Sorunları

Özellikle Veri Yönetişimi Yasası'na bakıldığında kamu, elinde bulundurduğu verileri erişime açmak istediği takdirde birçok yükümlülüğe tabi tutulmaktadır. Ancak bu yükümlülüklerin yerine getirilebilmesi için teknik altyapının yanında bilgi ve beceri sahibi personel ihtiyacı da gündeme gelecektir. Bir diğer ifade ile söz konusu mevzuatın yönetilmesi başlı başına ciddi bir maliyeti ve aynı zamanda insan kaynağı ihtiyacını beraberinde getirecektir. Kamunun elinde bulundurduğu her bir veriyi

tasniflendirmesi gerekecek, bunların korunması için gerekli önlemleri alması, sözleşmeler akdetmesi, teknik ve idari tedbirler öngörmesi ve daha da önemlisi bütün bu süreçleri yönetmesi gerekecektir.

İkinci bir husus, regülasyon mantığıyla alakalıdır. Şöyle ki dijital alanda riskin mutlak surette bertaraf edilmesi söz konusu değildir. Bu sebeple AB'nin dijital alanda getirdiği birçok düzenlemede risk temelli yaklaşım benimsenmektedir. AB'de kamu otoriteleri her zaman bir riskin mevcut olduğunu bildiği için kural olarak hemen yaptırım uygulanmamaktadır. Önce talimat verilir, ardından talimat yerine getirilmediğinde yaptırım uygulanmaktadır. Ayrıca bireyin önceden konu hakkında araştırma yapmış, görüşler almış ve uyum için çaba göstermiş olması da başlı başına olumlu olarak değerlendirilmekte, yaptırım uygulanacaksa, kanunun muhatabının bu çabası da olumlu olarak değerlendirilmektedir. Türkiye uygulamasında ise çoğu zaman incelemeler başlatılmakta, herhangi bir talimata ihtiyaç duyulmaksızın doğrudan yaptırım uygulanmaktadır. Kaldı ki otoritelerin sadece denetleyici değil, düzenleyici olması da gerekirken, otoritelerin düzenlemekten çok denetlediğini de vurgulamak gerekmektedir. Bilhassa dijital alanda faaliyet gösteren kamu otoritelerinin yayımladıkları rehberlerin somut bilgi içermekten çok soyut bilgiler vermesi, halihazırda mevcut olan belirsizlikleri bertaraf etmeye yaramamaktadır. Hal böyle olunca yeni düzenlemeler, daha karmaşık bir hukuki yapıyı beraberinde getirecek, piyasada belirsizlikler artacaktır. Buna karşılık otoriteler yol göstermek yerine yaptırım uygulamayı tercih edecek olursa artık Türkiye pazarı cazibesini bütünüyle yitirecektir. Dolayısıyla dijital mevzuata uyumla birlikte regülasyon mantığının da değişmesi kaçınılmazdır.



B. Fırsatlar

1. AB ile Uyum, Mal ve Hizmet İhracatında Kolaylık

AB'nin dijital alanda getirdiği birçok düzenleme, aynı zamanda bir pazara giriş engeli niteliği taşımaktadır. Bu husus, özellikle düzenlemelerin uygulama alanına bakıldığında daha da çarpıcı bir şekilde ortaya çıkmaktadır. Nitekim rekabet hukuku ve sermaye piyasası hukukundan esinlenerek benimsenen pazar yeri ilkesine göre bir pazara yönelik faaliyet gösteren, o pazarı hedefleyen her aktör, söz konusu pazarın şartlarına da riayet etmekle yükümlüdür. Bu açıdan bakıldığında GDPR ile başlayan dijital alandaki düzenlemeler, aktörün nerede kurulduğu ve faaliyet merkezinin nerede olduğundan bağımsız olarak AB pazarında faaliyet gösterilmesinin amaçlandığı takdirde AB mevzuatına uyum sağlanması zorunluluğunu öngörmektedir. Dolayısıyla AB dışında bulunan ve AB pazarında faaliyet göstermek isteyen aktörlerin de bu yükümlülüklere riayet etmesi gerekmektedir. AB mevzuatına uyum göstermeyen aktörler ise kural olarak AB pazarından dışlanacaktır.

Türkiye'de yerleşik veri ekonomisi aktörleri de bu durumdan doğrudan etkilenecektir. AB'de mevcut yasal düzenlemelere uyum sağlamayan aktörler açısından yukarıda etraflıca incelenen mevzuat hükümleri bir pazara giriş engeli teşkil edecektir. Dolayısıyla Türk hukukunun AB mevzuatına uyumlaştırılması, Türkiye'de yerleşik veri ekonomisi aktörleri açısından hem Türk, hem de AB mevzuatına uyum anlamına gelecek, bu çerçevede gerçekleştirilecek olan mal ve hizmet ihracatında yasal engeller gündeme gelmeyecektir.

2. Çifte Standart Sorunu ve Rekabet Açısından Dezavantajlar

AB mevzuatına uyum sağlamamanın bir diğer sonucu ise, AB pazarına ürün ya da hizmet sunmak isteyen Türk üreticinin, AB'ye mal satabilmek için oradaki mevzuata uyum için veri paylaşımı ve siber güvenlik için belirli gereksinimleri yerine getirecek olması, ancak aynı ürünü Türk piyasasına arz ettiğinde Türk kullanıcıyı bu haklardan mahrum bırakmasıdır. Örnek olarak AB pazarına akıllı çamaşır makinesi satacak olan Türk üretici, AB'deki kullanıcılara veri paylaşımına ilişkin bütün imkanları sunacak, onlarla veri lisansı sözleşmesi akdedecek, ancak aynı ürün Türkiye pazarına sunulduğunda bütün bu fonksiyonlar devre dışı olacaktır. Daha da önemlisi aynı şirketin elde ettiği veriler, AB'de kullanıcı ve diğer rakip firmalar ya da üçüncü kişiler tarafından kullanılacak, katma değer elde edilebilecek, Türkiye'deki kullanıcılar ve diğer rakipler ve üçüncü kişiler ise bu verilerden istifade edemeyecek, bunlardan herhangi bir katma değer elde edemeyecektir. Bu durumda aynı ürün açısından bir taraftan AB kullanıcısı ile Türk kullanıcısı açısından çifte standart uygulanmış olacaktır. Bu çifte standart sebebiyle aynı ürün vesilesiyle üretilen verilerden AB'deki kişiler katma değer elde edebilecek,

Türkiye'deki kişiler ise bu imkândan mahrum kalacaklar. Bu da ülkemizin dijital ekonomideki rekabet kabiliyeti açısından son derece olumsuz bir tabloya sebebiyet verecektir. Öte yandan uyum, hem çifte standartın önlenmesine, hem de rekabet avantajının sağlanmasına hizmet edebilecektir.

3. Türkiye'nin Kendi Standartlarını Oluşturması, Üreticinin Öncelikle Bu Standartlar Çerçevesinde Hareket Edebilmesi

Önem arz eden bir diğer husus, AB pazarında faaliyet göstermek isteyen Türk aktörlerin AB standartlarına uyum sağlamak zorunda olmalarına ilişkindir. Şöyle ki AB'ye mal veya hizmet ihracında bulunmak isteyen aktörler, AB tarafından geliştirilen standartları öncelikle esas alacak ve ürün ve hizmetlerini bu standartlara göre belirleyecektir. Bu durumda ise Türkiye'nin kendi ülkesinde kendi muhatapları üzerindeki hakimiyeti zayıflayacaktır. Nitekim Türk üretici ya da hizmet sunucu, Türk standartlarına göre değil AB standartlarına göre hareket edecektir. Ancak Türkiye'nin AB standartlarıyla uyumlu olacak şekilde kendi standartlarına sahip olması, bu standartları hızlı bir şekilde hayata geçirmesi, bir taraftan Türk veri ekonomisi açısından son derece faydalı olacak, diğer yandan AB ile uyum ve özellikle denetim hakimiyeti açısından önem taşıyacaktır. Nitekim söz konusu standartlara uyumu öncelikle Türk otoriteleri denetleyecek, bu sayede Türkiye'nin denetim hakimiyeti de tesis edilmiş olacaktır. Aksi takdirde dijital alandaki standart koyma hakimiyeti bütünüyle AB'ye devredilmiş olacaktır.

4. Türk Veri Ekonomisinin Teşvik Edilmesi, Özellikle Veri Alanlarının Oluşturulması, Rekabet Avantajları

Ülkemizde yıllardır "ortak gelir tuzağı" olarak nitelendirilen gelir seviyesinin aşılmasına yönelik çalışmalar mevcuttur. Bu çerçevede ise "Milli Teknoloji Hamlesi" büyük önem arz etmektedir. Bu çerçevede özellikle teknoloji odaklı bir büyüme hedeflenmekte, Türkiye'nin dijital dönüşümü yakalaması ve bu dönüşümden menfaat elde etmesi için çalışmalar yürütülmektedir. Bu amaca hizmet edecek şekilde veri ekonomisinden en üst seviyede istifade edilmesi kanaatimizce önemli bir hukuk politikası amacıdır. Ne var ki mevcut durumda Türk hukuk düzeni veriye kural olarak koruma amaçlı yaklaşmaktadır. Bunun ötesinde veriye tedavül niteliği kazandırma, veriden katma değer elde etmeyi teşvik etme amaçlarına hizmet edecek düzenlemeler mevcut değildir. Bu açıdan bakıldığında AB mevzuatında öngörülen farklı düzenlemelere uyum sağlamak, AB hukuk politikalarına benzer şekilde veriden katma değer elde etmeye yönelik faaliyetlerin teşvik edilebilmesi amacıyla gerekli hukuki çerçeveyi oluşturmak, ülke menfaatleri açısından büyük önem arz etmektedir. Ne var ki bunu yaparken

halihazırda öngörülen koruma mekanizmaları ile de sağlıklı bir dengenin tesis edilmesi gerekecektir. Bu sayede ülkemizin dijital alandaki rekabet gücünün de artırılması düşünülmektedir.

Bu açıklamalar ışığında yapılacak bir değerlendirme neticesinde veri ekonomisinin önemli bir boyutu olan IoT cihazlarından elde edilen verilerin kullanıcılar tarafından talep edilebilmesi, bunları üçüncü kişilerle de paylaşabilme imkânı, veri ekonomisindeki tekelleşmenin önüne geçebilecek ve bilhassa verilerin belirli üreticiler tekelinde toplanmasını önlemeye hizmet edebilecek niteliktedir.

Kamunun elinde bulundurduğu verilerin farklı amaçlarla yeniden kullanıma açılması da benzer şekilde veri ekonomisinin "canlandırılması" açısından büyük önem taşımaktadır. Bu bağlamda özellikle kamu denetiminde güvenli veri alanlarının açılması, bu verilerin gerekli idari ve teknik tedbirlerin alınması akabinde piyasadaki aktörlerin tasarrufuna sunulması, uygulamada bilhassa yapay zekâ gibi çokça veri ihtiyacı doğuran uygulamalar açısından son derece önemli fırsatlar sunabilecektir.

IV. Politika Önerileri ve Uyum Stratejileri

A. Hukuk Politikası Açısından Değerlendirmeler

Yukarıda yapılan risk ve fırsat analizi kapsamında AB'de hayata geçirilen düzenlemelere uyumun ülkemiz açısından çeşitli avantaj ve dezavantajlar barındırdığını söylemek mümkündür.

1. Opsiyon 1: AB Düzenlemelerine Uyum Sağlamamak

Her şeyden önce söz konusu düzenlemelere hiçbir şekilde uyum sağlamamak elbette mümkündür. Bu takdirde AB'ye mal veya hizmet sunmak isteyen Türkiye'deki yerleşik üreticiler, ticari faaliyetlerini devam ettirebilmek adına Birlik mevzuatına uyum sağlayacak, bu bağlamda bazı maliyetlere katlanacak, netice itibariyle aynı ürünü iki farklı şekilde, birincisi AB mevzuatına uyumlu ve diğeri AB mevzuatına uyumlu olmayacak şekilde, tasarlayıp piyasaya sürecektir. Bu senaryoda sadece AB'ye mal ve hizmet sunmayı amaçlayan üreticiler "uyum maliyetine" katlanmak zorunda kalacaktır. Türkiye'de yerleşik ve Türk pazarında faaliyet gösteren üreticiler ise herhangi bir maliyete katlanmayacaktır.

Diğer yandan bu senaryoda Türk üretici, kendi ürün ya da hizmetleri vesilesiyle elde ettiği verileri AB'deki muhataplarıyla paylaşmak zorunda olacakken, Türkiye'de bunları kullanıcı ya da üçüncü kişilerle paylaşmak zorunda kalmayacaktır. Bir diğer ifade ile veriler Birlik içerisinde üçüncü kişilerin kullanımına açılacak, bu kişilerin söz konusu verilerden katma değer elde etme imkânı olacak, ancak aynı durum Türkiye açısından gündeme gelmeyecektir. Yine kamu otoriteleri hukuki bir dayanak olmaksızın veri paylaşımı noktasında kendileri inisiyatif alacak ya da inisiyatif almaktan imtina edecek, verinin yeniden kullanımı noktasında hukuki açıdan belirsizlik devam edecektir. Ürün sorumluluğu noktasında ise bilhassa yazılımlar ile siber güvenlik hususlarındaki belirsizlik devam edecektir.

2. Opsiyon 2: AB Düzenlemelerine Uyum Sağlamak

AB düzenlemelerine uyum sağlanması halinde ise üreticinin AB pazarına ürün arz etme niyetinde olduğuna bakılmaksızın veri üreten bütün ürün ve hizmetler açısından, veriyi yeniden kullanıma açmak isteyen kamu otoriteleri, aracı veri hizmeti sağlayıcıları ve dijital ürün üreticileri açısından çeşitli yükümlülükler öngörülecektir. Bu yükümlülük elbette ciddi bir "uyum yükünü" beraberinde getirecektir. Gerçekten de bu senaryoda her bir ürünün kullanıcı bazında elde ettiği verilerin saklanması ve talep halinde paylaşılması söz konusu olacaktır. Bu durum ise operasyonel, teknik ve idari açıdan birçok sorunu beraberinde getirecektir. AB düzenlemelerine uyumun avantajı ise AB'ye ürün ya da hizmet ihraç etmek isteyenlerin ülke mevzuatına uyum göstermekle birlikte eş zamanlı olarak AB mevzuatına da uyum sağlamış olmaları ve dolayısıyla pazara giriş engellerine muhatap olmamalarıdır.

Bu değerlendirmeler ışığında Türk mevzuatının AB nezdinde hayata geçirilen veriye ilişkin düzenlemelere uyumunu haklı kılmak için kanaatimizce mal ve hizmet ihracatındaki kolaylıklar başlı başına yeterli bir gerekçe değildir. Belirtildiği üzere AB'ye mal veya hizmet sunmayı amaçlayan üreticiler halihazırda kendi bünyelerinde AB mevzuatına uyum sağlamak suretiyle söz konusu pazar engelini aşabilecektir. Ancak bu uyum maliyetini karşılayamayacak üreticiler, özellikle KOBİ'ler açısından bir dezavantaj söz konusu olacaktır. Bununla birlikte sırf uyum maliyetine katlanamayan Türk üreticilerinin rekabet dezavantajını bertaraf etmek amacıyla ülkedeki bütün üreticileri aynı yükümlülük altına sokmak, bunların hepsini insan, para ve zaman gerektirecek olan uyum maliyetlerine muhatap kılmak, mantıklı bir yaklaşım olmayacaktır.

Kanaatimizce AB'nin veri ekonomisine ilişkin mevzuatına uyumu Türkiye açısından haklı kılacak asıl sebep, mal ve ürün ihracatındaki kolaylık değil, Türk veri ekonomisinin güçlenmesi, yasal bir altyapıya kavuşarak hukuk güvenliğinin sağlanması ve veriden katma değer elde etme imkanının teşvik edilmesi olacaktır. Ancak bu takdirde, AB mevzuatına uyumun getirdiği maliyetleri haklı kılmak mümkün olacaktır. Zira AB mevzuatına uyumun sebebiyet vereceği maliyet, verinin tedavül niteliği kazanması sebebiyle sağlanan katma değerden daha yüksek olacaksa uyumun yapılmamasında, bir diğer ifade ile mevcut durumun muhafaza edilmesinde fayda olacaktır. Öte yandan veriye tedavül niteliği kazandırılması sebebiyle veriden katma değer elde edebilen bir veri ekonomisinin hayata geçirilmesi mümkün olduğu takdirde AB mevzuatına uyum tercih edilebilir bir hukuk politikası olarak değerlendirilmektedir.

Bu bağlamda Veri Yönetişimi Yasası, Veri Yasası ve Ürün Sorumluluğu Direktifi'ne ilişkin hazırlanan etki analiz raporlarına aşağıda yer verilecektir. Zira bu raporlarda öngörülen kazanımlar ile masraflar belirtilmiş, kazanımların muhtemel masrafların çok daha üzerinde olması sebebiyle ilgili düzenlemeler yasalaşmıştır.

a. AB Veri Yönetişimi Yasası Etki Analizi Raporu

Veri yönetişimi yasasına ilişkin hazırlanan etki analizi raporunda[43] düzenlemenin kimlere olumlu ve olumsuz etkilerde bulunacağına ilişkin önemli tespitlere yer verilmiştir.

Bu bağlamda her ne kadar elinde bulundurduğu veriyi paylaşırken belirli yükümlülüklere tabi olsa da söz konusu düzenlemelerin en büyük faydacılarından birisinin kamu sektörü olduğu belirtilmektedir. Zira veri yönetişiminin hukuki çerçevesinin netleştirilmesi sayesinde sağlık kuruluşları, ulaşım ya da toplu taşıma birimleri ve istatistik ofisleri gibi kamu kurumlarının ortak standartlar dahilinde hareket etmesine imkân sağlanılmakta, bu sayede idari süreçlerde daha yüksek düzeyde öngörülebilirlik elde edilmektedir. Bunun ötesinde kamunun elindeki veri setlerinin farklı paydaşlarca analiz edilmesi ve yeniden kullanımı, kamusal hizmetlerin kalitesini artırmakta ve kamu politikalarının oluşumunda daha isabetli kararlar alınmasına yol açmaktadır. Bu hususa örnek olarak şehir içi toplu taşıma planlamasında trafik akış verilerini değerlendirebilen ya da sağlık alanında klinik ve istatistiksel bilgileri karşılaştırarak hastalıklar hakkında derinlemesine çıkarımlar yapabilen kamu kurumları, somut verilere dayalı ve etkin çözümler geliştirebilir hale gelmektedir.

[43] Rapor için bkz.: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-study-accompanying-proposal-regulation-data-governance.

Olumlu etkinin söz konusu olacağı bir diğer grup, akademik ve araştırma kurumlarıdır. Bunlar, kamu verilerinin yeniden kullanım imkânı sayesinde bilimsel çalışmalarını derinleştirme fırsatı bulacak, özellikle mikro düzeydeki istatistiksel veri setleri veya sağlık alanında büyük ölçekli veriler, araştırmacıların daha güvenilir ve karşılaştırmalı analizler yapmasına olanak tanıyacaktır. Bu sayede, yeni yöntemlerin geliştirilmesi, bilimsel deneylerin tasarlanması ya da mevcut politikaların etkililiğinin ölçülmesi kolaylaşacaktır. Bu bağlamda ayrıca veri paylaşımının standartlarının oluşması sayesinde uyum açısından harcanan saat ve paranın da azalacağı öngörülmektedir.

Veri Yönetişimi Yasası'nın özel sektöre yönelik en önemli olumlu etkilerinden birisi, çeşitli sektörler arasında veri paylaşımını kolaylaştırması ve bu sayede çapraz sektörlü iş birliklerine yol açmasıdır. Özellikle KOBİ'ler, büyük veriye dayalı teknolojilerin geliştiği alanlarda rekabetçi kalabilmek için dış kaynağa gereksinim duymakta ve kamu verilerine erişim olanağı sayesinde daha yenilikçi ürünler geliştirebilmektedir. Buna karşılık, büyük ölçekli şirketler de veri paylaşımı ve standardizasyon süreçlerinde belirgin avantajlar elde ederek yeni pazarlara ve müşteri segmentlerine ulaşma şansı bulacaktır. Bu paylaşımın teknik boyutuna bakıldığında ise birlikte çalışılabilirlik standartlarının geliştirilmesinin önemli bir husus olduğu belirtilmektedir. Zira bu sayede küçük ölçekli şirketler dahi, kamu kurumlarıyla veya diğer işletmelerle eşit şartlarda veri alışverişi yapabilmekte; yüksek maliyetli altyapı gereksinimleri ise ortak standartlar ve düzenlemelerle hafifletilebilmektedir. Böylelikle, verinin üretilmesinden işlenmesine ve ticarileştirilmesine kadar uzanan tüm süreçlerin piyasa aktörleri açısından daha öngörülebilir hale geleceği belirtilmektedir.

Bireyler, şirketler ve kamu kurumları arasındaki veri alışverişini organize ederek, teknik, hukuki ve idari konularda ortak bir zemin oluşmasına katkı sunan aracı hizmet sağlayıcılarına ilişkin düzenlemeler bir taraftan kişisel verilerin korunmasına yönelik uyum süreçlerini diğer yandan ticari bilgilerin paylaşımını düzenlemeyi amaçladığı için, piyasada güven ve şeffaflık yaratacağı öngörülmektedir. Söz konusu hizmet sağlayıcılar, standartlara uyum ya da sertifikasyon süreçlerinde ek maliyetlere katlanmak zorunda kalacaktır.

Nihayet yasal düzenleme sayesinde bireylerin gerek kendi verilerinden faydalanabilmesi gerekse verilerini kamusal veya toplumsal yarara yönelik projelere gönüllü olarak sunabilmesinin mümkün olacağı, bu sayede verinin kişiselleştirilmiş hizmetlerde (örneğin sağlık uygulamaları veya enerji tüketimi yönetimi) kullanılabilmesinin kolaylaşmasının söz konusu olacağı belirtilmektedir. Özellikle nadir hastalıklarla ilgili veri setlerinin araştırmacılarla paylaşılması veya toplum sağlığına dair verilerin anonimleştirilerek analitik süreçlerde kullanılması, somut toplumsal faydalar sunacaktır. Bireyler

açısından bir diğer önemli boyut da veri taşınabilirliği ve sağlayıcılar arasında geçiş yapabilme imkânının genişlemesidir. Böylece kullanıcılara, farklı platformlarda kendi verilerini etkin biçimde değerlendirme ve dilediklerinde verilerini alternatif hizmet sunucularına taşıma özgürlüğü tanınmaktadır. Bu yaklaşım, dijital pazarlarda rekabeti artırmakta ve yeni girişimlerin ortaya çıkmasına elverişli bir ortam hazırlamaktadır.

Bu bulgulardan hareketle etki analiz raporunda Veri Yönetişimi Yasası'nın 2028 yılı itibarıyla AB veri ekonomisinde 7,2 milyar avro ila 10,9 milyar avro aralığında doğrudan bir etki oluşturacağı belirtilmektedir. Yasa ayrıca yapay zekâ da dâhil olmak üzere veri temelli daha verimli hizmetler ve yeni ürünlerin geliştirilmesine katalizör görevi görerek yalnızca veri ekonomisine değil, aynı zamanda AB ekonomisi ve toplumuna da önemli ölçüde fayda sağlayacaktır.

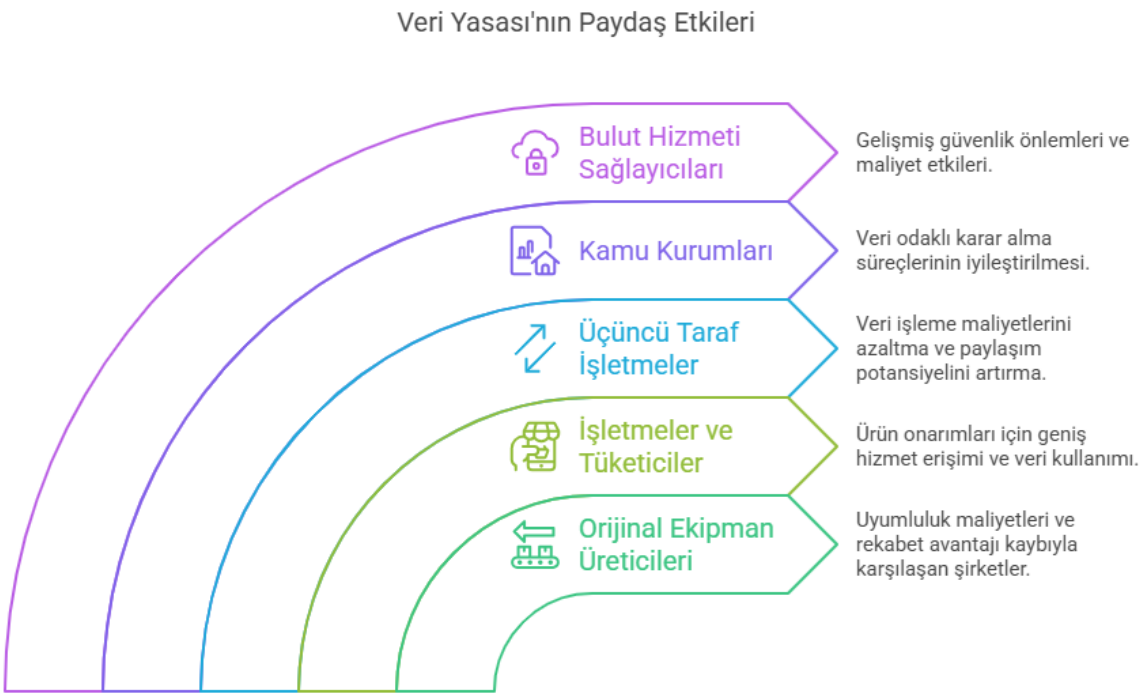
Rapora göre öngörülen yasal düzenlemenin AB ekonomisine kazanımları şu şekildedir:

- Nesnelerin İnterneti verilerinin kullanımıyla 2027 yılına kadar imalat sektöründe 1,3 trilyon €'ya varan potansiyel bir verimlilik artışı sağlanabileceği gibi;
- AB sağlık sektöründe de yılda yaklaşık 120 milyar € tasarruf edilebilecektir.
- Ayrıca verinin daha kolay erişilebilir olması sebebiyle yıllık 49,2 milyon €,
- Veri işleme ve yönetiminde maliyetin düşmesi sebebiyle yıllık 684 milyon € ve
- Avrupa Birliği Veri İnovasyon Kurulu'nun standardizasyon yönetimi sayesinde 5,3356 trilyon € tasarruf ve işlevsellik kazanımlarının elde edilmesi öngörülmektedir.
- Veriye erişimin kolaylaşması sayesinde daha iyi araştırma ve karar alma sebebiyle elde edilen kazanımlar ise 300 milyon € olarak belirtilmektedir.

Ancak düzenleme, elbette birçok maliyeti de beraberinde getirmektedir. Bu bağlamda raporda öngörülen maliyet kalemleri şu şekildedir:

- Kamu sektörünün elinde bulundurduğu verilerin yeniden kullanıma açılabilmesi için öngörülen masraflar veri sahibi kamu otoriteleri için yıllık 7.6 milyon €,
- Aracı veri hizmetleri sağlayıcıları için tek sefere mahsus 286.4 milyon ve yıllık 16.5 milyon €; yeniden kullanıcılar için yıllık 41.8 milyon € olarak belirtilmektedir.
- Ayrıca aracı veri hizmeti sağlayıcılarının akreditasyon için ilk seferde 20.000-50.000 € arası, yıllık ise 20.000-35.000 € arası maliyetlere katlanması öngörülmekte,
- Son olarak veri paylaşımı altyapısının kurulması ve işletilmesi için özel sektör ve kamu için yıllık 280.000 € civarında bir masraf öngörülmektedir.

b. AB Veri Yasası Etki Analizi Raporu



Veri Yasası'na ilişkin hazırlanan etki analizi raporunda[44] Veri Yasası'ndan etkilenecek olan aktörlerin en başında "orijinal ekipman üreticisi" (OEM - original equipment manifacturer) zikredilmektedir. Orijinal ekipman üreticileri, diğer teşebbüslere ürün, ürün bileşenleri ya da ekipman sağlayan, dolayısıyla OEM'nin ürünlerini kendi markalarına dahil edecek veya kendi ürünleri olarak satacak olan diğer teşebbüslere satan teşebbüslerdir. BU teşebbüslerin yeni düzenlemelerle birlikte uyum maliyetleri, hukuki danışmanlık giderleri ve ürün tasarımlarını adapte etme ihtiyaçları gibi çeşitli ek yükümlülüklerle karşılaşabilecekleri belirtilmektedir. Ayrıca, satış sonrası hizmet (aftermarket) pazarında sahip oldukları rekabet avantajını yitirme endişesi taşıyan büyük ve orta ölçekli şirketler, yasal düzenlemenin getirdiği artan şeffaflık ve veri paylaşımı neticesinde, müşteri verilerinin üçüncü taraflarca da işlenebilmesine yönelik adaptasyon süreçlerini yönetmek durumunda kalacaklardır.

Veri Yasası'nın etkileyeceği bir diğer grup, ürünleri aktif biçimde kullanan işletmeler ile bireysel tüketicilerdir. Zira Veri Yasası'nın uygulama alanına dahil olan ürünler bozulduğunda veya bakıma

[44] https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act.

ihtiyaç duyduğunda, kullanıcılar daha geniş bir yelpazedeki tamir ve bakım hizmetlerinden yararlanabilecek; bu da gereksiz yeni ürün satın alımlarının önüne geçebilecektir. Özellikle tarım sektöründe faaliyet gösteren çiftçilerin, ürünlerden gelen verileri hassas tarım tekniklerinde kullanarak verimliliği artırmaları, hava koşullarının yarattığı riskleri azaltmaları ve gübre, pestisit ile su tüketimini düşürmeleri mümkündür. Lojistik alanında şirketler, emisyon verilerini detaylı analiz ederek CO2 salımlarında neredeyse yarıya yakın düşüş sağlayabilecek ve inşaat sektöründe de atık miktarını yüz milyonlarca ton düzeyinde azaltma imkânı doğabilecektir.

Tüketiciler açısından bakıldığında ise üretilen veri artık sadece kişisel verilerle sınırlı kalmadan tüm kullanım verileri şeklinde erişilebilir hale gelecek ve kişilerin bu verileri nasıl değerlendireceklerine kendilerinin karar verebilmeleri mümkün olacaktır. Böylece, kullanıcılara tanınan veri erişim ve veri paylaşımı serbestisi, dijital pazarlarda rekabet ve inovasyon ortamının güçlenmesine katkıda bulunabilecektir.

Öte yandan, bu ürünlerden elde edilen verileri yeniden işlemek veya ticari faaliyete dönüştürmek isteyen üçüncü taraf işletmeler de önemli bir paydaş grubunu oluşturmaktadır. Birlikte çalışabilirlik (interoperability) konusundaki düzenlemelerin hayata geçirilmesi sayesinde, bu işletmelerin veri işleme maliyetlerini yaklaşık %30 oranında azaltması ve mevcut veri paylaşım potansiyelinin %40'ını aşan kayıpları önlemesi mümkün hale gelecektir.

Kamu kurumları açısından bakıldığında ise özel sektör elindeki verilere erişimin kolaylaştırılması, çeşitli alanlarda kamu yararı ve acil durumlar için gerekli veri talebinde bulunma süreçlerini iyileştirebilir. Örneğin ekonomik kayıplar hakkında bilgi toplanması, iklim değişikliğine uyum politikalarının oluşturulmasında daha isabetli risk değerlendirmeleri yapılmasını sağlayarak çevresel ve toplumsal etkilerin yönetimine katkıda bulunabilir. Kamusal istatistik, halk sağlığı ve çevre koruması gibi başlıklarda veri temelli karar alma süreçlerinin güçlenmesi beklenmektedir.

Veri Yasası'nın önemli bir diğer etki alanı, bulut hizmeti sağlayıcıları ve bu hizmetleri kullanan şirketler üzerinde görülmektedir. Önde gelen bulut hizmeti sağlayıcıları, hâlihazırda şifreleme, rol tabanlı erişim denetimleri, sertifikasyon ve raporlama gibi çeşitli koruma önlemlerini uygulamaktadır. Buna karşılık, yeni düzenlemelerin benimsenmesiyle birlikte daha gelişmiş güvenlik önlemlerinin de yaygınlaşması beklenmektedir. Bu tür ek tedbirlerin bir kısmı bulut hizmeti sağlayıcılarına ek maliyet getirse de, uyumluluk ve güvenlik avantajları uzun vadede rekabetçi avantaj sağlayabilir. Bulut hizmetlerini kullanan şirketler ise, veri birlikte çalışabilirliği şartlarının yerleşmesiyle işlem maliyetlerinde düşüş

eğilimi yaşayabilir. Yapılan hesaplamalar, bu nedenle ortaya çıkabilecek yıllık faydanın 7,1 milyar avro düzeyinde olabileceğine işaret etmektedir.

Satış sonrası servis (aftermarket) sektöründe faaliyet gösteren şirketlerin büyük bölümü KOBİ niteliğinde olduğundan, veri paylaşım düzenlemeleri bu kesimi yakından ilgilendirmektedir. KOBİ'ler, büyük şirketlerle yaptıkları sözleşmelerde Veri Yasası'nın haksız şartlara ilişkin hükümler sayesinde hukuki danışmanlık giderlerini azaltabilecektir. Bunun yanı sıra, küçük ve mikro ölçekteki işletmelerin, makinalardan veya ürünlerden kaynaklanan veri paylaşımında genel olarak muaf tutulması, bu tür işletmelerin idari ve mali yüklerini hafifletmektedir.

Veri paylaşımı ve birlikte çalışabilirlik standartlarının geliştirilmesinden sorumlu kuruluşlar, her bir standart için yaklaşık 1 milyon avroluk maliyetle karşılaşabilir. Bu rakam, ortak ve uyumlu standartların hazırlanması için gerekli teknik çalışmalar, test süreçleri, danışmanlık ve uzlaşma toplantılarını kapsamaktadır. Ancak bu maliyetin, piyasanın genelinde yaratacağı uzun vadeli verimlilik ve inovasyon artışı ile dengelenmesi beklenmektedir.

Buradan hareketle yapılan maliyet hesabına bakıldığında, Veri Yasası'nın 2028 yılına kadar AB-27'nin GSYİH'sini %1,98 artıracağı, 2024-2028 döneminde hükümet gelirlerini 96,8 milyar EUR, yatırım faaliyetlerini ise 30,4 milyar EUR artıracağı öngörülmektedir. Ayrıca söz konusu opsiyonun ek olarak 2,2 milyon yeni iş imkânı sağlayacağı belirtilmektedir. Bu bağlamda;

- **Bağlantılı ürünler ve ilgili hizmetleri kullanan tüketiciler ile şirketlerin güçlendirilmesi** ve ticari kullanım ile inovasyon için veri mevcudiyetinin artırılması, 2028 yılına kadar yıllık 196,7 milyar €'ya kadar ek gelir sağlayacaktır.
- **Sözleşmesel adilliğin iyileştirilmesi**, yıllık 7,4 milyar € ek gelir yaratacaktır.
- **Kamusal yarar amaçları doğrultusunda ticari olarak elde tutulan verilerin kullanımının kolaylaştırılması**, yıllık 155 milyon €'ya kadar idari yüklerin azalmasını sağlayacaktır.
- **Adil ve güvenilir bulut ve uç hizmetlerine erişimin kolaylaştırılması**, yıllık 7,1 milyar € ek gelir getirecektir.

Buna karşılık düzenlemenin sebebiyet vereceği masraflar ise şu şekilde hesaplanmıştır:

- **Üreticilerin, B2C veya B2B bağlamında erişim sağlama zorunluluğu** ve bununla ilgili teknik altyapılar:
    - Bir kerelik maliyetler: 410 milyon €
    - Yıllık tekrar eden maliyetler: 88 milyon €
- **Sözleşmesel adaletin sağlanması**: Yıllık 69 milyon €
- **İş dünyasından kamuya veri paylaşımı**:

- Bir kerelik maliyetler: 552,5 milyon €
- Yıllık tekrar eden maliyetler: 78,1 milyon €

- **Birlikte çalışabilirlik gereksinimleri**: Her bir standart için 1 milyon €.

c. AB Ürün Sorumluluğu Direktifi Etki Analizi Raporu

Etki analiz raporunda[45] yer verilen bilgilere göre yeni Ürün Sorumluluğu Direktifi, yazılım veya dijital unsurlara sahip ürünlere ilişkin kusursuz sorumluluk esasını genişleterek üreticilere daha öngörülebilir

[45] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en.

bir hukuki çerçeve sunmayı hedeflemektedir. Ürün güvenliğiyle doğrudan bağlantılı yazılımlar ile dijital hizmetler, döngüsel ekonomiye katkı sağlayan ürünler ve hatta dijital mülkiyet kavramına dâhil edilebilecek unsurlar, bu çerçevede Direktif kapsamına alınmaktadır. Ancak sorumluluğun genişletilmesi elbette üreticiler açısından risk anlamına gelmektedir. Maliyet boyutunda bakıldığında, sorumluluk sigortası bulunan üreticiler, artması muhtemel sigorta primlerinden etkilenecektir. Buna karşılık, bu üreticilerin sigorta poliçeleri kusurlu ürün kaynaklı zararlar nedeniyle ödenecek tazminatları ve yargılama giderlerini karşılayabilecektir. Sigorta yaptırmamış üreticiler ise benzer bir durumda zarar görenlerin zararlarını doğrudan tazmin etmek ve ihtilafın yargıya taşınması hâlinde hukuki masrafları üstlenmek zorunda kalabilecektir.

Diğer yandan sigorta şirketlerinin, kusurlu ürünün sebep olduğu zararlara ilişkin tazminat ödemelerinde artış yaşaması mümkündür. Ancak bu artış, sigorta primlerinde yapılacak sınırlı yükseltmelerle telafi edilebileceğinden, rapora göre uzun vadede sigorta şirketlerinin gelir akışlarında önemli bir değişiklik beklenmemektedir.

Nihayet düzenlemenin tüketici boyutunda yarattığı temel etki, kişilerin uğradığı zararın tazmini için üreticileri sorumlu tutabilme imkânının güçlenmesi ve böylelikle zararın karşılanması olasılığının yükselmesidir. Özellikle dijital bileşenlere veya doğrudan yazılıma sahip ürünlerin yol açabileceği zararları tazmin edebilir hale getiren bu yaklaşım, aynı zamanda siber güvenliğin teşviki yönünde de etki doğurmaktadır. Zira, üreticiler, ürünlerini güvenli kılmak ve gerekli güncellemeleri sunmak için ek tedbirler almak üzere teşvik edilmektedir. Bunun yanı sıra, tüketicilerin dijital mülkiyet unsurları (örneğin dijital verilerin saklandığı ve işlendiği platformlar) zarar gördüğünde veya yok edildiğinde, mülkiyet hakkının bir uzantısı olarak zararlarının tazmini de Direktif çerçevesinde mümkün hale gelecektir.

Bütün bu bulgulardan hareketle Türk hukukunda gerçekleştirilecek olan bir uyum çalışması çerçevesinde de veriye ilişkin getirilecek düzenlemelerin getirisi, AB'de olduğu gibi sebebiyet vereceği masrafların çok daha ötesinde ise uyum opsiyonun tercih edilmesi elbette isabetli olacaktır. Buna karşılık uyumun maliyeti getirisinden daha yüksek olacaksa özel sektöre halihazırda karmaşık olan regülasyonlara ilaveten ek yük getirmek kanaatimizce isabetli olmayacaktır.

3. Uyum Opsiyonunun Tercih Edilmesi Halinde Dikkat Edilmesi Gereken Hususlar

Uyum opsiyonunun tercih edilmesi halinde yine hukuk politikası açısından bazı önemli hususların dikkate alınması gerekecektir. Şöyle ki Avrupa Birliği, veri ekonomisine ilişkin düzenlemelerinde veri ekonomisini bir bütün olarak düzenlemek yerine, belirli noktalara odaklanmayı tercih etmiştir. Gerçekten de veri ekonomisi içerisinde nesnelerin interneti cihazları, aracı veri hizmet sağlayıcıları, kamunun elinde bulundurduğu veriler, müşterek veri alanları gibi konular esas alınmakla birlikte, veri ekonomisinin bir bütün olarak düzenlemeye tabi tutulduğu bir düzenleme söz konusu değildir. Dolayısıyla düzenlemelerin konuları arasında bağlantı kurmak her zaman mümkün olmamaktadır. Türk hukukunda şayet uyum çalışmaları yapılacaksa, bu takdirde düzenlemelerin veri ekonomisini bir bütün olarak mı yoksa belirli unsurlarını mı esas alacağı hususunun açıklığa kavuşturulması gerekecektir. Bütüncül bir düzenleme elbette sistematik açıdan daha isabetli ve hukuk güvenliği açısından da daha nitelikli bir neticeye sebebiyet verebilecektir. Bununla birlikte bu bağlamda öncelikle veri ekonomisinden neyin anlaşılacağı, Türkiye'deki veri ekonomisinin ihtiyaçlarının neler olduğu gibi hukuk alanı dışında kalan önsoruların cevaplandırılması gerekecektir.

Türkiye'de münhasıran veri ekonomisine ilişkin resmi bir çalışma ve istatistik -görebildiğimiz kadarıyla- mevcut olmasa da, bilgi ve iletişim teknolojileri sektörüne ilişkin Tübisad ile Deloitte

tarafından hazırlanan 2023 Pazar Verileri raporunda önemli bilgiler mevcuttur[46]. Bunlardan ilki, milli teknoloji hamlesinin kalbinde olduğu belirtilen bilişim sektörünün[47] Türkiye'deki pazar hacminin 784,6 milyar TL teşkil ettiğidir. Üstelik 2023 yılında kaydedilen bu artış, bir önceki yıla göre %83'lük bir oranda gerçekleşmiştir. Belirtilen rakamın 382,4 milyar TLsi iletişim teknolojilerine ilişkin, buna karşılık 402,2 milyarlık pay ise bilgi teknolojilerine ilişkin olarak kayıtlara geçmiştir. Bilgi teknolojileri kısmında ise en büyük pay, donanım ve hizmetten önce yazılım sektörüne ait olmuş, bu bağlamda 206,9 Milyar TL'lik bir pazar büyüklüğünden bahis açılmıştır. İhracat rakamlarına bakıldığında ise yine yazılım ihracatının %92lik bir değişim oranıyla 57,6 milyar TL olduğunu belirtmekte fayda olacaktır. Söz konusu yazılım teşebbüsleri ise bankacılık/finans uygulamaları, karar destek sistemleri, siber güvenlik, telekom ve network uygulamaları, web teknolojileri, kurumsal kaynak planlama modülleri, gömülü sistemler ve oyun sektörlerinde faaliyet göstermekle birlikte en büyük pay, bankacılık ve finans uygulamalarına ait olmuştur. Dolayısıyla yazılım sektörünün hem bilişim sektörü, hem de ihracat açısından büyük önem arz ettiğini belirtmek isabetli olacaktır. Bu verilerden hareketle bilişim sektörü açısından yazılım sektörünün menfaatlerinin dikkate alınması, bu alandaki istihdamın teşvik edilmesi, ihracatın artırılması için gerekli altyapının sağlanması isabetli gözükmektedir.

Ayrıca Birlik hukukundaki düzenlemeler çerçevesinde kişisel verilerin korunmasına ilişkin mevzuat hükümleri de saklı tutulmuştur. Bu netice, Avrupa Birliği'nin kişisel verilerin korunmasına verdiği önemin bir göstergesidir. Bununla birlikte Türk hukukunda da Anayasa mertebesinde korunan bu hakkın veri ekonomisi ve veriye tedavül niteliği kazandırma amacıyla kısıtlanıp kısıtlanmayacağı sorusuna da cevap vermek gerekecektir. Nitekim görüldüğü üzere kişisel verilerin önemli bir ekonomik değer arz ettiği hususunda hiçbir tereddüt yoktur. Hal böyle olunca bu verilerden katma değer elde etme aşamasında hukuk düzenimizin bütünüyle koruyucu şekilde yaklaşmasının isabetli olup olmadığının sorgulanması gerekmektedir. Kanaatimizce en azından araştırma-geliştirme ya da bilimsel çalışmalar gibi veriden katma değer elde edilmesi ihtimalinin yüksek olduğu faaliyetler çerçevesinde kişisel verilerin kullanımının kolaylaştırılması isabetli bir yaklaşım olacaktır. Aynı durum, fikri ve sınai haklar ve ticari sırlar gibi hukuken korunan diğer veri türleri açısından da söz konusu olacaktır.

[46] Bilgi ve İletişim Teknoloji Sektörü, 2023 Pazar Verileri, Mayıs 2024, https://www.tubisad.org.tr/tr/images/pdf/tubisad-bit-2023-tr.pdf

[47] Sanayi ve Teknoloji Bakan Yardımcısı Zekeriya Çoştu: "Bilişim sektörü Milli Teknoloji Hamlesi'nin tam kalbinde yer alan bir sektör. Bu bakımdan sektörün büyümesi, çeşitlenmesi, derinleşmesi ve ihracat potansiyelini artırması ülkemiz için son derece önemli bir öncelik.", https://www.aa.com.tr/tr/ekonomi/turkiye-bilgi-ve-iletisim-teknolojileri-sektorunun-buyuklugu-785-milyar-liraya-ulasti/3232917#:~:text=Rapora%20g%C3%B6re%2C%20T%C3%BCrkiye%20bilgi%20ve,%C3%B6l%C3%A7%C3%BCmlemeye%20yeni%20eklenen%20%C5%9Firketler%20olu%C5%9Fturdu.

Ürün sorumluluğu noktasında ise AB mevzuatına uyum, sadece AB pazarına ürün ve hizmet sunanlar açısından değil, bütün kullanıcılar açısından bir fayda sağlayacaktır. Kanaatimizce son dönemde artan siber riskler dikkate alındığında yazılımların da ürün kavramına dahil edilmesi, bu sayede hukuki belirliliğin sağlanması, üreticiler açısından her ne kadar belirli maliyetlere sebebiyet verecekse de, kanunda yazılımların da açıkça zikredilmesi, bu risklerin de artık sigortalanabilir olduğu anlamına gelecektir. Kaldı ki yazılımlar ile siber risklerin de Birlik hukukunda ürün sorumluluğuna dahil edilmesi, Türkiye'den Avrupa Birliği'ne gerçekleştirilecek yazılım ihracatı açısından da önem taşıyacaktır. Burada yapılacak uyum faaliyetleri, hem Türkiye iç pazarında dijital ürünlerin daha güvenli olmasına, hem de Birlik hukukuna uyum ve ihracatın kolaylaşmasına sebebiyet verecektir.

B. Yöntem

1. Yatay İlişkide Veriye Erişim Hakkına İlişkin Yöntem

Özel hukuk süjeleri arasındaki ilişkide verinin hangi hukuki çerçevede alışverişe konu olacağı hususu son yıllarda çokça tartışmalara sebebiyet vermiştir. Bu bağlamda özellikle veri üzerinde bir mülkiyet hakkının tanınıp tanınmaması gerektiğine ilişkin farklı görüşler ortaya atılmıştır. Ancak veriyi mülkiyet hakkının konusu olan eşyadan ayıran en önemli özelliği, birden fazla kişi tarafından aynı zamanda kullanılabilirliği ve bu takdirde de tüketiminin söz konusu olmayışıdır. Buradan hareketle herkese karşı ileri sürülebilecek mutlak hak niteliğindeki mülkiyet hakkının veriler üzerinde tahsis edilmesinin birçok soruna sebebiyet vereceği aşikardır ve bu sebeple çoğunluktaki görüş veri üzerindeki mülkiyet hakkını reddetmiştir. Netice itibariyle de Birlik hukukunda veri üzerinde mülkiyet hakkı yaklaşımı reddedilmiş, bunun yerine farklı aktörlere erişim yetkisi tanınmıştır.

Kanaatimizce Türk hukukunda da AB veri hukuku düzenlemelerine uyum sağlanacağı takdirde veri üzerinde mülkiyet hakkının benimsenmesi yerine veriye erişim hakkının öngörülmesi daha isabetli olacaktır. Aksi takdirde verinin niteliği ve mülkiyet hakkı çerçevesinde yaşanacak sorunlar bir yana, uluslararası düzlemde de veriyi mülkiyet hukuku çerçevesinde koruyan tek ülke Türkiye olacak, bu farklılık, ülkemizi veri ekonomisinde tercih edilmeyecek bir ülke statüsüne büründürecektir.

Diğer taraftan erişim yetkisinin şartlarının da belirlenmesi gerekecektir. Şöyle ki AB erişim yetkisini nesnelerin interneti cihazlarıyla sınırlı kılmıştır. Buna karşılık AB hukukunda halihazırda Genel Veri Koruma Tüzüğü bağlamında kişisel veriler için ve Dijital Piyasalar Yasası'nda (Digital Markets Act) eşik bekçileri aleyhine ve kullanıcılar lehine bir veri taşıma hakkı mevcuttur. Türk hukukuna bakıldığında ise veri taşınabilirliği hakkının kişisel verilerin korunması bağlamında tanınmadığı, buna karşılık elektronik ticaret hukukunda elektronik ticaret aracı hizmet sağlayıcı ile elektronik ticaret

hizmet sağlayıcı ilişkisinde öngörüldüğünü söylemek mümkündür. Dolayısıyla öncelikle piyasa ihtiyaçlarını tespit etmek, veri taşınabilirliği hakkının veriden katma değer elde etmeye hizmet edebileceği sektörleri belirlemek ve bu sektörlerde bilhassa veri taşınabilirliği, veriye erişim haklarını öngörmek kanaatimizce isabetli bir yaklaşım olacaktır. Bu bağlamda yine bütüncül bir etki analiz raporunun kaleme alınması isabetli olarak değerlendirilmektedir. Buna karşılık genel bir veri taşınabilirliği hakkının öngörülmesi kanaatimizce yönetilebilir olmayacak ve -hak sahibinin kimler olacağı, erişim/taşımanın esas ve usulü gibi- birçok hukuki belirsizliği de beraberinde getirecektir. Diğer yandan hukuk politikası tercihi münhasıran AB mevzuatına uyum sağlamaksa, erişim hakkını nesnelerin interneti cihazlarıyla sınırlandırmak yeterli olacaktır.

Veri Yasası'nın bir diğer önemli konusu veri hizmetlerine ilişkindir. Türkiye'de de bu tür hizmetlerden istifade edilmektedir. Bu bağlamda piyasadaki büyük aktörlerin ekonomik gücünü kullanıp müşteriler üzerinde bir bağımlılık ilişkisi yaratması söz konusu ise bunun rekabete ilişkin olumsuz sonuçlarının tespit edilmesi, bu tespitin akabinde de tıpkı Veri Yasasında olduğu gibi eş zamanlı olarak birden çok hizmet sağlayıcıdan hizmet alınmasını mümkün kılan ya da bunlar arasında değişimin kolaylaştırılacağı düzenlemelere yer vermek isabetli olacaktır.

2. Dikey İlişkide Veriye Erişim Hakkına İlişkin Yöntem

Öncelikle belirtelim ki kamu ile birey arasındaki ilişkide AB mevzuatına uyum sağlanması, kural olarak Türkiye'den Avrupa Birliği'ne ürün ya da hizmet ihracatı açısından herhangi bir öneme sahip değildir. Bir diğer ifade ile Veri Yönetişimi Yasasında kamunun elinde bulundurduğu verilerin yeniden kullanımı açısından öngörülen düzenlemelerin Türkiye'den Avrupa Birliği'ne ürün ya da hizmet satmak isteyen üreticiler açısından herhangi bir etkisi olmayacaktır. Dolayısıyla kanun koyucunun hukuk politikası münhasıran AB mevzuatına uyum sağlamaksa, veri yönetişimine ilişkin düzenlemelere uyum sağlamaya gerek olmayacaktır.

Ancak Türk kanun koyucusunun hukuk politikası, Türkiye'deki veri ekonomisinin güçlendirilmesi, veriden katma değer elde edilmesinin mümkün kılınmasıysa, bu taktirde veri yönetişimine ilişkin düzenlemelere benzer düzenlemelerin Türk hukukunda da öngörülmesinde isabet bulunmaktadır. Bunları kamunun elinde bulundurduğu verilere erişim ile aracı veri hizmeti sağlayıcılarına ilişkin düzenlemeler olarak ikiye ayırmakta fayda olacaktır.

Kamunun elinde bulundurduğu verilere erişim bağlamında ise Türkiye'nin kamu hizmetlerinin dijitalleşmesi noktasında halihazırda olumlu tecrübelere sahip olduğunu tespit etmek mümkündür. Buradan hareketle kamunun elinde bulundurduğu verilere yeniden kullanım amacıyla erişim

mekanizması Türkiye'de şu şekilde olabilecektir: e-devlet üzerinde oluşturulan bir merkezi başvuru noktasında kamunun çeşitli birimleri, elinde bulundurdukları verilere erişim, erişim ücreti, erişim şartları gibi hususları ilan edecektir. Bu şartları sağladığını düşünen bireyler, merkezi başvuru noktası üzerinden çeşitli kurumlara taleplerini iletecektir. İlgili kurum, bu talebi değerlendirip olumlu ya da olumsuz kararını bildirecektir. Bu çerçevede Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, bütün hizmetleri koordine eden, çeşitli kurumlar ve bireyler arasındaki iletişimi sağlayan, kurumları verinin hazırlanması, anonimleştirilmesi, aktarılması, iletilmesi, ilgili standart sözleşmelerin hazırlanması gibi süreçlerde destekleyecektir.

Bu bağlamda ayrıca AB örneklerinden de istifade etmek mümkündür. Zira Birlik, yasama sürecinde de özellikle Finlandiya'nın sosyal ve sağlık verilerini belirli şartlar altında kullanıcılara sunduğu "FINDATA" örneğini zikretmiştir[48]. İlgili otoritenin websitesinde hangi verilerin kimler tarafından ve hangi şartlar altında sunulduğu belirtilmekte, ayrıca ilgili kişilere de haklarına ilişkin bilgilendirme yapılmaktadır. Dolayısıyla FINDATA örneği Türkiye uygulaması açısından da dikkate alınabilecektir.

Aracı veri hizmet sağlayıcıları açısından öngörülebilecek düzenlemeler ise daha farklıdır. Şöyle ki AB hukukunda aracı veri hizmeti sağlayıcılarına ilişkin bir sicil kaydı öngörülmekte, ayrıca bu kişilerin kanunda öngörülen şartları yerine getirmeleri beklenmektedir. Türk hukukunda da kişisel verilerin korunması hukuku bağlamında VERBİS sicil kayıt sistemi mevcuttur. Burada edinilen tecrübelerden hareketle aracı veri hizmeti sağlayıcılarına yönelik bir sicil kayıt sistemi öngörülebilecektir. Bununla birlikte böyle bir düzenlemenin Türk veri ekonomisine katkıdan çok zararının da olması ihtimal dahilindedir. Nitekim söz konusu yükümlülükler, aracı veri hizmet sağlayıcıları açısından maliyet anlamına da gelecek, dolayısıyla söz konusu aktörler bu maliyetlerin olmadığı diğer ülkeleri tercih edebilecektir. Bununla birlikte aracı veri hizmet sağlayıcılarına yönelik düzenlemeler, aynı zamanda kamu tarafından oluşturulacak olan veri alanlarına da dayanak teşkil etmektedir. Özellikle sektör bazında öngörülen sağlık verisi alanı gibi kamu denetim ve gözetiminde verinin ortak kullanımını öngören inovatif yöntemler açısından söz konusu düzenlemeler önem taşımaktadır.

Kanaatimizce AB hukukuna uyumdan bağımsız olarak kamu tarafından oluşturulan, kamunun gözetim ve denetiminde olan, yüksek güvenlikli, gerekli idari ve teknik tedbirlere uyum sağlayabilen herkesin eşit şartlar altında erişimine açık veri alanlarının oluşturulması, Türk ekonomisi açısından son derece önemli bir hususdur.

[48] https://findata.fi/en/.

3. Ürün Sorumluluğuna İlişkin Yöntem

Ürün sorumluluğu bağlamında şayet AB mevzuatına uyum sağlanacaksa, 7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanunu açısından yapılması gereken birçok değişiklik söz konusu olacaktır. Şöyle ki;

AB hukukunda mevcut olan ürün güvenliği ile ürün sorumluluğu ilişkisinin Türk hukukunda yeniden gözden geçirilmesi gerekmektedir. Zira her ne kadar aynı amaca hizmet etseler de Birlik hukukunda ürün güvenliği mevzuatı ile ürün sorumluluğu mevzuatı birbirinden bağımsız iki farklı düzenleme olarak ele alınmıştır. Ürün güvenliği düzenlemeleri, kamu hukuku kaynaklı olup, kanun koyucunun ürünlere ilişkin öngördüğü risklerin önlenmesini amaçlamaktadır. Ancak bu risklerin bütünüyle tespit edilmesi ve bu doğrultuda düzenleme yapılması mümkün olmayacağı için, bir "güvenlik ağı" sıfatıyla ürün sorumluluğu hukuku devreye girmektedir. İşte özel hukuk kaynaklı olan ürün sorumluluğu hukuku, her ne kadar ürün güvenliği hukukuyla benzer amaçlar gütse de, işlev bakımından daha geniş bir uygulama alanına sahiptir. Kanun koyucunun ürün güvenliği mevzuatı kapsamında öngöremediği risklerden kaynaklanan zararları da kusursuz sorumluluk çerçevesinde telafi etmeyi amaçlayan ürün sorumluluğu hukuku bu açıdan daha geniş bir uygulama alanına sahip olmakta, ürün güvenliği hukukunun öngöremediği riskler açısından bir "güvenlik ağı" işlevi görmektedir. Nitekim bu bağlamda yeni Ürün Sorumluluğu Direktifi, bir ürünün hatalı olup olmadığını tayin ederken ürün güvenliği hükümlerine uyumlu olmayı münhasıran yeterli görmemektedir. Bilakis Ürün Sorumluluğu Direktifi md. 7 bağlamında ürünün hatalı olup olmadığını değerlendirirken ürün güvenliği mevzuatına riayet edilmiş olması hususu, örnekseme yoluyla sayılan dokuz kriterden sadece bir tanesidir. Bir diğer ifade ile ürün güvenliği mevzuatına riayet edilmiş olması iktisadi işletmeciyi doğrudan sorumluluktan muaf kılmaya yeterli değildir. Buna karşılık 7223 sayılı Kanun'un ürün sorumluluğuna ilişkin md. 6 hükmünde ürün güvenliğine riayet edilmiş olması, iktisadi işletmecinin sorumluluktan kurtulması için yeterli gözükmektedir. Buradan hareketle ürün güvenliği mevzuatına uyum, ürün sorumluluğunu da ortadan kaldırmakta, dolayısıyla ürün sorumluluğu hukuku, ürün güvenliği hukukunda öngörülmeyen riskler açısından "güvenlik ağı" işlevini kaybetmektedir[49].

Belirtilen bu sorunlardan hareketle her ne kadar yapay zekâ ya da siber güvenlik alanında ürün güvenliği ekseninde AB hukukunda yapılan düzenlemeler Türk hukukuna iktibas edilse de, bu düzenlemeler kapsamında öngörülmeyen riskler açısından bireyler, yukarıda işaret edilen ürün güvenliği ile ürün

[49] Konu hakkında daha geniş bilgi için bkz. Çekin, Güncel Gelişmeler Işığında AB ve Türk Hukukunda Dijital Ürünlere İlişkin Ürün Sorumluluğu ve Ürün Güvenliği Düzenlemeleri Üzerine Değerlendirme, Türk-Alman Üniversitesi Hukuk Fakültesi Dergisi, Y. 2025, C. 7 S. 1, s. 156 vd.

sorumluluğu arasındaki mutlak ilişki sebebiyle korumasız kalacaktır. Dolayısıyla söz konusu düzenlemelerin bireyleri korumak yerine onların aleyhine sonuç doğurması dahi ihtimal dahilindedir.

Türk hukukunda ürün sorumluluğuna ilişkin mevzuat kapsamında ayrıca "dijital ürünlere" ilişkin herhangi bir düzenleme mevcut değildir. Hatta yazılım gibi gayrı cismani varlıkların "ürün" kavramına dahil edilip edilmemesi konusu dahi tartışmalıdır. Bunun ötesinde bu tür ürünlere mahsus risklerin de ürün sorumluluğu hukuku açısından özel olarak ele alınması, bu bağlamda sadece maddi hukuk değil, bilhassa ispat hukuku açısından da tüketicileri koruyucu düzenlemelerin hayata geçirilmesi gerekecektir.

Yine bağlamda rizikonun sigortalatılabilmesi, sorumluluğun genişletilmesinin yazılım sektörüne maliyeti gibi hususların da önceden araştırılması, bir etki analizi raporu yapılması kanaatimizce isabetli olacaktır.

2. Kısım: Avrupa Birliği'nde Siber Güvenliğin Regülasyonu

Siber Dayanıklılık Yasası İncelemesi

I. Giriş

Dünyada siber güvenlik tehditleri artmakta, tehditler şekil ve nitelik değiştirmekte, bu tehditlerin etkilediği alanlar farklılaşmaktadır. Siber tehditler, kişilerin sadece verilerini veya bilişim sistemlerini değil kişilerin mal ve can güvenliği tehlikeye atılmaktadır. Kişilerin özel hayatlarının mahremiyetinden ticari faaliyetlerine kadar çok geniş bir yelpazede etki etmektedir. Bir uygulamadaki veya cihazdaki siber güvenlik riski, tüm ekonomiyi ve toplumsal faaliyetleri felç edebilmektedir. Bu söylemler artık teorik düzlemde kalmamakta bizatihi tecrübe edilmektedir.

Dijitalleşmenim en büyük çıkmazı güvenlik sorunudur. Diğer tüm regülatif güçler gibi Avrupa Birliği de bu güvenlik çıkmazını hukuk kurallarıyla ortadan kaldırmaya çalışmıştır. AB içerisinde bilişim sistemlerinin güvenliğine yönelik düzenlemeler uzun yıllar içerisinde geliştirilmiştir. Düzenlemelerin bu şekilde zamana yayılmasının sebebi değişen risk ortamına göre tepki gösterilmiş olmasıdır. Diğer bir deyişle, güvenlik risklerinin niteliğine göre farklı enstrümanlarla karşılık verilmiştir.

AB'de siber güvenlikle bağlantılı ilk hukuki düzenleme 1992 yılında kabul edilmiş olan 92/242/EEC sayılı Konsey kararıdır.[50] Karar, çok temel bir belge niteliğindedir ve Avrupa Komisyonu'na elektronik olarak depolanan, işlenen veya iletilen bilgilerin kullanıcılarına ve üreticilerine, bilgi sistemlerinin kazara veya kasıtlı tehditlere karşı uygun şekilde korunmasını sağlamayı amaçlayan genel stratejilerin geliştirilmesi için eylem planı hazırlama ödevi vermiştir.

AB genelinde güvenliğe yönelik en önemli gelişme 1995 yılında kişisel verilerin korunmasına yönelik 95/46/AT sayılı AB Direktifinin kabul edilmesi olmuştur.[51] 95/46 sayılı Direktif, genel bir bilgi güvenliği düzenlemesi niteliğinde olmasa da kişisel verilerin korunmasına yönelik açık talimatlar içerdiği için dolaylı olarak siber güvenliğin sağlanmasına hizmet etmiştir.[52] Bu düzenleme kabul edilmeden önce, bilgi güvenliği ve veri koruması üye devletler tarafından ulusal düzeyde

[50] 92/242/EEC - Council Decision of 31 March 1992 in the field of security of information systems, OJ L 123, 8.5.1992.
[51] EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, L 281 23.11.1995.
[52] 95/46 sayılı Direktifin 'İşleme güvenliği' başlıklı 17. maddesinde belirtildiği üzere "*Üye devletler veri sorumlularının, özellikle işleme faaliyetinin verilerin bir ağ üzerinden aktarılmasını içerdiği hallerde, kişisel verilerin kazara veya yasadışı imhasına veya kazara kaybına, değiştirilmesine, yetkisiz ifşasına veya erişimine ve diğer tüm yasadışı işleme biçimlerine karşı korunmasına yönelik uygun teknik ve organizasyonel tedbirleri uygulamalarını temin etmeleri zorunludur.*".

yönetilmekteydi. Her ülkenin kişisel verileri korumak ve bilgi güvenliğini sağlamak için kendi iç hukuk düzenlemeleri bulunmaktaydı ve AB genelinde bütüncül bir yaklaşım bulunmamaktaydı.[53]

Kişisel verilerin korunmasına yönelik temel çerçeveyi çizen 95/46 sayılı Direktif, üye devletler tarafından iç hukuka aktarılmaya başlanmıştır. Bir yandan da sektörel düzenlemelere ağırlık verilmiştir. İlk kapsamlı düzenlemeye alınan sektör elektronik haberleşme sektörü olmuştur.

Elektronik haberleşme sektöründe kişisel verilerin korunması ve mahremiyetin sağlanması amaçlı ilk düzenleme 97/66/AT sayılı Elektronik Haberleşmede Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifidir.[54] Bu düzenleme de siber güvenlik düzenlemesi olmasa da bilgi güvenliğine yönelik getirmiş olduğu kurallar dolaylı olarak siber güvenliğin sağlanmasına hizmet etmiştir.[55] Söz konusu düzenleme, gelişen teknolojiler ve değişen elektronik haberleşme piyasalarının gerekliliklerine uyum sağlamak için hazırlanmış, ancak zamanla yetersiz kalmıştır. Bu doğrultuda, 2002/58 sayılı Elektronik Haberleşmede Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifle ilga edilmiştir.[56] Elektronik haberleşme alanına ilişkin en kapsayıcı düzenleme olan bu Direktif de 2009/136 sayılı Direktifle değişikliğe uğramıştır.[57] 2009/136 sayılı Direktif, çerezlerden davranışsal reklamcılığa kadar uygulanabilecek çok geniş spektrumda kurallar getirdiği için bu düzenleme AB Çerez Direktifi olarak da anılmaktadır.

Kişisel verilerin düzenlenmesi sonrasında siber güvenliğe ilişkin ilk kapsamlı çalışma 2005 yılında atılmıştır. 2005/22/JHA sayılı Konsey Çerçeve Kararıyla bilgi sistemlerine yönelik saldırılar konusu ilk

---

[53] Örneğin, Almanya'nın kendi ulusal bilgi güvenliği düzenlemesi bulunmaktaydı. 1991 yılında kurulan BSI (*Bundesamt für Sicherheit in der Informationstechnik*), bilişim sistemlerinin güvenliğini sağlamak ve kritik altyapıyı güvenlik açıklarından korumakla görevlendirilmiştir. Bkz. **John A. Foulks** (2018) German IT Security Law, 6(2) Journal of Law & Cyber Warfare 165-190; 95/46 sayılı Direktiften önce Fransa, bilgi güvenliğini çeşitli ulusal güvenlik stratejileri ve önlemleri aracılığıyla düzenlemiştir. Fransız Savunma Bakanlığı kritik altyapıların ve hassas bilgilerin korunmasında önemli bir rol oynamıştır. Ayrıca Fransız Ulusal Güvenlik Konseyi bilgi güvenliği de dahil olmak üzere ulusal güvenliğin korunmasına yönelik çabaları koordine etmiştir. Bkz. Agence Nationale de la Sécurité Des Systèmes D'Information, Information systems defence and security - France's strategy, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/France_2011_2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

[54] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30.1.1998.

[55] 97/66 sayılı Direktifin 'Güvenlik' başlıklı 4. maddesi şu şekildedir: "*Kamuya açık bir telekomünikasyon hizmetinin sağlayıcısı, hizmetlerinin güvenliğini korumak için uygun teknik ve kurumsal tedbirleri almalı, gerekirse ağ güvenliği konusunda kamuya açık telekomünikasyon ağının sağlayıcısı ile birlikte hareket etmelidir.*"

[56] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31/07/2002.

[57] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ 2009 L 337.

defa AB genelinde düzenleme konusu yapılmıştır.[58] Bu Çerçeve Kararın amacı, bilgi sistemlerine yönelik saldırılar alanında üye devletlerdeki ceza hukukuna ilişkin kuralların yakınlaştırılması yoluyla, üye devletlerin polis ve diğer uzmanlaşmış kolluk kuvvetleri de dahil olmak üzere adli ve diğer yetkili makamları arasındaki iş birliğini geliştirmektir.

2005/22 sayılı Çerçeve Karar, ilk defa bilişim sistemini tanımlamış, bilişim sistemine girme, müdahale ve sistemi engelleme eylemlerinin tüm üye devletlerce suç olarak kabul edilmesini emretmiş ve bu eylemlerin suç olarak kabul edilmesi durumunda asgari verilmesi gereken cezalara ilişkin çerçeveyi belirlemiştir. Belirtmek gerekir ki, bu Çerçeve Karar, Budapeşte Sözleşmesi olarak da anılan Avrupa Konseyi Siber Suç Sözleşmesiyle oluşturulan yeni hukuki rejimle AB hukukunu uyumlaştırmaya çalışmıştır.[59]

2005/22 sayılı Çerçeve Karar bilişim suçları açısından suçsallaştırma ve işbirliği için temel çerçeveyi çizse de siber suçlarla mücadele için yetersiz kalmış ve 2013 yılında ilga edilerek yerini 2013/40/AB sayılı Bilişim Sistemlerine Saldırılara İlişkin Direktife bırakmıştır.[60] 2013/40 sayılı Direktif, AB üye devletlerinin iç hukukunun yeknesaklaştırma çalışmalarının bir ürünüdür.[61] Direktif, ceza hukuku bağlamında bilişim sistemlerine yönelik saldırılara ilişkin suçları ve cezaları AB nezdinde uyumlaştırmıştır.

Bu dönemde sektörel iki düzenleme de yürürlüğe konulmuştur. Bunların ilki, güven hizmetleri düzenlemesi veya EIDAS olarak da anılan 910/2014 sayılı AB Tüzüğüdür. [62] Bir diğeri ise radyo ekipmanlarına ilişkin bilgi güvenliği kuralları içeren 2014/53 sayılı Direktiftir.[63] Görüldüğü üzere, bu döneme kadar AB siber güvenlik konusunu doğrudan odağına almamış ceza hukuku ve iş birliği bağlamında meseleyi ele almıştır.

95/46 sayılı Direktifin üye devletler tarafından uyumlu şekilde iç hukuklarına aktarılamaması AB genelinde işlem maliyetini artıran bir unsur haline gelmiştir. Hem kuralların hem de yaptırımların

---

[58] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, L 69/67, 16.3.2005.
[59] Bkz. Council of Europe – Convention on Cybercrime, European Treaty Series – No. 185, Budapest, 23.XI.2001.
[60] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, L 218/8 14.8.2013.
[61] Bu konuda kapsamlı inceleme için bkz. **Adrian Cristian Moise** (2015) Analysis of Directive 2013/40/EU on Attacks Against Information Systems in the Context of Approximation of Law at the European Level, Journal of Law and Administrative Sciences 374-383.
[62] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, L 257/73 28.8.2014.
[63] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, L 153/62, 22.5.2014.

yeknesak uygulanmaması sebebiyle 95/46 sayılı Direktifin reform edilmesi gündeme gelmiştir. Mahremiyeti artırmak, veri koruma düzenlemelerini yeknesaklaştırmak, iş yapmayı kolaylaştırmak ve en önemlisi de büyük miktarlarda kişisel veri işleyen Amerikan teknoloji şirketlerinin hesap verebilirliğini temin etmek amacıyla AB 2016 yılında GDPR olarak da anılan Genel Veri Koruma Tüzüğünü kabul etmiştir.[64]

GDPR, kişisel verilerin teknik olarak korunması için kapsamlı bir çerçeve çizmiştir. GDPR önemli bir boşluğu dolduruyor olsa da siber güvenliğe ilişkin uçtan uca tüm hususları kapsar nitelikte değildir. Bu amaçla, GDPR kabul edildiği aynı dönemde AB NIS 1 olarak da anılan Şebeke ve Bilgi Güvenliği Direktifini kabul etmiştir.[65]

NIS 1 kritik altyapının korunmasına odaklanarak AB'deki genel siber güvenlik seviyesini artırmak için yatay yasal kurallar getirmiştir. 2022 yılında NIS 1 Direktifi ilga edilerek ve daha geniş kapsamlı NIS 2 Direktifi kabul edilmiştir.[66]

AB, 2019 yılında Birliğin temel siber güvenlik kurumu olan ENISA'nın yetkilerini artırdığı ve bilişim ürünleri, hizmetleri ve süreçlerinin siber güvenlik özelliklerine uygulanacak sertifikasyon programlarının düzenlendiği Siber Güvenlik Yasasını (Cybersecurity Act) kabul etmiştir.[67] Siber Güvenlik Yasası altında düzenlenen siber güvenlik programları gönüllülük esasına dayanmaktadır. Yine de farklı mevzuatlardaki atıflarla bu tür siber güvenlik programları, siber güvenlik yükümlülüklerine uyumu ispat için temel kriter olarak haline gelmiştir.

Genel düzenlemeler dışında Directive on the Resilience of Critical Entities (CER)[68] düzenlemesi kritik olarak nitelendirilen kurum ve kuruluşlar için ve Regulation on Operational Resilience of the Financial Sector (DORA)[69] finans alanındaki aktörler için özel siber güvenlik ve raporlama yükümlülükleri

[64] EU Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement Of Such Data, And Repealing Directive 95/46/EC (General Data Protection Regulation) – EUR Lex L 119 4.5.2016.
[65] EU 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 – EUR Lex L 194/1 19.7.2016.
[66] EU 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) – EUR Lex L 333/80 27.12.2022.
[67] EU 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), EUR Lex L 151/15 7.6.2019.
[68] EU Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC – EUR Lex L 333/164 27.12.2022.
[69] EU Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 – EUR Lex L 333/1 27.12.2022.

getirmiştir. Keza, aynı dönemlerde kabul edilen Çifte Kullanım Tüzüğü ise belirli siber güvenlik ürünlerine yönelik ihracat kısıtları getirmiştir.[70]

Bu düzenlemeler dışında Radio Equipment Directive (RED), the Medical Device Regulation (MDR), The In Vitro Diagnostic Medical Devices Regulation, the Vehicle General Safety Regulation, the Common Rules in Civil Aviation Regulation, the Machinery Regulation gibi düzenlemeler de kendi özel alanlarına ilişkin siber güvenlik kuralları getirmiştir.

Kritik ve önemli kurum ve kuruluşlara ilişkin siber güvenlik yükümlülükleri NIS 2 ve CER ile düzenlenmiş ve sektörel düzenlemelerle de belirli ürün ve hizmetlere ilişkin siber güvenlik kuralları getirilmiştir. Bu düzenlemelerde boşlukta kalan genel bir ürün temelli siber güvenlik düzenlemesidir.

Dijitalleşmenin yaygınlaşmasıyla dijital unsurlu ürün ve hizmetlerin güvenliği önemli bir sorun haline gelmiştir. Akıllı sensörlerden akıllı oyuncaklara kadar internete bağlı cihazların (IoT) günlük hayatının neredeyse her alanında kullanılmasıyla sorun daha kritik hale gelmiştir. Her an hem sıradan internet kullanıcıları hem de şirketler bir siber saldırıya maruz kalmaktadır. Siber saldırıların artması, risklerin değişmesi ve siber tehditlerin oluşturduğu etkinin artmasıyla birlikte bu konuda özel düzenlemeler yapılması ihtiyacı daha belirgin hale gelmiştir.

Avrupa Birliği, dijital unsurlu ürünlere ilişkin ortaya çıkan siber güvenlik sorunlarını ortadan kaldırmak amacıyla 2024 yılında Siber Dayanıklılık Yasası (*Cyber Resilience Act* veya *CRA*) isimli yasayı kabul etmiştir.[71] CRA, 20 Kasım 2024 tarihli AB Resmî Gazetesinde yayımlanmış olup tüm hükümleriyle 11 Aralık 2027 itibariyle uygulanmaya başlanacaktır.

CRA, amaçlanan ve öngörülebilir kullanımı bir cihaza veya ağa doğrudan veya dolaylı veri bağlantısı içeren dijital unsurlara sahip tüm ürünlere siber güvenlik yükümlülükleri getirmekte ve bu tür ürünlere tasarım ve varsayılan olarak siber güvenlik ilkelerini (*cybersecurity by design* ve *cybersecurity by default*) getirerek ürünlerin yaşam döngüsü için bir özen yükümlülüğü oluşturmaktadır.

Yukarıda da izah edildiği üzere CRA, AB'nin siber güvenliğe ilişkin ilk düzenlemesi değildir. Avrupa Birliği CRA öncesinde siber güvenliğin farklı boyutlarını ele alan muhtelif düzenlemeler yapılmıştır. CRA, bu düzenlemeleri tamamen ortadan kaldırmamakta; bilakis tamamlamaktadır.

[70] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast).
[71] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) – EUR Lex L 20.11.2024.

II. Kurumsal Siber Güvenlik Uyumu: NIS 1 ve NIS 2 Direktifleri

AB'de NIS düzenlemesi kurumsal eksende siber güvenlik uyumunu CRA ise ürün ekseninde siber güvenlik uyumunu düzenlemektedir. Bu haliyle bütüncül bir koruma sağlanması amaçlanmaktadır. CRA detaylı incelenmeden evvel NIS direktifinin zamanla evrimine hızlıca bakmak yerinde olacaktır. Nihayetinde, CRA'daki NIS çapraz-atfı sebebiyle iki düzenleme birbiriyle doğrudan ilişki içerisindedir.

A. NIS 1 Direktifi

NIS Direktifi 2016 yılında kabul edilmiştir. Direktifin gerekliliklerini iç hukuklarına aktarmaları için üye devletlere 2018 yılına kadar süre tanımıştır. Direktif, şebeke ve bilgi güvenliğine ilişkin bağlayıcı kurallar getiren sayılı düzenlemeden biridir.

NIS Direktifi, AB üyesi devletlere şebeke ve bilgi güvenliği konusunda ulusal bir strateji belirleme yükümlülüğü getirmektedir. Ayrıca üye devletler arası stratejik iş birliğini ve bilgi alışverişini desteklemek ve güveni geliştirmek için iş birliği grubu kurmaktadır. Direktif, iş birliğini daha somut bir hâle getirerek üye devletler arası operasyonel iş birliğini teşvik etmek için bir siber güvenlik acil müdahale ekipleri (CSIRT) ağı oluşturmakta ve kapsamına giren hizmet sağlayıcılar için temel güvenlik gereksinimlerini belirlemektedir.

NIS Direktifinin temel ilkeleri şu şekilde özetlenebilir:

- Şebeke ve bilgi güvenliğinde sınır ötesi iş birliğinin geliştirilmesi
- Risk yönetimi kültürünün desteklenmesi
- Üye devlet stratejileri ile birlikte yeknesaklaşma sağlanması
- Etkili bir siber güvenlik müdahale süreci yürütülmesi
- Olay raporlama
- Asgari düzeyde uyumluluk (Daha yüksek düzeyde güvenlik öngörülebilir.)

NIS Direktifi, aşağıda ele alınan şu iki temel aktöre sorumluluk getirmektedir: temel hizmet operatörü ve dijital hizmet sağlayıcı.

1. Temel hizmet operatörü

Temel hizmet operatörü, NIS Direktifi Ek II'de sayılan sektörler ve alt sektörler için her bir üye devlet tarafından müstakil olarak belirlenecektir. Bu tanımlama yapılırken hizmetin kritik sosyal/ekonomik faaliyetlerin sürdürülmesi için gerekli olup olmadığı, hizmetin sağlanmasının şebeke ve bilgi güvenliğine bağlı bulunup bulunmadığı ve bu hizmete yönelik bir siber olayın, bu hizmetlerin sunulması

üzerinde yıkıcı etkisi olup olmadığı dikkate alınacaktır. Dolayısıyla, bu kriterlere uygun olarak her bir üye devlette farklı türden kuruluşların kapsama alınması söz konusu olabilecektir.

Peki, yıkıcı etki nasıl belirlenecektir? NIS Direktifi'ne göre yıkıcı etki belirlenirken (i) ilgili hizmetten yararlanan kullanıcı sayısı, (ii) olayın, ekonomik ve toplumsal faaliyetler veya kamu güvenliği üzerinde ne kadar süreyle ve ne derece etki gösterebileceği, (iii) işletmenin o sektördeki pazar payı, (iv) olaydan etkilenebilecek coğrafi alan ve ayrıca o sektöre mahsus özel faktörler dikkate alınacaktır.

Temel hizmet operatörü belirlenmesi gereken ve NIS Direktifi Ek II'de yer alan sektörler ve alt sektörler şunlardır:

1) Enerji
    a) Elektrik
    b) Petrol
    c) Doğal gaz
2) Ulaştırma
    a) Hava yolu taşımacılığı
    b) Demir yolu taşımacılığı
    c) Su yolu taşımacılığı
    d) Kara yolu taşımacılığı
3) Bankacılık
4) Finansal Piyasa Altyapıları
5) Sağlık Sektörü
6) Su Yönetimi (İçme Suyu Temini ve Dağıtımı)
7) Dijital Altyapı
    a) İnternet değişim noktaları (IXP)
    b) Alan adı hizmet sağlayıcıları (DNS)
    c) Üst seviye alan adı sicilleri (TLD)

Temel hizmetlerin neler olduğu ve bu hizmetleri sunan operatörlerin kimler olduğu üye devletlerce müstakil olarak belirlenecek ve bu bilgileri içeren listeler belirli aralıklarla güncellenecektir.

NIS Direktifi, temel hizmet operatörlerine temel bir siber güvenlik sağlama yükümlülüğü getirmektedir. Direktif uyarınca temel hizmet operatörleri; siber riski önlemek veya bunun etkilerini asgari düzeye indirmek için riske uygun ve operasyonel tedbirler almak, şebeke ve bilgi sistemlerinin güvenliğini sağlamakla yükümlüdür.

Temel hizmet operatörlerine getirilen bir diğer yükümlülük ise siber güvenlik olaylarını bildirim yükümlülüğüdür. Temel hizmet operatörleri, herhangi bir kişisel veri içersin veya içermesin, bilişim sistemlerini ilgilendiren her siber güvenlik olayını yetkili makamlara bildirmek ve olaydan etkilenen kullanıcı sayısını, olayın süresini ve olaydan etkilenen coğrafi alanı kapsamlı şekilde raporlamakla yükümlüdür.

NIS Direktifi, üye devletlere de temel bir ödev yüklemektedir. Temel hizmet operatörlerine ilişkin listenin güncellenmesinin yanı sıra üye devletler; temel hizmet operatörünün NIS Direktifi'ne uyumluluğunu, ulusal yetkili makam veya nitelikli bir denetçi tarafından gerçekleştirilecek güvenlik denetimi vasıtasıyla değerlendirmekle yükümlüdür. Bu şekilde, siber güvenliğin sürekliliği temin edilmeye çalışılmaktadır.

Önemle belirtmek gerekir ki NIS Direktifi, deniz taşımacılığını bir temel hizmet olarak nitelendirmektedir. Direktif, üye devletlerin, Uluslararası Denizcilik Örgütü (*International Maritime Organisation* - IMO) başta olmak üzere, ilgili uluslararası kuruluşların kuralları ve rehberleri ışığında bu alandaki temel hizmet operatörlerini tespit etmeleri gerektiğini belirtmektedir.

NIS Direktifi, yumuşak hukuk kuralı niteliğindeki IMO rehberlerine atıf yapmaktadır. Bunun arka planında siber güvenliğin dinamik yapısı sebebiyle her türlü bağlayıcı kuralın tespit edilmesinin imkânsızlığı yatmaktadır. Bu, NIS Direktifi'nin en temel ilkesi olan "uluslararası standartların gözetilmesi"ne de uyumlu bir yaklaşımdır.

2. Dijital hizmet sağlayıcı

NIS Direktifinde tanımlanan diğer bir aktör ise dijital hizmet sağlayıcılardır. Bunlar Direktifte organik şekilde tanımlanmıştır. Dijital hizmet sağlayıcılar, NIS Direktifi Ek III'te listelenen tipte olan ve dijital bir hizmet sunan tüzel kişilerdir. Temelde şu üç kategoriye giren hizmet sağlayıcılardır:

1) Çevrim içi pazar
2) Çevrim içi arama motoru
3) Bulut bilişim hizmeti

NIS Direktifi uyarınca dijital hizmet sağlayıcılar, uygun ve orantılı güvenlik önlemlerini almakla ve yetkili makamlara bildirmekle yükümlüdür. Ancak bu yükümlülük *ex-post* bir yükümlülük olup üye devletler, dijital hizmet sağlayıcıların yükümlülüklerine uyup uymadığını *ex-ante* denetlemeyecektir meğerki belirli bir olaya ilişkin açık kanıtlar ortaya koyulmuş olsun. Dijital hizmet sağlayıcıların bilgi toplumu hizmet sağlayıcıları olmasından dolayı devletler, dijital hizmet sağlayıcılara NIS Direktifi'nin

öngördüğünden daha fazla güvenlik veya bildirim şartı getiremez. NIS Direktifi bunu açıkça yasaklamakta, bu şekilde ölçülülüğü temin etmeye çalışmaktadır.

Dijital hizmet sağlayıcıların temel yükümlülüğü, şebeke ve bilgi sistemlerinin güvenliği ile sistem ve tesislerin güvenliğini sağlamaktadır. Keza tüm iş süreçlerinde uluslararası standartlara uygunluğu da temin etmekle yükümlüdürler.

Dijital hizmet sağlayıcılara, tıpkı temel hizmet operatörleri gibi, siber güvenlik olaylarını bildirim yükümlülüğü getirilmiştir. Bu doğrultuda dijital hizmet sağlayıcılar, kişisel veri içersin veya içermesin, herhangi bir siber güvenlik olayı yaşadıkları takdirde bunu yetkili makamlara derhâl bildireceklerdir. Ayrıca, olaydan etkilenen kullanıcı sayısını, hizmetin işleyişinin aksama derecesini, olayın süresini, ekonomik ve sosyal faaliyetler üzerindeki etkisinin düzeyini ve olaydan etkilenen coğrafi alanı kapsamlı olarak raporlayacaklardır. Hangi olayların bildirileceğini ve bunun belirlenme usullerinin detaylarını üye devletler tayin edecektir.

Bildirim yükümlülüğü, NIS Direktifinin en önemli ilkesidir. Direktif 'in temel amacı, siber güvenliğin sağlanması ve bu şekilde AB içerisindeki tüm paydaşların siber dayanıklılığının temin edilmesidir. Amaç, tehditlerin ortadan kaldırılması ve bir tehdidin kalıcı bir risk olarak ortaya çıkmasının önlenmesidir. Diğer bir deyişle amaç, önleyici tedbirler sayesinde virüsün bir pandemiye yol açmasını önlemektir. Bunun yolu da tüm paydaşların, kendilerini herhangi bir baskı altında hissetmeksizin ve tereddüt etmeksizin bilgi paylaşımı yapmasından geçmektedir. Bunu temin etmek amacıyla NIS Direktifi, bildirim yapılmasının bildirim yapana ek bir sorumluluk getirmeyeceğinin altını çizmektedir.

NIS Direktifi'nin bir diğer temel ilkesi ise standardizasyondur. Direktifle üye devletlere bir ödev getirilerek onlardan bir teknolojiyi dayatmadan, teknolojiler arasında ayrım yapmadan şebeke ve bilgi güvenliğinin sağlanmasında ilgili Avrupa standartlarının veya uluslararası kabul görmüş standartların kullanılmasını teşvik etmesi beklenmektedir.

Peki, siber güvenlik konularında bağlayıcılık nasıl temin edilecektir? AB üyesi devletler siber güvenliğin temini için yaptırım öngörebilir mi? NIS Direktifinden doğan tüm yükümlülüklere ilişkin yaptırım getirilmesi tamamen üye devletlerin takdirindedir. Direktif; yaptırımların etkili, orantılı ve caydırıcı olması gerektiğinin altını çizmektedir.

B. NIS 2 Direktifi

2021 yılında, NIS Direktifinin güncellenmesine ilişkin bir tasarı sunulmuş olup Direktifin, kapsamı genişletilmek suretiyle AB içinde genel bir şebeke ve bilgi güvenliği yasasına dönüşmesi

hedeflenmiştir. Bu hedef 2022 yılında somutlaşmış ve NIS 1 Direktifi ilga edilerek NIS 2 Direktifi yürürlüğe koyulmuştur.

NIS 1 Direktifi, kritik sektörler ve dijital hizmet sağlayıcılar için bağlayıcı kurallar getirmiştir. Direktif, siber güvenliğe ilişkin temel altyapıyı oluşturmayı amaçlamıştır. O yüzden kapsam dar tutulmuştur. Direktifin bir öncü düzenlemedir ve Avrupa Birliği'nde siber güvenlik hukukunun temelini atmıştır. NIS 1 Direktifinin bu seçici ve kademeli geçiş yaklaşımı meyvesini NIS 2 Direktifi olarak vermiştir. Avrupa Birliği, NIS 1 Direktifi ile kurumsal çerçeveyi güçlendirmiş ve daha kapsayıcı bir düzenleme için altyapıyı oluşturmuştur.

Tıpkı NIS 1 gibi NIS 2 Direktifinin de temel hedefi, AB genelinde yüksek düzeyde ortak bir siber güvenlik seviyesine ulaşmaktır. Peki NIS 1 ve NIS 2 arasındaki temel farklar nelerdir?

Genişletilmiş Kapsam: Daha fazla sektör ve işletme kapsama alınmıştır.

Güçlendirilmiş Güvenlik Gereksinimleri: Tedarik zinciri güvenliği de dahil olmak üzere daha sıkı ve daha kapsamlı güvenlik önlemleri getirilmiştir.

İyileştirilmiş Olay Raporlaması: Raporlama yükümlülükleri kolaylaştırılmış ve olay raporlaması için daha ayrıntılı gereklilikler getirilmiştir.

Yeknesak Yaptırımlar: Tutarlı uygulama için AB genelinde aynı nitelikte yaptırımlar ve cezalar oluşturulmuştur.

Geliştirilmiş Ulusal Stratejiler: Üye devletlerin ulusal siber güvenlik stratejilerini düzenli olarak gözden geçirmeleri ve güncellemeleri ve sınır ötesi işbirliğini geliştirmeleri öngörülmüştür.

NIS 2 Direktifinde temel iki aktör vardır:

- Temel hizmet sağlayıcılar (*essential entities*)
- Önemli hizmet sağlayıcılar (*important entities*)

NIS 2 Direktifinde yüksek kritik sektörler (*sectors of high criticality*) şu şekilde belirlenmiştir:

1. Enerji: Elektrik, Isıtma ve Soğutma, Petrol, Doğalgaz, Hidrojen
2. Ulaştırma: Hava, Demiryolu, Su, Karayolu
3. Bankacılık
4. Finansal piyasa altyapıları
5. Sağlık
6. İçme suyu

7. Atık suyu
8. Dijital altyapı
9. Bilişim hizmetleri yönetimi (B2B)
10. Kamu hizmetleri
11. Uzay

Diğer kritik sektörler (*other critical sectors*) ise şunlardır:

1. Posta ve diğer taşıma hizmetleri
2. Atık yönetimi
3. Kimyasalların imalat, üretim ve dağıtımı
4. Gıdaların üretimi, işlemesi ve dağıtımı
5. İmalat
6. Dijital sağlayıcılar
7. Araştırma

NIS 1 Direktifinde olmayıp NIS 2 Direktifinde ilk defa kapsama alınan sektörler ve aktörler şunlardır:

- Elektronik haberleşme hizmet sağlayıcıları
- Sosyal ağ sağlayıcıları ve veri merkezi hizmetleri gibi dijital hizmetler
- Atık su ve atık yönetimi
- Uzay
- Bazı kritik ürünlerin imalatı (İlaç, medikal aletler ve kimyasallar)
- Posta ve taşıma hizmetleri
- Gıda
- Kamusal yönetim hizmetleri

NIS 2 Direktifindeki temel yükümlülükler şu şekilde özetlenebilir:

- Siber olay yönetimi ve kriz yönetimi
- Açık yönetimi ve ifşası
- Risk yönetim tedbirlerinin etkinliğinin değerlendirilmesi
- Basit bilişim hijyen uygulamaları ve siber güvenlik eğitimi
- Kriptografinin etkin şekilde uygulanması
- İnsan kaynağı güvenliği
- Erişim kontrol politikaları
- Varlık yönetimi

Önemle vurgulamak gerekir ki, NIS 2 Direktifi halefinden farklı olarak idari para cezalarına ilişkin açık kurallar getirmiştir. Şöyle ki, NIS 2 Direktifine aykırılık durumunda, €10 Milyon Euro'ya kadar idari para cezası veya küresel cironun %2'sine kadar idari para cezası (hangisi yüksekse) uygulanması söz konusu olacaktır. İdari yaptırımlar yoluyla NIS 2 Direktifi caydırıcı ve etkin şekilde siber güvenliği kurumsal seviyede sağlamayı hedeflemektedir.

III. Siber Dayanıklılık Yasası (CRA)

CRA, AB'nin ürün özelinde siber güvenliğe özgülenmiş ilk genel düzenlemesi niteliğindedir. AB'nin bugüne kadar ki ürün güvenliği (*safety*) yaklaşımının oluşturmuş olduğu eksiklik, bu yasayla genel güvenlik (*security*) unsuru da eklenerek AB iç pazarında dijital unsuru olan ürünlerin oluşturduğu risklere karşı bütüncül bir yaklaşım sağlanmaya çalışılmıştır.

CRA, ürün temelli siber güvenlik standartlarını kapsamlı olarak düzenlemiştir. CRA, ürünler-arası düzenleme (*cross-product regulation*) yaklaşımını esas almaktadır ve 5G ve bulut bilişim gibi belirli teknolojiler başta olmak üzere ürün temelli siber güvenlik sertifikasyon standartlarının belirlenmesi için temel yasal dayanak olmuştur.

Halihazırda siber güvenlikle ilgili uluslararası uygulanan standartların karşısında AB'nin kendi standart ve sertifikasyon planlarını uygulamaya alması beraberinde uyum sorunsalını getirmiştir.

AB, "New Legislative Framework" olarak da anılan Yeni Yasal Çerçeve isimli paketle zaten 2008 yılında kapsamlı bir ürün güvenliği ve standartları kuralları ortaya koymuştur.[72]

- Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products
- Decision 768/2008 on a common framework for the marketing of products, which includes reference provisions to incorporate in product legislation revisions. In effect, it is a template for future product harmonisation legislation
- Regulation (EU) 2019/1020 on market surveillance and compliance of products

2008 yılında başlayan harmonizasyon sürecinin bir neticesi olarak müteakipteki düzenlemelerde değişiklikler yapılmış veya yeni düzenlemeler kabul edilmiştir:

1) Toy Safety - Directive 2009/48/EU
2) Transportable pressure equipment - Directive 2010/35/EU

[72] New legislative framework, https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en.

3) Restriction of Hazardous Substances in Electrical and Electronic Equipment - Directive 2011/65/EU
4) Construction products - Regulation (EU) No 305/2011
5) Pyrotechnic Articles - Directive 2013/29/EU
6) Recreational craft and personal watercraft - Directive 2013/53/EU
7) Civil Explosives - Directive 2014/28/EU
8) Simple Pressure Vessels - Directive 2014/29/EU
9) Electromagnetic Compatibility - Directive 2014/30/EU
10) Non-automatic Weighing Instruments - Directive 2014/31/EU
11) Measuring Instruments - Directive 2014/32/EU
12) Lifts - Directive 2014/33/EU
13) ATEX - Directive 2014/34/EU
14) Radio equipment - Directive 2014/53/EU
15) Low Voltage - Directive 2014/35/EU
16) Pressure equipment - Directive 2014/68/EU
17) Marine Equipment - Directive 2014/90/EU
18) Cableway installations - Regulation (EU) 2016/424
19) Personal protective equipment - Regulation (EU) 2016/425
20) Gas appliances - Regulation (EU) 2016/426
21) Medical devices - Regulation (EU) 2017/745
22) In vitro diagnostic medical devices - Regulation (EU) 2017/746
23) EU fertilising products – Regulation (EU) 2019/1009
24) Drones - Commission Delegated Regulation (EU) 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems
25) Batteries - Regulation (EU) 2023/1542
26) Machinery - Regulation (EU) 2023/1230 (replacing Directive 2006/42/EC that entered into force before the NLF, still applicable until 20/1/2027)
27) Ecodesign requirements for sustainable products - Regulation (EU) 2024/1781
28) Artificial Intelligence Act - Regulation (EU) 2024/1689
29) Cyber Resilience Act - Regulation (EU) 2024/2847

CRA, ürün güvenliği standartlarını siber güvenlik odağında ileriye taşıyan bir düzenleme olarak hazırlanmıştır. ENISA'ya da temel teknolojilerin siber güvenlik gereksinimlerini belirleme görevi verilmiştir.

IV. CRA'nın Temel Çerçevesi

A. Genel olarak

CRA, yukarıda da belirtildiği üzere AB'nin siber güvenliğini artırmak amacıyla hazırladığı en teknik düzenlemelerden birisidir. Siber Güvenlik Yasası ve NIS2 düzenlemelerinden sonraki en önemli gelişme olan bu düzenleme özünde AB'nin teknoloji alanındaki egemenliğini pekiştirme çalışmalarının bir ürünüdür.

CRA şu hususları düzenlemektedir:[73]

(1) Söz konusu ürünlerin siber güvenliğini sağlamak amacıyla dijital unsurlu ürünlerin piyasaya sunulmasına ilişkin kurallar;
(2) Dijital unsurlar içeren ürünlerin tasarımı, geliştirilmesi ve üretimi için temel siber güvenlik gereklilikleri ve müteşebbislerin bu ürünlerle ilgili olarak siber güvenliğe ilişkin yükümlülükleri;
(3) Dijital unsurlar içeren ürünlerin kullanımda olması beklenen süre boyunca siber güvenliğini sağlamak için üreticiler tarafından uygulamaya konulan güvenlik açığı yönetme süreçlerine ilişkin temel siber güvenlik gereklilikleri ve müteşebbislerin bu süreçlere ilişkin yükümlülükleri;
(4) CRA'nın kapsamına giren hususlara ilişkin izleme ve kural ve gerekliliklerinin uygulanması dahil olmak üzere piyasa gözetimine ilişkin kurallar.

CRA, dijital unsur içeren ürünleri genel olarak kapsamına alarak bu tür ürünlerin uçtan uca siber güvenlik süreçlerine yönelik kurallar getirmektedir. Kurallar, tasarım, gelişim ve üretim süreçlerinin tamamını kapsamaktadır. Bu kuralların yanı sıra, bu kuralların AB iç pazarında uçtan uca uygulanması için de detaylı piyasa gözetim ve denetim kuralları inşa etmektedir.

Siber güvenliğe ilişkin kuralların yeknesak uygulanmasına ilişkin duyulan ihtiyaç ve konunun iç pazarda malların serbest dolaşımını ilgilendirdiği için AB konuyu bir tüzük (*regulation/act*) aracılığıyla düzenlemeyi tercih etmiştir. Direktif yerine tüzük tercih edildiği için CRA doğrudan AB genelinde uygulama alanı bulacaktır. İlave bir iç hukuka aktarım düzenlemesi gerektirmemektedir.

[73] CRA, Madde 1.

B. Kapsam

CRA, piyasaya arz edilen, kullanım amacı veya makul olarak öngörülebilir kullanımı bir cihaza ya da ağa doğrudan veya dolaylı mantıksal veya fiziksel veri bağlantısı içeren dijital unsurlara sahip ürünlere uygulanmak üzere hazırlanmıştır. İlkesel olarak dijital unsuru olan tüm ürünler -donanım veya yazılım fark etmeksizin- özel olarak istisna edilmediği sürece ve üreticisinin de kim olduğuna bakılmaksızın CRA'nın kapsamına girmektedir.

CRA'nın muhtelif istisnaları bulunmaktadır. CRA'nın 'Kapsam' başlıklı 2. maddesi uyarınca bazı tam bazı ise kısmi istisnalar tanınmıştır:

1. Açıkça belirtilen tam istisnalar

Aşağıdaki hallerde CRA tamamen uygulanmaz:

(1) Tıbbi cihazlara ilişkin 2017/745 sayılı Tüzüğe tabi olan dijital unsurlu ürünler,[74]

(2) In vitro diagnostik tıbbi cihazlarla ilişkin 2017/746 sayılı Tüzüğe tabi olan dijital unsurlu ürünler,[75]

(3) Motorlu taşıtlar mevzuatına tabi cihazlara ilişkin 2019/2144 sayılı Tüzüğe tabi olan dijital unsurlu ürünler,[76]

(4) Dijital unsurları olsa da sivil havacılık alanında 2018/1139 sayılı Tüzük uyarınca sertifikasyonlandırılmış olan ürünler,[77]

(5) Deniz ekipmanlarına ilişkin 2014/90 sayılı Direktifinin uygulandığı ekipmanlar,[78]

---

[74] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117/1, 5.5.2017.

[75] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, OJ L 117/176, 5.5.2017.

[76] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166, OJ L 325/1, 16.12.2019.

[77] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91, OJ L 212/1, 22.8.2018.

[78] Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC, OJ L 257/146, 28.8.2014.

(6) Dijital unsurlara sahip ürünlerdeki aynı bileşenleri değiştirmek için piyasada bulunan ve değiştirilmesi amaçlanan bileşenlerle aynı özelliklere göre üretilen yedek parçalar,

(7) Münhasıran ulusal güvenlik veya savunma amaçları için geliştirilen veya değiştirilen dijital unsurlara sahip ürünler ile gizli bilgileri işlemek için özel olarak tasarlanmış ürünler.

2. Kısmi veya özel istisnalar

CRA'nın uygulanması CRA'nın EK 1 bölümünde belirtilen temel siber güvenlik gerekliliklerinin kapsadığı risklerin tamamını veya bir kısmını ele alan gereklilikleri ortaya koyan diğer AB kuralları tarafından kapsanan dijital unsurlara sahip ürünlere uygulanması için sınırlandırılabilir veya CRA tamamen kapsam dışında tutulabilir. Bu tür bir sınırlandırma veya kapsam dışı bırakmanın gerçekleşebilmesi için şu şartlardan birinin gerçekleşmesi gerekmektedir:

(1) Söz konusu sınırlama veya kapsam dışı tutma, bu ürünler için geçerli olan genel düzenleyici çerçeve ile tutarlı olmalıdır; veya

(2) Sektörel kurallar, CRA tarafından sağlanan koruma ile aynı veya daha yüksek bir koruma seviyesine ulaşmış olmalıdır.

Peki, kısıtlama veya kapsam dışı olma nasıl belirlenecektir? Bu konuda CRA, Avrupa Komisyonu'na genel bir yetki vermektedir. CRA'nın 2. maddesinin beşinci fıkrası uyarınca, Avrupa Komisyonu CRA'nın 61. maddesi uyarınca, CRA'yı tamamlamak üzere, söz konusu sınırlama veya hariç tutmanın gerekli olup olmadığını, ilgili ürün ve kuralları ve ilgili olması halinde sınırlamanın kapsamını belirlemek suretiyle yetki devrine dayanan özel düzenlemeler kabul etme yetkisine sahiptir.

Bu bağlamda, temel gerekliliklerin kapsadığı risklerin tamamını veya bir kısmını ele alan ve aynı koruma seviyesine ulaşan gereklilikleri ortaya koyan diğer AB kuralları tarafından kapsanan dijital unsurlara sahip ürünler genel olarak kapsam dışındadır denilebilir.

CRA, bu bağlamda amaçsal bir yaklaşım sergilemekte ve fonksiyonel olarak CRA'nın öngördüğü güvenlik seviyelerinin aynısı veya daha üst düzeyinin sağlanması durumunda kendisini kapsam dışı bırakarak diğer AB düzenlemelerine uygulama önceliği vermektedir.

3. Ulusal güvenlik, kamu güvenliği ve savunmaya ilişkin kısıtlamalar

CRA, tam veya kısmi olarak kapsamda olan dijital unsurlu tüm ürünlere ilişkin genel bir kısıtlama daha getirmektedir. CRA'nın 2. maddesinin sekizinci fıkrası uyarınca, CRA'da öngörülen yükümlülükler ifşa edilmesi üye devletlerin ulusal güvenlik, kamu güvenliği veya savunmasının temel çıkarlarına aykırı

olacak bilgilerin sağlanmasını gerektirmez. Bu şekilde güvenlik ve gizlilik arasında bir denge kurulmaktadır.

4. Özel tam istisna: ticari amaçlı hareket etmeme unsuru

Her ne kadar CRA'nın 'Kapsam' başlıklı 2. maddesinde yer almasa da CRA'nın muhtelif yerlerindeki atıflarla özel bir tam istisna hükmünün daha varlığından bahsedilmesi mümkündür. Bu tam istisnanın temel kriteri müteşebbisin ticari amaçlı hareket edip etmemesidir.

CRA, 'piyasaya sunma' eylemini dijital unsurlar içeren bir ürünün, ister ödeme karşılığında ister ücretsiz olsun, ticari bir faaliyet sırasında AB pazarında dağıtılmak veya kullanılmak üzere tedarik edilmesi olarak tanımlamıştır.[79] Dibacede de izah edildiği üzere CRA, müteşebbisler için yalnızca piyasada bulunan dijital unsurlara sahip ürünlerle ilgili olarak, dolayısıyla ticari bir faaliyet sırasında AB piyasasında dağıtım veya kullanım için tedarik edilen haller için uygulama alanı bulacaktır.[80]

Peki, ticari bir faaliyet kapsamında tedarikten ne anlaşılmalıdır? Ticari bir faaliyet kapsamında tedarik, yalnızca dijital unsurlar içeren bir ürün için bir fiyat talep etmek şeklinde yorumlanmaması gerekmektedir.

CRA'ya göre:

(1) Gerçek maliyetlerin karşılanmasına hizmet etmeyen nitelikte teknik destek hizmetleri için bir bedel talep edilmesi,
(2) Üreticinin diğer hizmetlerini para karşılığı sunduğu bir yazılım platformu sağlayarak para kazanma niyetiyle hareket etmesi,
(3) Kişisel verilerin yalnızca yazılımın güvenliğini, uyumluluğunu veya birlikte çalışabilirliğini iyileştirmek dışındaki nedenlerle işlenmesini bir kullanım koşulu olarak talep edilmesi,
(4) Dijital unsurlar içeren bir ürünün tasarımı, geliştirilmesi ve sağlanması ile ilgili maliyetleri aşan bağışların kabul edilmesi,

gibi hallerde de ticari bir faaliyet kapsamında tedarikten söz edilecektir.

Kâr elde etme niyeti olmaksızın bağış kabul etmek ticari bir faaliyet olarak değerlendirmemektedir.[81] Dolayısıyla, dijital unsurlu ürünün piyasaya ücretsiz sunulması ve bir yandan bağış alınması durumunda CRA bakımından kapsam dışılık kriteri sağlanmış olacaktır.

[79] CRA, Madde 3(22).
[80] CRA, Resital 15.
[81] CRA, Resital 15.

Görüldüğü üzere, ticari amaçlı hareket etme unsuru açısından sınır net olarak çizilmiş değildir. Dibacede yer alan durumlar örnek mahiyetindedir. Her somut olayın özelliklerine göre bir değerlendirme yapılarak ticari amaçlı hareket edilip edilmediğinin tespiti gereklidir.

V. CRA'daki Temel Tanımlar

CRA, kazuistik bir düzenlemedir ve *dijital unsurlu ürün, uzaktan veri işleme, siber güvenlik, yazılım, donanım, bileşen, elektronik bilgi sistemi, mantıksal bağlantı, fiziksel bağlantı, dolaylı bağlantı, son nokta, müteşebbis, üretici, açık kaynak yazılım sorumlusu, yetkili temsilci, ithalatçı, dağıtıcı, tüketici, mikro işletmeler, küçük işletmeler, destek süresi, piyasaya arz, piyasada bulundurma, kullanım amacı, makul ölçüde öngörülebilir kullanım, makul ölçüde öngörülebilir kötüye kullanım, bildirim makamı, uygunluk değerlendirmesi, uygunluk değerlendirme kuruluşu, onaylanmış kuruluş, önemli değişiklik, CE işareti, Birlik uyum mevzuatı, piyasa gözetim otoritesi, uluslararası standart, Avrupa standardı, uyumlaştırılmış standart, siber güvenlik riski, önemli siber güvenlik riski, yazılım malzeme listesi, güvenlik açığı, istismar edilebilir güvenlik açığı, aktif olarak istismar edilen güvenlik açığı, olay, dijital unsurlar içeren ürünün güvenliği üzerinde etkisi olan olay, ramak kala, siber tehdit, kişisel veri, ücretsiz ve açık kaynaklı yazılım, geri çağırma, geri çekme, koordinatör olarak belirlenen CSIRT* gibi 51 farklı tanım yapmaktadır.[82]

CRA'nın uygulama alanının belirlenebilmesi için bazı temel tanımların detaylıca incelenmesi gerekmektedir.

A. Dijital unsurlu ürün (product with digital element)

CRA'nın odağında dijital unsurlu ürün (*product with digital element*) yer almaktadır. Dijital unsurlu ürün, "*yazılım veya donanım bileşenlerinin ayrı olarak piyasaya sürülmesi de dahil olmak üzere, bir yazılım veya donanım ürünü ve onun uzak veri işleme çözümleri*" olarak tanımlanmıştır.[83]

[82] Tanımlar: product with digital elements, remote data processing, cybersecurity, software, hardware, component, electronic information system, logical connection, physical connection, indirect connection, end-point, economic operator, manufacturer, open-source software steward, authorised representative, importer, distributor, consumer, microenterprises', 'small enterprises, support period, placing on the market, making available on the market, intended purpose, reasonably foreseeable use, reasonably foreseeable misuse, notifying authority, conformity assessment, conformity assessment body, notified body, substantial modification, CE marking, Union harmonisation legislation, market surveillance authority, international standard, European standard, harmonised standard, cybersecurity risk, significant cybersecurity risk, software bill of materials, vulnerability, exploitable vulnerability, actively exploited vulnerability, incident, incident having an impact on the security of the product with digital elements, near miss, cyber threat, personal data, free and open-source software, recall, withdrawal, CSIRT designated as coordinator.

[83] CRA, Madde 3(1).

Dijital unsurlu ürünün üç alt bileşeni vardır: yazılım, donanım ve uzak veri işleme çözümü kavramlarının da anlaşılması gerekmektedir:

(1) Yazılım: *bir elektronik bilgi sisteminin bilgisayar kodundan oluşan kısmı*

(2) Donanım: *dijital verileri işleyebilen, depolayabilen veya iletebilen fiziksel bir elektronik bilgi sistemi veya parçaları*

(3) Uzaktan veri işleme: *yazılımın üretici tarafından tasarlandığı ve geliştirildiği veya üreticinin sorumluluğu altında olduğu ve yokluğunda dijital unsurlara sahip ürünün işlevlerinden birini yerine getirmesini engelleyecek bir mesafede veri işleme*

Söz konusu tanımlar, CRA'nın yer ve kişi bakımından uygulanması açısından da kritiktir. Bilhassa, uzaktan veri işleme, internet bağlı temel cihazlar (Internet of Things (IoT) veya Industrial Internet of Things (IIoT)) gibi tamamen veya kısmen bulut bilişim altyapıları üzerinde ana fonksiyonlarını yerine getiren ürünler için kritik önemi haizdir. Bu açıdan AB dışındaki bir bulut bilişim hizmet sağlayıcısı dijital unsurlu bir ürüne uzaktan veri işleme hizmeti sunduğu için CRA'nın kurallarına tabi olabilecektir.

CRA, genel dijital unsurlu ürünlerin iki alt türünü de düzenlemektedir. Bunlar dijital unsurlu önemli ürünler ile dijital unsurlu kritik ürünlerdir.

Mevcut ürün sınıflandırması şu şekilde özetlenebilir:

(1) Dijital unsurlu genel ürünler (*Products with digital elements*)
(2) Dijital unsurlu önemli ürünler (*Important products with digital elements*)
    a. Sınıf I
    b. Sınıf II
(3) Dijital unsurlu kritik ürünler (*Critical products with digital elements*)

B. Üretici (manufacturer)

Üretici, dijital unsurlar içeren ürünler geliştiren veya üreten ya da dijital unsurlu ürünler tasarlatan, geliştiren veya ürettiren ve bunları kendi adı veya ticari markası altında ücretli, paralı veya ücretsiz olarak pazarlayan gerçek veya tüzel kişiyi ifade etmektedir.

CRA'daki temel aktör üreticidir ve sorumluluk rejimi açısından üreticiden hareket edilmektedir.

C. İthalatçı (importer)

İthalatçı, AB dışında yerleşik bir gerçek veya tüzel kişinin adını veya ticari markasını taşıyan dijital unsurlu bir ürünü piyasaya süren AB içinde yerleşik gerçek veya tüzel kişiyi ifade etmektedir.

Ç. Dağıtıcı (distributor)

Dağıtıcı, tedarik zincirinde yer alan, üretici veya ithalatçı dışında, dijital unsurlu bir ürünü özelliklerini etkilemeden AB pazarında kullanılabilir hale getiren gerçek veya tüzel kişi anlamına gelmektedir.

D. Statülerin Değişmesi Kuralı

Önemle vurgulamak gerekir ki, üretici, ithalatçı ve dağıtıcı kavramları geçişken niteliktedir ve organik değil fonksiyonel olarak tanımlanmıştır. CRA'nın 'Üreticilerin yükümlülüklerinin ithalatçı ve dağıtıcılara uygulandığı durumlar' başlıklı 21. maddesi uyarınca bir ithalatçı veya dağıtıcı, dijital unsurlu bir ürünü kendi adı veya ticari markası altında piyasaya sürdüğünde veya piyasaya sürülmüş olan dijital unsuru bir üründe esaslı bir değişiklik yaptığında, CRA'nın amaçları doğrultusunda üretici olarak kabul edilir ve CRA'nın üreticilere getirilen 13. ve 14. maddelere tabi olur.

Üreticinin yükümlülüklerinin üretici dışındaki üçüncü kişilere yansıtıldığı tek durum bu değildir. CRA'nın 'Üreticilerinin yükümlülüklerinin geçerli olduğu diğer durumlar' başlıklı 22. maddesi uyarınca, dijital unsurlu bir üründe esaslı bir değişiklik yapan ve bu ürünü piyasaya arz eden üretici, ithalatçı veya dağıtıcı dışındaki bir gerçek veya tüzel kişi de CRA'nın amaçları doğrultusunda üretici olarak kabul edilecektir. Öyle ki, bu kişiler, dijital unsurlu ürünün esaslı değişiklikten etkilenen kısmı için veya esaslı değişikliğin dijital unsurlu ürünün bir bütün olarak siber güvenliği üzerinde bir etkisi olması halinde ürünün tamamı için CRA'nın 13. ve 14. maddelerinde belirtilen yükümlülüklere tabi olacaktır.

Görüldüğü üzere, üreticinin dijital unsurlu ürününü kendi ad veya ticari markası altında piyasaya sürme ve dijital unsurlu bir üründe esaslı değişiklik yapma bu bağlamda tüm sorumluluk rejimini değiştirmektedir.

VI. Dijital Unsurlu Ürün Türleri

A. Dijital Unsurlu Önemli Ürünler

Dijital unsurlu önemli ürünler, çapraz-atıf yöntemiyle belirlenmiştir. CRA'nın EK 3. bölümünde belirtilen bir ürün kategorisinin temel işlevselliğine sahip olan dijital unsurlu ürünler, dijital unsurlu önemli ürünler olarak kabul edilmektedir.[84]

[84] CRA, Madde 7(1).

Peki, dijital unsurlu önemli ürün olarak nitelendirilmenin hukuki neticesi nedir? CRA uyarınca, bir ürün dijital unsurlu önemli ürün olarak nitelendirilmesi durumunda CRA'nın 32. maddesinin iki ve üçüncü fıkrasında yer alan uygunluk değerlendirme prosedürlerine tabi olacaktır.

Dijital unsurlu önemli ürün olarak nitelendirilmek önemli bir hukuki ve teknik külfet getirmektedir. Uygulamadaki belirsizlikleri ortadan kaldırmak adına CRA, ürün entegrasyonlarına ilişkin belirlilik getirmektedir. CRA uyarınca, EK 3. Bölümdeki ürün kategorisindeki ürünün temel işlevselliğine sahip olan dijital unsurlu ürünün başka bir ürüne entegre edilmesi, entegre edildiği ürünü doğrudan CRA'nın 32. Maddesinin ikinci ve üçüncü fıkralarındaki uygunluk değerlendirme prosedürlerine tabi hale getirmeyecektir.[85]

CRA'nın EK 3. Bölümünde dijital unsurlu önemli ürünler Sınıf I ve Sınıf II olmak üzere iki farklı kategoride belirlenmiştir. Her iki sınıftaki ürünlerin özel uyum kurallarına tabi olması için müteakip kriterleri sağlaması gerekmektedir:[86]

(1) Dijital unsurlu ürün, kimlik doğrulama ve erişim, izinsiz giriş önleme ve tespit, uç nokta güvenliği veya ağ koruması dahil olmak üzere diğer ürünlerin, ağların veya hizmetlerin siber güvenliği için kritik işlevleri yerine getirir.
(2) Dijital unsurlu ürün, ağ yönetimi, yapılandırma kontrolü, sanallaştırma veya kişisel verilerin işlenmesi dahil olmak üzere merkezi bir sistem işlevi gibi doğrudan manipülasyon yoluyla çok sayıda başka ürünü veya kullanıcılarının sağlığını, güvenliğini veya emniyetini bozma, kontrol etme veya bunlara zarar verme yoğunluğu ve yeteneği açısından önemli bir olumsuz etki riski taşıyan bir işlevi yerine getirir.

Dijital unsurlu önemli ürünler listesinin genişletilmesi için Avrupa Komisyonu'na özel bir yetki verilmiştir.[87] Avrupa Komisyonu, CRA'nın 6. maddesi uyarınca yetki devrine dayanan tasarruflar kabul etmek suretiyle, CRA'nın EK 3. Bölümünde yer alan ürünlere ilişkin şu değişiklikleri yapabilir:

(1) Dijital unsurlu ürün kategorilerinin her bir sınıfına yeni bir kategori eklenmesi,
(2) Tanımının belirtilmesi,
(3) Bir ürün kategorisinin bir sınıftan diğerine taşınması,
(4) Mevcut bir kategorinin bu listeden çıkarılması

[85] CRA, Madde 7(1).
[86] CRA, Madde 7(2).
[87] CRA, Madde 7(3).

Avrupa Komisyonu, EK 3. Bölümde yer alan listenin değiştirilmesine yönelik ihtiyacı değerlendirirken, dijital unsurlu önemli ürünlere ilişkin temel kriterleri ve bu bağlamda dijital unsurlu ürünlerin siber güvenlikle ilgili işlevlerini veya işlevini ve oluşturduğu siber güvenlik riskinin seviyesini dikkate alacaktır.[88]

EK 3. Bölüme ilişkin bir değişiklik gerçekleşirse zaman bakımından uygulaması nasıl gerçekleşecektir? Avrupa Komisyonu tarafından yetki devrine dayanan bir tasarruf yöntemiyle EK 3. Bölümde değişiklik yapıldığı zaman, bilhassa dijital unsurlu yeni bir ürün kategorisi Sınıf I veya Sınıf II listesine eklenirse veya Sınıf I'de düzenlenen bir ürün Sınıf II'ye taşındığı zaman, CRA'nın 32. maddesinin iki ve üçüncü fıkrasındaki uygunluk değerlendirme prosedürleri uygulanmaya başlanmadan evvel en azından 12 aylık bir geçiş süresi tanınması gerekmektedir.[89] Durum aciliyetinin haklı göstermesi durumunda daha kısa bir geçiş dönemi uygulanması gerektiği durumlarda bu sürenin kısaltılması mümkündür.

Avrupa Komisyonu'nun 11 Aralık 2025 tarihine kadar CRA'nın EK 3. Bölümünde belirtilen Sınıf I ve Sınıf II kapsamına giren dijital unsurlu ürün kategorilerinin teknik tanımını ve EK 4. Bölümde belirtildiği üzere dijital unsurlu ürün kategorilerinin teknik tanımını belirleyecek bir uygulama düzenlemesi hazırlaması gerekmektedir.[90]

CRA'nın Ek 3. Bölümünde listelenen dijital unsurlu önemli ürünler şu şekildedir:

Sınıf I

(1) Biyometrik okuyucular dahil olmak üzere kimlik doğrulama ve erişim kontrolü okuyucuları ile kimlik yönetim sistemleri ve ayrıcalıklı erişim yönetimi yazılımı ve donanımı
(2) Bağımsız ve gömülü tarayıcılar
(3) Şifre yöneticileri
(4) Kötü amaçlı yazılımları arayan, kaldıran veya karantinaya alan yazılımlar
(5) Sanal özel ağ (VPN) işlevine sahip dijital unsurlu ürünler
(6) Ağ yönetim sistemleri
(7) Güvenlik bilgi ve olay yönetimi (SIEM) sistemleri
(8) Önyükleme yöneticileri
(9) Açık anahtar altyapısı ve dijital sertifika oluşturma yazılımları
(10) Fiziksel ve sanal ağ arayüzleri

[88] CRA, Madde 7(3).
[89] CRA, Madde 7(3).
[90] CRA, Madde 7(4).

(11) İşletim sistemleri

(12) Routerlar, internet bağlantısı için tasarlanmış modemler ve switchler

(13) Güvenlikle ilgili işlevlere sahip mikroişlemciler

(14) Güvenlikle ilgili işlevlere sahip mikrodenetleyiciler

(15) Güvenlikle ilgili işlevlere sahip uygulamaya özel entegre devreler (ASIC) ve sahada programlanabilir kapı dizileri (FPGA)

(16) Akıllı ev genel amaçlı sanal asistanlar

(17) Akıllı kapı kilitleri, güvenlik kameraları, bebek izleme sistemleri ve alarm sistemleri dahil olmak üzere güvenlik işlevlerine sahip akıllı ev ürünleri

(18) . Avrupa Parlamentosu ve Konseyi'nin 2009/48/EC sayılı Direktifi[91] kapsamındaki sosyal etkileşimli özelliklere (konuşma veya film çekme gibi) veya konum izleme özelliklerine sahip internet bağlantılı oyuncaklar

(19) Sağlık izleme (takip gibi) amacı taşıyan ve 2017/745/EU sayılı ve 2017/746/EU sayılı Tüzüğün uygulanmadığı ve insan vücuduna takılan veya yerleştirilen kişisel giyilebilir ürünler veya çocuklar tarafından ve çocuklar için kullanılması amaçlanan kişisel giyilebilir ürünler

Sınıf II

1. İşletim sistemlerinin ve benzer ortamların sanallaştırılmış yürütülmesini destekleyen hipervizörler ve konteyner çalışma zamanı sistemleri
2. Güvenlik duvarları, saldırı tespit ve önleme sistemleri
3. Müdahaleye dayanıklı mikroişlemciler
4. Müdahaleye dayanıklı mikrodenetleyiciler

B. Dijital Unsurlu Kritik Ürünler

Dijital unsurlu kritik ürünler, çapraz-atıf yöntemiyle belirlenmiştir. CRA'nın Ek 4. bölümünde belirtilen bir ürün kategorisinin temel işlevselliğine sahip olan dijital unsurlu ürünler, dijital unsurlu kritik ürünler olarak kabul edilmektedir.[92]

Avrupa Komisyonu, dijital unsurlu ürün kategorilerini kapsayan bir Avrupa siber güvenlik sertifikasyon programının 2019/881/EU sayılı Tüzük uyarınca kabul edilmiş ve üreticilerin kullanımına sunulmuş olması koşuluyla, CRA'nın EK 1. Bölümünde veya ekin bazı kısımlarında belirtilen temel siber

[91] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys, OJ L 170/1, 30.6.2009.
[92] CRA, Madde 8(1).

güvenlik gerekliliklerine uygunluğu göstermek amacıyla CRA'nın EK 4. Bölümünde belirtilen bir ürün kategorisinin temel işlevselliğine sahip dijital unsurlu hangi ürünlerin 2019/881/EU sayılı Tüzük uyarınca kabul edilen bir Avrupa siber güvenlik sertifikasyon programı kapsamında en az 'önemli' güvence seviyesinde bir Avrupa siber güvenlik sertifikası alması gerektiğini belirlemek üzere, CRA'yı tamamlamak üzere 61. madde uyarınca yetki devrine dayalı tasarruflar kabul etme yetkisine sahiptir.[93]

Bu yetkilendirilmiş tasarruflar, dijital unsurlu ürünlerle ilişkili siber güvenlik riski düzeyiyle orantılı olması ve 2022/2555 sayılı Direktifin 3. maddesinin birinci fırkasında atıfta bulunulan temel kuruluşların bunlara olan kritik bağımlılığı da dahil olmak üzere amaçlanan hedeflerini dikkate alarak gerekli güvence düzeyini belirleyecektir.

Bu yetki devri tasarrufları, dijital unsurlu ürünlerle ilişkili siber güvenlik riski seviyesiyle orantılı olacak gerekli güvence seviyesini belirleyecek ve 2022/2555/EU sayılı Direktifin 3. maddesinin birinci fıkrasında atıfta bulunulan temel kuruluşların bunlara olan kritik bağımlılığı da dâhil olmak üzere, amaçlanan hedeflerini dikkate alacaktır.

Bu tür yetki devrine dayalı tasarrufları kabul etmeden önce Avrupa Komisyonu, öngörülen tedbirlerin potansiyel piyasa etkisine ilişkin bir değerlendirme yapması ve 2019/881/EU sayılı Tüzük kapsamında kurulan Avrupa Siber Güvenlik Sertifikasyon Grubu da dâhil olmak üzere ilgili paydaşlarla istişarelerde bulunması gerekmektedir. Değerlendirme, üye devletlerin ilgili Avrupa siber güvenlik sertifikasyon programının uygulanmasına yönelik hazırlık ve kapasite düzeyini dikkate alacaktır.

Avrupa Komisyonu'nun anılan yetki devri tasarruflarının henüz kabul edilmediği dönemde, CRA'nın EK 4. Bölümünde belirtilen bir ürün kategorisinin temel işlevselliğine sahip dijital unsurlu ürünler CRA'nın 32. maddesinin üçüncü fıkrasında bulunan uygunluk değerlendirme usullerine tabi olacaktır.

Yetki devri tasarrufları, aciliyet gerektiren nedenlerle daha kısa bir geçiş dönemi gerekçe gösterilmedikçe, en az altı aylık bir geçiş dönemi öngörmesi gerekmektedir.

Avrupa Komisyonu, 61. madde uyarınca, dijital unsurlu kritik ürün kategorilerinin eklenmesi veya çıkarılması suretiyle CRA'nın EK 4. Bölümünde değişiklik yapmak üzere yetki devrine dayalı tasarruflar kabul etme yetkisine sahiptir.[94] Komisyon, dijital unsurlu kritik ürün kategorilerini ve gerekli güvence seviyesini belirlerken, CRA'nın 7. maddesinin ikinci fıkrasında atıfta bulunulan kriterleri

[93] CRA, Madde 8(1).
[94] CRA, Madde 8(2).

dikkate alması gerekmektedir ve dijital unsurlara sahip ürün kategorilerinin aşağıdaki kriterlerden en az birini karşılamasını sağlayacaktır:

(1) 2022/2555/EU sayılı Direktifinin 3. maddesinde atıfta bulunulduğu üzere, dijital unsuru ürünler kategorisinde temel kuruluşların kritik bir bağımlılığı söz konusudur;
(2) Dijital unsuru ürünler kategorisine ilişkin olaylar ve istismar edilen güvenlik açıkları, AB iç pazarı genelinde kritik tedarik zincirlerinde ciddi aksamalara yol açabilir.

Avrupa Komisyonu, bu tür yetki devri tasarrufları kabul etmeden evvel, öngörülen tedbirlerin potansiyel piyasa etkisine ilişkin bir değerlendirme yapması ve 2019/881/EU sayılı Tüzük kapsamında kurulan Avrupa Siber Güvenlik Sertifikasyon Grubu da dâhil olmak üzere ilgili paydaşlarla istişarelerde bulunması gerekmektedir.

Yetki devri tasarrufları, aciliyet gerektiren nedenlerle daha kısa bir geçiş dönemi gerekçe gösterilmedikçe, en az altı aylık bir geçiş dönemi öngörmesi gerekmektedir.

EK 4

DİJİTAL UNSURLU KRİTİK ÜRÜNLER

1. Güvenlik kutulu donanım cihazları
2. 2019/944/EU sayılı Direktifin[95] 2. maddesinin yirmi üçüncü bendinde tanımlanan akıllı ölçüm sistemlerindeki akıllı sayaç ağ geçitleri ve güvenli kripto işlemecileri dahil olmak üzere gelişmiş güvenlik amaçlı diğer cihazlar
3. Güvenli unsurlar dahil akıllı kartlar veya benzeri cihazlar

VII. Dijital Unsurlu Ürünlerin Birlik İçerisinde Serbest Dolaşımına İlişkin Kurallar

CRA, bir Tüzük olarak dijital unsurlu ürünlerin siber güvenliğine ilişkin kriterleri belirlemektedir. AB genelinde yeknesak bir uygulama sağlamaktadır. CRA'nın 'Serbest dolaşım' başlıklı 4. maddesinde de vurgulandığı üzere üye devletler, CRA kapsamına giren konularda, CRA ile uyumlu dijital unsurlu ürünlerin piyasaya sunulmasını engellemeyecektir. AB iç pazarında dijital unsurlu ürünlerin serbest dolaşım açısından CRA genel bir serbestlik rejimi temin etmektedir.

Peki, dijital unsurlu bir ürün CRA'ya tam uyum sağlamayan veya henüz tamamlanmamış ürünlerin AB içerisinde dolaşıma girebilir mi? CRA, bu konuda da bir kural getirmektedir. Üye devletler, ticaret fuarlarında, sergilerde, gösterimlerde veya benzer etkinliklerde, prototipleri de dahil olmak üzere, CRA

[95] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019.

ile uyumlu olmayan dijital unsurlu bir ürünün, ürünün CRA ile uyumlu olmadığını ve uyumlu hale gelene kadar piyasaya sürülmeyeceğini açıkça belirten görünür bir işaretle sunulması koşuluyla, sunulmasını veya kullanılmasını engellemeyecektir.[96]

Benzer şekilde, üye devletleri yazılımın CRA ile uyumlu olmadığını ve test dışında bir amaçla piyasada bulunmayacağını açıkça belirten görünür bir işaret ile yalnızca test amacıyla gerekli olan sınırlı bir süre için kullanıma sunulması koşuluyla, CRA ile uyumlu olmayan tamamlanmamış yazılımın piyasada bulunmasını engellemeyecektir.[97] Tamamlanmamış yazılımlara ilişkin verilen özel izin, AB'nin uyumlaştırma mevzuatı kapsamına gire güvenlik bileşenleri için uygulama alanı bulmayacaktır.[98]

Peki, üye devletler dijital unsurlu ürünler için CRA'da belirtilen güvenlik kriterlerini aşan ilave güvenlik kriterleri getirebilirler mi? CRA'nın 'Dijital unsurlu ürünlerin tedariği ve kullanımı' başlıklı 5. maddesi bu konuda özel bir kural getirmektedir. Söz konusu hüküm uyarınca CRA, üye devletlerin dijital unsurlu ürünleri, bu ürünlerin ulusal güvenlik veya savunma amaçları için tedarik edildiği veya kullanıldığı durumlar da dahil olmak üzere, belirli amaçlar doğrultusunda tedarik edilmesi veya kullanılması için, söz konusu gerekliliklerin üye devletlerin AB hukukunda belirtilen yükümlülükleriyle tutarlı olması ve bu amaçların gerçekleştirilmesi için gerekli ve orantılı olması koşuluyla, ek siber güvenlik gerekliliklerine tabi tutmasını engellememektedir.

AB hukukunda belirlenen yükümlülüklerle tutarlı olması ve bu amaçların gerçekleştirilmesi için gerekli ve orantılı olması koşullarıyla dijital unsurlu ürünler için üye devletler tarafından ek siber güvenlik gereklilikleri getirilebilecektir.

Kamu alımları için ise daha objektif bir kriter getirilmektedir. AB'nin kamu ihale hukukuna ilişkin temel düzenlemeleri olan 2014/24/EU[99] ve 2014/25/EU[100] sayılı Direktiflerindeki kurallara halel gelmeksizin, üye devletlerin CRA'nın kapsamına giren dijital unsurlu ürünler tedarik ederken, bilhassa üreticilerin siber güvenlik açıklarını etkili şekilde yönetme kabiliyetlerine ilişkin olanlar başta olmak üzere, CRA'nın EK 1. Bölümünde yer alan temel siber güvenlik gerekliliklerini yerine getiriyor olmaları gerekmektedir.

---

[96] CRA, Madde 4(2).
[97] CRA, Madde 4(3).
[98] CRA, Madde 4(4).
[99] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, OJ L 94/65, 28.3.2014.
[100] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC, OJ L 94/243, 28.3.2014.

CRA, 2014/24/EU ile 2014/25/EU sayılı Direktiflere ilave bir kamu alımı teknik şartname kriteri getirmektedir. Kamu ihale piyasasına girişte CRA yükümlülüklerinin yerine getirilmiş olması (bilhassa da güvenlik açığı yönetim yeteneği) temel bir yeterlilik kriteri niteliğine dönüşmüştür.

VIII. CRA'nın Diğer Düzenlemelerle İlişkisi

A. Ürün Güvenliği Kurallarıyla İlişki

CRA gibi başka düzenlemeler de ürün güvenliğine ilişkin kurallar getirmektedir. Bunlardan en kapsayıcı olanı 2023/988 sayılı AB Ürün Güvenliği Tüzüğü'dür.[101] CRA, Ürün Güvenliği Tüzüğüyle olan ilişkisini özel olarak düzenlemektedir.

CRA, siber güvenlik risklerini hedefli şekilde düzenliyor olsa da dijital unsurlu ürünler, her zaman siber güvenlikle ilgili olmayan ancak bir güvenlik ihlalinin sonucu olabilecek başka güvenlik riskleri oluşturabilmektedir.[102] CRA uyarınca bu tür riskler CRA dışındaki ilgili AB uyum mevzuatı tarafından düzenlenmeye devam etmelidir.

CRA dışında herhangi bir AB uyum mevzuatının uygulanabilir olmaması halinde, CRA'nın hedeflenen niteliği ışığında AB Ürün Güvenliği Tüzüğü uygulanacaktır. Şöyle ki, AB Ürün Güvenliği Tüzüğü'nün 2. maddesinin birinci fıkrasının üçüncü bendinin (b) alt bendine istisna olarak, dijital unsurlu ürünler, CRA'nın kapsamına girmeyen hususlar ve riskler veya risk kategorileriyle ilgili olarak, AB Ürün Güvenliği Tüzüğü'nün 3. maddesinin yirmi yedinci fıkrasında tanımlanan 'Birlik uyum mevzuatında' belirtilen özel gerekliliklere tabi değillerse, AB Ürün Güvenliği Tüzüğü'nün Üçüncü Bölümünün Birinci Kısmı, Beşinci ve Yedinci Bölümü, Dokuzuncu Bölümü, Onuncu Bölümü ve On Birinci Bölümü kurallarına tabi olacaktır.[103]

B. Yapay Zekâ Kurallarıyla İlişki

CRA'nın ilişkisini açıkça çizdiği bir diğer düzenleme ise AB Yapay Zekâ Tüzüğü'dür.[104] Yapay Zekâ Tüzüğü'nün 15. maddesinde öngörülen doğruluk ve dayanıklılığa ilişkin gereklikler saklı kalmak kaydıyla, CRA kapsamına giren ve Yapay Zekâ Tüzüğü'nün 6. maddesi uyarınca yüksek riskli yapay

[101] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, EUR Lex OJ L 135, 23.5.2023.
[102] CRA, Resital 50.
[103] CRA, Madde 11.
[104] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) - EUR Lex L 2024/1689 12.7.2024.

zekâ sistemi olarak sınıflandırılan dijital unsurlu ürünler, CRA'nın 15. maddesinde belirtilen siber güvenlilik gerekliliklerine müteakipteki şekillerde uyum göstereceklerdir:[105]

(1) Bu ürünler CRA'nın EK Birinci Bölümünün 1. Kısmında belirtilen siber güvenlik gerekliliklerini karşılamalıdır.
(2) Üretici tarafından uygulamaya konulan süreçlerin CRA'nın EK 1. Bölümünün 2. Kısmında belirtilen temel siber güvenlik gerekliliklerine uygun olmalıdır; ve
(3) Yapay Zekâ Tüzüğü'nün 15. maddesi kapsamında gerekli olan siber güvenlik koruma seviyesine ulaşıldığı, CRA kapsamında düzenlenen AB uygunluk beyanında gösterilmelidir.

Bu kapsama giren dijital unsurlu ürünler ve gerekli siber güvenlik yükümlülükleri için Yapay Zekâ Tüzüğü'nün 43. maddesinde öngörülen uyumluluk değerlendirme prosedürü uygulanacaktır.

IX. Üreticinin CRA Yükümlülükleri

Girişte açıklandığı üzere üretici, dijital unsurlu ürünler geliştiren veya üreten ya da dijital unsurlu ürünler tasarlatan, geliştiren veya ürettiren ve bunları kendi adı veya ticari markası altında ücretli, paralı veya ücretsiz olarak pazarlayan gerçek veya tüzel kişiyi ifade etmektedir.

Dijital unsurlu ürünler, AB iç pazarında yalnızca CRA'nın EK 1 bölümünde belirtilen temel siber güvenlik gerekliliklerini sağlamaları ve uygun şekilde kurulmaları, bakımlarının yapılması ve amaçları doğrultusunda kullanılmaları veya makul olarak öngörülebilen koşullar altında ve uygulanabilir olduğu durumlarda, gerekli güvenlik güncellemeleri yüklenmiş olmaları halinde ve üretici tarafından uygulanan süreçlerin CRA'nın EK 1 Bölümünün 2. Kısmında yer alan temel siber güvenlik yükümlülükleriyle uyumlu olması durumunda AB iç pazarında dolaşıma girebilecektir.[106]

A. Üreticinin Siber Güvenlik Yükümlülükleri

1. CRA'nın EK 1 bölümünde yer alan gerekliliklere uygun tasarım, geliştirme ve üretim yapma yükümlülüğü

Üretici, dijital unsurlu bir ürünü piyasaya sürerken, bu ürünün CRA'nın EK 1 bölümünde belirtilen temel siber güvenlik gerekliliklerine uygun olarak tasarlandığından, geliştirildiğinden ve üretildiğinden emin olmak zorundadır.[107]

[105] CRA, Madde 12(1).
[106] CRA, Madde 6.
[107] CRA, Madde 13(1).

2. Siber güvenlik risk değerlendirmesi yapma yükümlülüğü

Üreticiler, dijital unsurlu bir ürünle ilişkili siber güvenlik risklerinin değerlendirmesini yapmalı ve bu değerlendirmenin sonucunu, siber güvenlik risklerini en aza indirmek, olayları önlemek ve kullanıcıların sağlık ve güvenliği de dahil olmak üzere etkilerini en aza indirmek amacıyla dijital unsurlu ürünün planlama, tasarım, geliştirme, üretim, teslimat ve bakım aşamalarında dikkate almalıdır.[108]

3. Siber güvenlik risk değerlendirmesini belgelendirme ve risk değerlendirmesini güncelleme yükümlülüğü

CRA, siber güvenliğe ilişkin hesap verebilirlik yaklaşımını benimsemiştir. Siber güvenlik gerekliliklerine tasarım, geliştirme ve üretim aşamalarında uyum yeterli değildir. Ayrıca bunun belgelendirilmesi gerekmektedir.

CRA uyarınca siber güvenlik risk değerlendirmesinin belgelendirilmesi ve CRA'da belirlenen destek süresi boyunca da güncellenmesi zorunludur.[109] Dolayısıyla, siber risk değerlendirmesi bir seferlik yapılan ve sona eren bir yükümlülük değil, tüm destek süresince devam eden bir yükümlülüktür. Dolayısıyla, üreticinin güncellemeleri de içeren bir süreç tasarımı yapması gerekmektedir.

CRA, siber riske yönelik hesap verebilirliğe ilişkin genel bir yükümlülük getirmekle yetinmeyip bu konuda nasıl hesap verileceğini, diğer bir deyişle risk değerlendirmesinin kapsamını da detaylıca belirlemektedir.

Siber güvenlik risk değerlendirmesi neleri içermelidir? Siber güvenlik risk değerlendirmesi, ürünün kullanımda olmasının beklendiği süreyi de dikkate alarak, asgari olarak operasyonel ortam veya korunacak varlıklar gibi dijital unsurlu ürünün kullanım koşullarının yanı sıra kullanım amacına ve makul olarak öngörülebilir kullanımına dayalı olarak siber güvenlik risklerinin bir analizini içermelidir.

Siber güvenlik risk değerlendirmesi, EK 1. Bölüm 1. Kısım, madde (2)'de belirtilen güvenlik gerekliliklerinin dijital unsurlu ilgili ürüne uygulanıp uygulanmayacağını ve uygulanacaksa ne şekilde uygulanacağını ve siber güvenlik risk değerlendirmesi tarafından bilgilendirilen bu gerekliliklerin nasıl uygulandığını da belirtmelidir. Ayrıca, üreticinin EK 1. Bölüm 1. Kısım, madde (1) ve EK 1. Bölüm 2. Kısım'da belirtilen güvenlik açığı işleme gerekliliklerini nasıl uygulayacağını da belirtmelidir.

[108] CRA, Madde 13(2).
[109] CRA, Madde 13(3).

4. Siber risk değerlendirmesine ilişkin şeffaflık yükümlülüğü

Dijital unsurlu bir ürün piyasaya arz edildiği zaman, üretici siber güvenlik risk değerlendirmesini CRA'nın 31. maddesi ve Ek 7. Bölüm uyarınca gerekli olan teknik belgelere dahil etmekle yükümlüdür.[110] Eğer ki, dijital unsurlu ürün başka bir AB düzenlemesine tabiyse ve o düzenleme kapsamında bir risk değerlendirmesi yapılması gerekiyorsa, üreticinin teknik dökümantasyonda temel siber güvenlik gerekliliklerinin dijital unsurlu ürün için geçerli olmadığına dair açık bir bilgiye yer vermesi gerekmektedir.[111]

5. Üçüncü taraflara ait bileşenlerin siber güvenlik uyumluluğuna dair özen gösterme yükümlülüğü

Üretici, siber güvenliğe ilişkin temel yükümlülükleri yerine getirmek amacıyla üçüncü taraflardan temin edilen bileşenleri entegre ederken bu tür bileşenlerin dijital unsurlu ürünlerin siber güvenliğine halel getirmediğine dair gerekli özeni göstermekle yükümlüdür.[112] Bu özen yükümlülüğü, ticari bir faaliyetle piyasaya sunulmamış olan açık kaynak yazılım (*free and open-source software*) bileşenlerini de entegre ederken geçerlidir.

6. Güvenlik açığını bildirme yükümlülüğü

Üretici, dijital unsurlu ürüne entegre edilmiş açık kaynak kodlu bir bileşen de dahil olmak üzere bir bileşende güvenlik açığı tespit ettiğinde, güvenlik açığını bileşeni üreten veya bakımını yapan kişi veya kuruluşa bildirmek ve güvenlik açığını CRA'nın EK 1. Bölümünün 2. Kısmında belirtilen güvenlik açığı işleme gerekliliklerine uygun olarak ele almak ve düzeltmekle yükümlüdür.[113]

Üretici, söz konusu bileşendeki güvenlik açığını ele almak için bir yazılım geliştirdiğinde veya donanım değişikliği gerçekleştirdiğinde, ilgili kodu veya belgeleri, bileşeni üreten veya bakımını yapan kişi veya kuruluşla uygun olduğunda makine tarafından okunabilir bir formatta paylaşmakla yükümlüdür.

7. Siber güvenlik risklerini sistematik şekilde belgelendirme yükümlülüğü

Üretici, farkına vardığı güvenlik açıklarını ve üçüncü taraflarca sağlanan ilgili bilgiler de dahil olmak üzere, dijital unsurlu ürünlerle ilgili siber güvenlik hususlarını, siber güvenlik risklerinin niteliği ve

[110] CRA, Madde 13(4).
[111] CRA, Madde 13(4).
[112] CRA, Madde 13(5).
[113] CRA, Madde 13(6).

siber güvenlik riskleriyle orantılı bir şekilde sistematik olarak belgelemek ve uygun olduğu hallerde, ürünlerin siber güvenlik risk değerlendirmesini güncellemekle yükümlüdür.[114]

8. Siber güvenlik açıklarını etkin şekilde yönetme yükümlülüğü

Üretici, dijital unsurlu bir ürünü piyasaya sürerken ve destek süresi boyunca, bileşenleri de dahil olmak üzere bu ürünün güvenlik açıklarının etkili bir şekilde ve CRA'nın EK 1. Bölümünün 2. Kısmında belirtilen temel siber güvenlik gerekliliklerine uygun olarak yönetmekle yükümlüdür. [115]

9. Siber güvenlik için destek süresi belirleme yükümlülüğü

CRA'da üreticiye getirilen bir diğer yükümlülük ise siber güvenlik için bir destek süresi belirleme yükümlülüğüdür.[116] Üretici, destek süresini, özellikle makul kullanıcı beklentilerini, kullanım amacı da dahil olmak üzere ürünün doğasını ve dijital unsurlu ürünün kullanım ömrünü belirleyen ilgili AB düzenlemelerini dikkate alarak, ürünün kullanımda olmasının beklendiği süreyi yansıtacak şekilde belirlemekle yükümlüdür.

Üretici, destek süresini belirlerken, diğer üreticiler tarafından piyasaya sürülen benzer işlevselliği haiz dijital unsurlu ürünlerin destek sürelerini, işletim ortamının kullanılabilirliğini, temel işlevleri sağlayan ve üçüncü taraflardan temin edilen entegre bileşenlerin destek sürelerini ve CRA'nın 52. maddesinin on beşinci fıkrası uyarınca kurulan özel idari işbirliği grubu (*Administrative Cooperation Group - ADCO*) ve Avrupa Komisyonu tarafından sağlanan ilgili rehberleri gözetecektir. Destek süresinin belirlenmesi için dikkate alınacak hususların orantılılığı sağlayacak şekilde ele alınması gerekmektedir.

CRA, destek süresinin nasıl belirleneceğine ilişkin kriterleri koyduktan sonra özel bir destek süresi de belirlenmelidir. CRA'ya göre destek süresi en az beş yıl olmalıdır.[117] Dijital unsurlu ürünün beş yıldan daha kısa bir süre kullanılmasının beklendiği durumlarda ise destek süresi beklenen kullanım süresine karşılık gelecektir. Diğer bir deyişle, CRA alt limiti kendisi belirlemekte, üst limit için ise üreticinin belirlenen kriter çerçevesinde aksiyon almasını öngörmektedir.

Avrupa Komisyonu, ADCO'nun tavsiyelerini dikkate alarak, piyasa gözetim verilerinin yetersiz destek sürelerine işaret ettiği belirli ürün kategorileri için asgari destek süresini belirlemek suretiyle düzenleme yapma yetkisini haizdir.[118]

---

[114] CRA, Madde 13(7).
[115] CRA, Madde 13(8).
[116] CRA, Madde 13(8).
[117] CRA, Madde 13(8).
[118] CRA, Madde 13(8).

Üretici, dijital unsurlu bir ürünün destek süresini belirlemek için dikkate alınan bilgileri CRA'nın EK 7. Bölümünde belirtildiği şekilde teknik belgelere dahil etmekle yükümlüdür.

10. Güvenlik açığı ifşa politikası başta olmak üzere uygun politika ve prosedürleri hazırlama yükümlülüğü

Üretici, dahili veya harici kaynaklardan bildirilen dijital unsurlu üründeki potansiyel güvenlik açıklarını işlemek ve düzeltmek için koordineli güvenlik açığı ifşa politikaları da dahil olmak üzere uygun politika ve prosedürlere sahip olması gerekmektedir.[119]

11. Güvenlik güncellemelerini en az 10 yıl boyunca kullanılabilir kılma yükümlülüğü

Üretici, destek süresi boyunca kullanıcılara sunulan her bir güvenlik güncellemesinin, yayınlandıktan sonra en az 10 yıl boyunca veya destek süresinin geri kalanı boyunca (hangisi daha uzunsa) kullanılabilir durumda kalmasını sağlamakla yükümlüdür.[120]

12. Yazılımların son sürümünde temel siber güvenlik gerekliliklerini sağlama yükümlülüğü

Üretici, bir yazılım ürününün büyük ölçüde değiştirilmiş sonraki sürümlerini piyasaya sürdüğü durumlarda, bu üretici yalnızca piyasaya en son sürdüğü sürüm için temel siber güvenlik gerekliliğine uygunluğu sağlamakla yükümlüdür.[121]

CRA, yeni bir versiyon geldiği zaman eski versiyonu kullanan kullanıcıları koruyucu nitelikte özel bir kural getirmektedir. Şöyle ki, daha önce piyasaya sürülen sürümlerin kullanıcıları, piyasaya en son sürülen sürüme ücretsiz olarak erişebilmeli ve bu ürünün orijinal sürümünü kullandıkları donanım ve yazılım ortamını yeniden ayarlamak için ek maliyet ödemek zorunda bırakılmamalıdır.

13. Halka açık yazılım arşivlerinde desteklenmeyen yazılım kullanımıyla ilgili riskler hakkında bilgilendirme yapma yükümlülüğü

Üretici, kullanıcıların geçmiş sürümlere erişimini artıran halka açık yazılım arşivleri tutması mümkündür.[122] Bu durumlarda, kullanıcılar desteklenmeyen yazılımların kullanımıyla ilgili riskler hakkında kolay erişilebilir bir şekilde açıkça bilgilendirilmelidir.

[119] CRA, Madde 13(8).
[120] CRA, Madde 13(9).
[121] CRA, Madde 13(10).
[122] CRA, Madde 13(11).

14. Teknik dökümantasyon hazırlama yükümlülüğü

Üretici, dijital unsurlu bir ürünü piyasaya sürmeden önce, CRA'nın 31. maddesinde düzenlenen teknik dokümantasyonu hazırlamakla yükümlüdür.[123]

15. Seçili uygunluk değerlendirme prosedürlerini yerine getirme yükümlülüğü

Üretici, CRA'nın 32. maddesinde düzenlenen seçilmiş uygunluk değerlendirme prosedürlerini yürütmek ve yürütülmesini sağlamakla yükümlüdür.[124]

16. Uygunluk beyanı hazırlama yükümlülüğü

Dijital unsurlu ürünün temel siber güvenlik gerekliliklerine ve üretici tarafından uygulamaya konulan süreçlerin temel siber güvenliğe uygunluğunun söz konusu uygunluk değerlendirme prosedürü ile kanıtlandığı durumlarda, üretici CRA'nın 28. maddesi uyarınca AB uygunluk beyanını hazırlamak ve CRA'nın 30. maddesi uyarınca CE işaretini ürüne eklemekle yükümlüdür.[125]

17. Teknik dökümantasyonu ve AB uygunluk beyanını 10 yıl boyunca hazır tutma yükümlülüğü

Üretici, dijital unsurlu ürüne ilişkin teknik dökümantasyonu ve AB uygunluk beyanını, dijital unsurlu ürünün piyasaya sürülmesinden sonra en az 10 yıl boyunca veya destek süresi boyunca (hangisi daha uzunsa) piyasa gözetim makamlarının kullanımına hazır tutmakla yükümlüdür.[126]

18. Seri üretimin parçası olan dijital unsurlu ürünlerin CRA'ya uyumlu kalması için tedbir alma yükümlülüğü

Üretici, bir seri üretimin parçası olan dijital unsurlu ürünlerin CRA'ya uyumlu kalması için prosedürler gelişmek zorundadır.[127] Üretici, dijital unsurlu ürünün geliştirme ve üretim sürecindeki veya tasarımındaki ya da özelliklerindeki değişiklikleri ve uyumlaştırılmış standartlardaki, Avrupa siber güvenlik sertifikasyon programlarındaki veya dijital unsurlu ürünün uygunluğunun beyan edildiği veya uygunluğunun doğrulandığı CRA'nın 27. maddesinde atıfta bulunulan ortak şartnamelerdeki değişiklikleri uygun şekilde dikkate almakla yükümlüdür.

[123] CRA, Madde 13(12).
[124] CRA, Madde 13(12).
[125] CRA, Madde 13(12).
[126] CRA, Madde 13(13).
[127] CRA, Madde 13(14).

19. Belirleyici kullanma yükümlülüğü

Üretici, dijital unsurlu ürünlerinin tip, parti veya seri numarası ya da tanımlanmalarını sağlayan başka bir unsur taşımasını veya bunun mümkün olmadığı durumlarda, bu bilgilerin ambalajlarında veya dijital unsurlu ürüne eşlik eden bir belgede yer almasını sağlamakla yükümlüdür.[128]

20. Tanıtıcı bilgilerini paylaşma ve erişilebilir kılma yükümlülüğü

Üretici, üreticinin adını, tescilli ticari unvanını veya tescilli ticari markasını ve posta adresini, e-posta adresini veya diğer dijital iletişim bilgilerini ve uygun olduğu hallerde üreticiyle iletişime geçilebilecek web sitesini dijital unsurlu ürünün üzerinde, ambalajında veya dijital unsurlu ürüne eşlik eden bir belgede belirtmekle yükümlüdür.[129] Bu bilgiler aynı zamanda kullanıcıya verilen bilgi ve talimatlarda da yer almak zorundadır. İletişim bilgileri, kullanıcılar ve piyasa gözetimi ve denetimi yetkilileri tarafından kolayca anlaşılabilecek bir dilde olmalıdır.

21. Tek iletişim noktası belirleme ve bunu şeffaf şekilde duyurma yükümlülüğü

Üretici, dijital unsurlu ürünün güvenlik açıklarının bildirilmesini kolaylaştırmak da dahil olmak üzere, kullanıcıların kendileriyle doğrudan ve hızlı bir şekilde iletişim kurmalarını sağlamak için tek bir iletişim noktası belirlemek ve bunu duyurmakla yükümlüdür.[130] Üretici, tek iletişim noktasının kullanıcılar tarafından kolayca tanımlanabilir olmasını sağlamakla yükümlüdür. Üretici, tek iletişim noktasını kullanıcıya verilen bilgi ve belgelere de dahil etmek zorundadır. Tek iletişim noktası, kullanıcıların tercih ettikleri iletişim araçlarını seçmelerine izin verecek şekilde tasarlanmalıdır ve tek irtibat noktası araçları otomatik araçlarla sınırlandırılmamalıdır.

22. Teknik bir dökümantasyon sağlama ve 10 yıl boyunca bu dökümantasyonu erişilebilir kılma yükümlülüğü

Üretici, dijital unsurlu ürünlere CRA'nın EK 2. bölümünde belirtilen kullanıcıya yönelik bilgi ve talimatların kâğıt veya elektronik formda eklemek zorundadır.[131] Bu tür bilgi ve talimatlar, kullanıcılar ve piyasa gözetimi ve denetimi yetkilileri tarafından kolayca anlaşılabilecek bir dilde sağlanmalıdır. Keza, açık, anlaşılır, anlaşılabilir ve okunaklı olmalıdırlar. En önemlisi de dijital unsurlu ürünlerin güvenli bir şekilde kurulmasına, çalıştırılmasına ve kullanılmasına izin vermelidirler.

[128] CRA, Madde 13(15).
[129] CRA, Madde 13(16).
[130] CRA, Madde 13(17).
[131] CRA, Madde 13(18).

Üreticiler, Ek 2. Bölümünde belirtilen kullanıcıya yönelik bilgi ve talimatları, dijital unsurlu ürünün piyasaya sürülmesinden sonra en az 10 yıl boyunca veya destek süresi boyunca (hangisi daha uzunsa) kullanıcıların ve piyasa gözetim ve denetim kuruluşlarının kullanımına hazır tutmakla yükümlüdür. Bu tür bilgi ve talimatların çevrimiçi olarak sağlandığı durumlarda, üreticiler bunların erişilebilir, kullanıcı dostu ve dijital unsurlu ürünün piyasaya sürülmesinden sonra en az 10 yıl boyunca veya destek süresi boyunca (hangisi daha uzunsa) çevrimiçi olarak mevcut olmasını sağlamakla yükümlüdür.

23. Destek süresini belirtme yükümlülüğü

Üretici, destek süresinin bitiş tarihini, en azından ay ve yıl da dahil olmak üzere, satın alma sırasında kolay erişilebilir bir şekilde ve uygun olduğu hallerde dijital unsurlu ürünün üzerinde, ambalajında veya dijital yollarla açık ve anlaşılır bir şekilde belirtilmesini sağlamakla yükümlüdür.[132] Dijital unsurlu ürünün niteliğine teknik olarak uygun düştüğü ölçüde, üretici kullanıcılara dijital unsurlu ürünlerinin destek süresinin sonuna ulaştığını bildiren bir bildirim görüntülemekle yükümlüdür.

24. AB uygunluk beyanını sunma yükümlülüğü

Üretici, ya AB uygunluk beyanının bir kopyasını ya da dijital unsurlar içeren basitleştirilmiş bir AB uygunluk beyanını ürünle birlikte sunmakla yükümlüdür.[133] Basitleştirilmiş bir AB uygunluk beyanı sağlandığında, tam AB uygunluk beyanına erişilebilecek tam internet adresi bu beyanla birlikte kullanıcıya sunulmalıdır.

25. CRA'ya uyumsuzlukta geri çağırma dahil derhal düzeltici eylemde bulunma yükümlülüğü

Piyasaya arzdan itibaren ve destek süresi boyunca, dijital unsurlu ürünün veya üretici tarafından uygulanan süreçlerin CRA'nın EK 1. bölümünde belirtilen temel siber güvenlik gerekliliklerine uygun olmadığını fark eden veya buna ilişkin için haklı gerekçesi olan üretici, dijital unsurlu ürünü veya üreticinin süreçlerini uygun hale getirmek için gerekli düzeltici önlemleri derhal almakla veya uygun olduğu şekilde ürünü geri çekmekle veya geri çağırmakla yükümlüdür.[134]

26. Piyasa gözetimi ve denetimi otoritelerine ilgili bilgi ve belgeleri verme ve işbirliği yapma yükümlülüğü

Üretici, bir piyasa gözetimi ve denetimi kuruluşunun gerekçeli talebi üzerine, söz konusu kuruluşa, dijital unsurlu ürünün ve üretici tarafından uygulamaya konulan süreçlerin CRA'nın EK 1. Bölümünde

[132] CRA, Madde 13(19).
[133] CRA, Madde 13(20).
[134] CRA, Madde 13(21).

belirtilen temel siber güvenlik gerekliliklerine uygunluğunu göstermek için gerekli olan tüm bilgi ve belgeleri, söz konusu kuruluşun kolayca anlayabileceği bir dilde, fiziken veya elektronik ortamda sağlamakla yükümlüdür.[135] Üretici, piyasaya sürdükleri dijital unsurlu ürünün oluşturduğu siber güvenlik risklerini ortadan kaldırmak için alınan her türlü önlem konusunda, talebi üzerine söz konusu kuruluşla işbirliği yapmakla yükümlüdür.

27. Faaliyetleri durdurmadan önce bunu duyurma yükümlülüğü

Faaliyetlerini durduran ve bunun sonucunda CRA'ya uyması mümkün olmayan bir üretici, faaliyetlerin durdurulması yürürlüğe girmeden önce, ilgili piyasa gözetimi ve denetimi makamlarının yanı sıra, mevcut herhangi bir yolla ve mümkün olduğu ölçüde, piyasaya sürülen dijital unsurlara sahip ilgili ürünlerin kullanıcılarına faaliyetlerin yaklaşan durdurulması konusunda bilgilendirmekle yükümlüdür.[136]

B. Üreticinin Siber Güvenlik Açığını Bildirim Yükümlülüğü

1. Genel siber güvenlik açığı bildirim yükümlülüğü

Üretici, farkına vardığı dijital unsurlu üründe bulunan ve aktif olarak istismar edilen herhangi bir güvenlik açığını eş zamanlı olarak uyarınca koordinatör olarak belirlenen Siber Olaylara Müdahale Merkezi (*CSIRT - Computer Security Incident Response Team*) birimine ve ENISA'ya bildirmekle yükümlüdür.[137] Üretici, aktif olarak istismar edilen güvenlik açığını CRA'nın 16. maddesi uyarınca oluşturulan tek raporlama platformu aracılığıyla ilgili birimlere bildirmesi beklenmektedir.

Peki, bildirim yükümlülüğünün kapsamı nedir? Üretici neleri bildirmek zorundadır? Üretici güvenlik açığı olduğu durumlarda şu kapsamda bildirim yapmak zorundadır:[138]

(1) Aktif olarak istismar edilen bir güvenlik açığına ilişkin olarak, gecikmeksizin ve her halükârda üreticinin bundan haberdar olmasından itibaren 24 saat içinde, uygulanabildiği hallerde, üreticinin dijital unsurlu ürünlerinin kullanıma sunulduğundan haberdar olduğu üye devletleri belirten bir erken uyarı bildirimi;

(2) İlgili bilgiler halihazırda sağlanmamışsa, gecikmeksizin ve her halükarda üreticinin aktif olarak istismar edilen güvenlik açığından haberdar olmasından itibaren 72 saat içinde, ilgili dijital unsurlu ürün hakkında, mevcut olduğu kadarıyla genel bilgiler içeren, istismarın ve ilgili güvenlik açığının

[135] CRA, Madde 13(22).
[136] CRA, Madde 13(23).
[137] CRA, Madde 14(1).
[138] CRA, Madde 14(2).

genel niteliği ile alınan düzeltici veya hafifletici önlemler ile kullanıcıların alabileceği düzeltici veya hafifletici tedbirleri, ayrıca, uygun olduğu hallerde, üreticinin bildirilen bilgileri ne kadar hassas olarak değerlendirdiğini belirten bir güvenlik açığı bildirimi;

(3) İlgili bilgiler halihazırda sağlanmamışsa, düzeltici veya hafifletici bir önlemin mevcut olmasından sonra en geç 14 gün içinde, en azından aşağıdakileri içeren bir nihai rapor:

   a. Şiddeti ve etkisi de dahil olmak üzere güvenlik açığının bir tanımı;
   b. Varsa, güvenlik açığından yararlanan veya yararlanmakta olan herhangi bir kötü niyetli aktörle ilgili bilgiler;
   c. Güvenlik açığını gidermek için kullanıma sunulan güvenlik güncellemesi veya diğer düzeltici önlemler hakkında ayrıntılar.

Bildirimi ilk alan koordinatör olarak belirlenen CSIRT, gerektiğinde üreticilerden aktif olarak istismar edilen güvenlik açığı hakkında ilgili durum güncellemeleri hakkında bir ara rapor sunmalarını talep etme yetkisini haizdir.[139]

2. Dijital unsurlu ürünün güvenliği üzerinde etkisi olan ciddi olayların bildirimi

Üretici, dijital unsurlu ürünün güvenliği üzerinde etkisi olan her türlü ciddi olayı eş zamanlı olarak uyarınca koordinatör olarak belirlenen CSIRT birimine ve ENISA'ya bildirmekle yükümlüdür.[140] Üretici, söz konusu olayı CRA'nın 16. maddesi uyarınca oluşturulan tek raporlama platformu aracılığıyla ilgili birimlere bildirmesi beklenmektedir.

Peki, bildirim yükümlülüğünün kapsamı nedir? Üretici neleri bildirmek zorundadır? Üretici güvenlik açısından etkili olan olaya ilişkin şu kapsamda bildirim yapmak zorundadır:[141]

(1) Dijital unsurlu ürünün güvenliği üzerinde etkisi olan ciddi bir olayın erken uyarı bildirimi, gecikmeksizin ve her halükârda üreticinin olaydan haberdar olmasından itibaren 24 saat içinde, en azından olayın yasadışı veya kötü niyetli eylemlerden kaynaklandığından şüphelenilip şüphelenilmediğini de içerecek şekilde, uygulanabilir olduğu hallerde, üreticinin dijital unsurlu ürününün kullanıma sunulduğunu bildiği üye devletleri de belirtecek şekilde;

(2) İlgili bilgiler halihazırda sağlanmamışsa, gecikmeksizin ve her halükârda üreticinin olaydan haberdar olmasından itibaren 72 saat içinde, varsa olayın niteliği, olayın ilk değerlendirmesi, alınan düzeltici veya hafifletici önlemler ve kullanıcıların alabileceği düzeltici veya hafifletici önlemler

[139] CRA, Madde 14(6).
[140] CRA, Madde 14(3).
[141] CRA, Madde 14(4).

hakkında genel bilgi sağlayacak ve ayrıca, uygun olduğu hallerde, üreticinin bildirilen bilgilerin ne kadar hassas olduğunu düşündüğünü belirtecek şekilde bir olay bildirimi;

(3) İlgili bilgiler halihazırda verilmemişse, olay bildiriminin yapılmasından sonraki bir ay içinde, en azından aşağıdakileri içeren bir nihai rapor:
    a. Olayın ciddiyeti ve etkisi de dahil olmak üzere ayrıntılı bir açıklaması;
    b. Olayı tetiklemiş olması muhtemel tehdit türü veya kök neden;
    c. Uygulanan ve devam eden hafifletme tedbirleri.

Ciddi etki unsuru nasıl belirlenecektir? Dijital unsurlu ürünün güvenliği üzerinde etkisi olan olay şu durumlarda ciddi olarak nitelendirilecektir:[142]

(1) Dijital unsurlu ürünün hassas veya önemli verilerin veya işlevlerin kullanılabilirliğini, gerçekliğini, bütünlüğünü veya gizliliğini koruma kabiliyetini olumsuz yönde etkiliyor veya olumsuz etkileyebilecek nitelikte olması; veya
(2) Dijital unsurlu bir ürüne veya dijital unsurlu bir ürünün kullanıcısının ağına ve bilgi sistemlerine kötü amaçlı kodun girmesine veya yürütülmesine yol açmış olması veya yol açabilecek nitelikte olması.

Bildirimi ilk alan koordinatör olarak belirlenen CSIRT, gerektiğinde üreticilerden dijital unsurlu ürünün güvenliği üzerinde etkisi olan ciddi olay hakkında ilgili durum güncellemeleri hakkında bir ara rapor sunmalarını talep etme yetkisini haizdir.[143]

3. Ortak hükümler

a. Yetkili makamlara bildirim

Üreticilerin yapacağı bildirimler, elektronik bildirim uç noktalarından biri kullanılarak tek raporlama platformu aracılığıyla sunulması gerekmektedir.[144] Bildirim, üreticinin AB içinde ana kuruluşlarının bulunduğu üye devletin koordinatörü olarak belirlenen CSIRT'in elektronik bildirim uç noktası kullanılarak sunulması ve eş zamanlı olarak ENISA tarafından erişilebilir hale getirilmesi gerekmektedir.

Peki, ana kuruluş nasıl belirlenecektir? CRA'nın amaçları doğrultusunda, bir üreticinin AB'deki ana kuruluşunun bulunduğu yer, dijital unsurlu ürünün siber güvenliğine ilişkin kararların ağırlıklı olarak

[142] CRA, Madde 14(5).
[143] CRA, Madde 14(6).
[144] CRA, Madde 14(7).

alındığı üye devlette olduğu kabul edilir.[145] Böyle bir üye devletin belirlenememesi halinde, ana kuruluşun, ilgili üreticinin AB içinde en fazla çalışana sahip kuruluşunun bulunduğu üye devlette olduğu kabul edilir.

Bir üreticinin AB'de ana işletmesinin bulunmadığı durumlarda, üretici bildirimlerini aşağıdaki sıraya göre belirlenen üye devlette koordinatör olarak belirlenen CSIRT'in elektronik bildirim uç noktasını kullanarak ve üreticinin elindeki bilgilere dayanarak göndermesi beklenmektedir:

(1) Üretici adına hareket eden yetkili temsilcinin, söz konusu üreticinin en fazla dijital unsurlu ürünü için yerleşik olduğu üye devlet,
(2) Üretici adına hareket eden yetkili temsilcinin, söz konusu üreticinin en fazla sayıda dijital unsurlu ürünü için yerleşik olduğu üye devlet,
(3) Söz konusu üreticinin dijital unsurlu en fazla sayıda ürünü piyasaya arz eden dağıtıcının yerleşik olduğu üye devlet,
(4) Söz konusu üreticinin dijital unsurlu ürünlerinin en fazla sayıda kullanıcısının bulunduğu üye devlet. (Bu durumda üretici, dijital unsurlu ürünün güvenliği üzerinde etkisi olan ve daha sonra aktif olarak istismar edilen herhangi bir güvenlik açığı veya ciddi olayla ilgili bildirimleri, ilk bildirimde bulunduğu koordinatör olarak belirlenmiş aynı CSIRT'e göndermesi mümkündür.)

b. Kullanıcılara bilgilendirme

CRA, yetkili kamu otoritelerine bildirim dışında tıpkı GDPR'ın veri öznelerine bildirimi gibi kullanıcılara da bilgi verilmesini öngören bir kural içermektedir.

Üretici, aktif olarak istismar edilen bir güvenlik açığının veya dijital unsurlu ürünün güvenliği üzerinde etkisi olan ciddi bir olayın farkına vardıktan sonra, dijital unsurlu ürünün etkilenen kullanıcılarını ve uygun olduğu durumlarda tüm kullanıcıları bu güvenlik açığı veya olay hakkında bilgilendirmekle yükümlüdür.[146]

Gerekli görülen hallerde, kullanıcıların söz konusu güvenlik açığı veya olayın etkisini azaltmak için uygulayabilecekleri her türlü risk azaltma ve düzeltici önlem de kullanıcılara bildirilmelidir. Uygun olduğu ölçüde bu bildirim yapılandırılmış, makine tarafından okunabilir ve otomatik olarak kolayca işlenebilir bir formatta gerçekleştirilmelidir.

[145] CRA, Madde 14(7).
[146] CRA, Madde 14(8).

Üreticinin dijital unsurlu ürünün kullanıcılarını zamanında bilgilendirmemesi durumunda, koordinatör olarak belirlenen bildirilmiş CSIRT'ler, söz konusu güvenlik açığı veya olayın etkisinin önlenmesi veya azaltılması için orantılı ve gerekli olduğu düşünüldüğünde kullanıcılara bu tür bilgileri sağlama yetkisini haizdir.[147]

CRA, siber olaydan hem etkilenen hem de etkilenmemiş olan tüm kullanıcıların bilgilendirilmesini öngörmektedir. Bu şekilde en üst düzey şeffaflığı sağlamaya çalışmaktadır.

B. Gönüllü Bildirim

CRA, tıpkı NIS 2 Direktifi gibi gönüllü bildirime izin vermektedir.[148] Üretici ve diğer gerçek veya tüzel kişiler, dijital unsurlu bir üründe bulunan herhangi bir güvenlik açığını ve dijital unsurlu bir ürünün risk profilini etkileyebilecek siber tehditleri, koordinatör olarak belirlenen bir CSIRT'e veya ENISA'ya gönüllülük esasına göre bildirebilirler. Keza, üretici ve diğer gerçek veya tüzel kişiler, dijital unsurlu ürünün güvenliği üzerinde etkisi olan herhangi bir olayı ve böyle bir olayla sonuçlanabilecek muhtemel durumları gönüllü olarak koordinatör olarak belirlenmiş bir CSIRT'e veya ENISA'ya bildirebilirler.

Koordinatör olarak belirlenen CSIRT veya ENISA bildirimleri prosedüre uygun olarak işleme koymakla yükümlüdür. Koordinatör olarak belirlenen CSIRT, zorunlu bildirimlerin işlenmesine gönüllü bildirimlere göre öncelik vermesi mümkündür.

Üretici dışındaki bir gerçek veya tüzel kişinin aktif olarak kullanılan bir güvenlik açığını veya dijital unsurlu bir ürünün güvenliği üzerinde etkisi olan ciddi bir olayı bildirmesi halinde, koordinatör olarak belirlenen CSIRT üreticiyi gecikmeksizin bilgilendirmekle yükümlüdür. Bu tür biri durumda, koordinatör olarak belirlenen CSIRT'ler ve ENISA, bildirimde bulunan bir gerçek veya tüzel kişi tarafından sağlanan bilgilerin gizliliğini ve uygun şekilde korunmasını sağlayacaktır.

Önemle vurgulamak gerekir ki, cezai suçların önlenmesi, soruşturulması, tespiti ve kovuşturulmasına halel getirmeksizin, gönüllü bildirim, bildirimde bulunan gerçek veya tüzel kişiye, bildirimde bulunmamış olsaydı tabi olmayacağı herhangi bir ilave yükümlülük yüklenmesine yol açmayacaktır.

C. Üreticinin Temsilci Kullanmasına İlişkin Özel Kurallar

CRA, üreticinin yetkili bir temsilci kullanmasını ilkesel olarak yasaklamamaktadır. Ancak bir temsilci kullanılacaksa buna ilişkin bazı kurallar belirlemekte ve bazı kısıtlamalar koymaktadır. CRA uyarınca

[147] CRA, Madde 14(8).
[148] CRA, Madde 15.

bir üretici, yazılı bir talimatla yetkili birisini belirleyebilecektir.[149] CRA, yazılı talimat ifadesini kullanmak suretiyle özel bir şekil şartı belirlemektedir.

Peki, CRA'daki tüm konulara ilişkin temsilci atanabilir mi? CRA, bu konuda belirli yasaklar koyarak temsilcinin CRA'nın 13. maddesinin 1 ila 11. fıkraları ile 13. maddenin on ikinci fıkrasının birinci bendi ve 13. maddenin on dördüncü fıkrasına ilişkin temsil yetkisi verilemeyeceğini öngörmüştür.[150]

Yetkili bir temsilci, üreticiden alınan talimatlarda belirtilen görevleri yerine getirmesi gerekmektedir. Yetkili temsilci, her şeyden evvel, üretici tarafından verilen yetki belgesinin bir kopyasını talep üzerine ilgili piyasa gözetimi ve denetimi otoritesine vermekle yükümlüdür.

Üretici tarafından yapılan yetkilendirmenin asgari olarak aşağıdaki hususları kapsaması zorunludur:[151]

(1) AB uygunluk beyanı ve atıfta bulunulan teknik belgeleri, dijital unsurlu ürün piyasaya sürüldükten sonra en az 10 yıl boyunca veya destek süresi boyunca (hangisi daha uzunsa) piyasa gözetim ve denetim makamlarının kullanımına hazır tutma;
(2) Bir piyasa gözetim otoritesinden gelen gerekçeli bir talebe ek olarak, ürünün dijital unsurlara uygunluğunu göstermek için gerekli tüm bilgi ve belgeleri söz konusu otoriteye sağlama;
(3) Yetkili temsilcinin yetkilendirmesi kapsamındaki dijital unsurlu ürünün oluşturduğu riskleri ortadan kaldırmak için alınan her türlü önlem konusunda, talepleri üzerine, piyasa gözetimi ve denetimi makamlarıyla işbirliği yapma.

Diğer bir ifadeyle CRA, atanan temsilcinin etkin bir temsilci olmasını ve CRA'ya ilişkin kritik konularda aktif rol oynayabilmesini aramaktadır.

X. İthalatçının CRA Yükümlülükleri

Girişte belirtildiği üzere ithalatçı, AB dışında yerleşik bir gerçek veya tüzel kişinin adını veya ticari markasını taşıyan dijital unsurlu bir ürünü piyasaya süren AB içinde yerleşik gerçek veya tüzel kişiyi ifade etmektedir.

CRA'nın odak noktası önceki bölümde ifade edildiği üzere üreticidir. Üretici dışında önemli rol ve sorumluluklar verilen bir diğer aktör ise ithalatçıdır. CRA, ithatlatçı üzerinden üretici üzerinden kontrol oluşturmaya çalışmakta ve CRA'yı tüm tedarik zinciri üzerinde uygulamaya çalışmaktadır.

[149] CRA, Madde 18(1).
[150] CRA, Madde 18(2).
[151] CRA, Madde 18(3).

A. CRA'ya uygun dijital unsurlu ürünü piyasaya arz etme yükümlülüğü

İthalatçı, CRA'nın EK 1. bölümünün birinci kısmında belirtilen temel siber güvenlik gerekliliklerine uygun olan ve üretici tarafından uygulanan süreçlerin CRA'nın EK 1. Bölümünün 2. Kısmında belirtilen siber güvenlik gerekliliklerine uygun olan dijital unsurlu ürünleri piyasaya sürebilir.[152]

B. Dijital unsurlu ürünü piyasaya sürmeden evvel teknik kontrol yapma yükümlülüğü

İthalatçı, dijital unsurlu bir ürünü piyasaya sürmeden evvel müteakipteki gerekliliklerin yerine getirildiğini temin etmek zorundadır:[153]

(1) CRA'nın 32. maddesinde düzenlenen ilgili uygunluk değerlendirme prosedürlerinin üretici tarafından yerine getirildiğini;
(2) Üretici tarafından teknik dökümantasyonun hazırlanmış olduğunu;
(3) Dijital unsurlu ürünün CRA'nın 30. maddesinde düzenlenen CE işaretini taşıdığını ve 13. maddenin yirminci fıkrasında düzenlenen AB uygunluk beyanının eklendiğini ve CRA'nın EK 2. bölümünde düzenlenen talimatların kullanıcılar ve piyasa gözetimi ve denetimi makamları tarafından kolayca anlaşılabilecek bir dilde olduğunu;

C. CRA'ya uyumululuğuna ilişkin belgeleri sağlama yükümlülüğü

CRA, üretici gibi ithalatçının da hesap verebilirlik yaklaşımıyla hareket etmesini beklemektedir. Bu doğrultuda, ithatlatçı CRA yükümlülüklerini yerine getirdiğini ispat eder nitelikteki belgeleri sağlamakla yükümlü tutulmuştur.[154]

Ç. CRA'ya uyumsuzluk durumunda piyasaya arzı durdurma yükümlülüğü

Bir ithalatçı, dijital unsurlu ürünün veya üretici tarafından uygulanan süreçlerin CRA ile uyumlu olmadığını düşündüğü veya buna inanmak için bir nedeni olduğu durumlarda, söz konusu ürün veya üretici tarafından uygulanan süreçler CRA ile uyumlu hale getirilinceye kadar ürünü piyasaya arz edemez.[155]

[152] CRA, Madde 18(1).
[153] CRA, Madde 18(2).
[154] CRA, Madde 18(2).
[155] CRA, Madde 18(3).

D. Dijital unsurlu üründe önemli bir siber güvenlik riski tespit edilmesi durumunda üretici ve piyasa gözetimi ve denetimi makamlarına bildirimde bulunma yükümlülüğü

Dijital unsurlu ürünün önemli bir siber güvenlik riski bulundurması durumunda ithalatçı, üreticiyi ve piyasa gözetimi ve denetimi makamlarını bu hususta bilgilendirmekle yükümlüdür.[156] Keza ithalatçı, dijital unsurlu ürünün teknik olmayan risk faktörleri ışığında önemli bir siber güvenlik riski oluşturabileceğine inanmak için nedenlerinin olması halinde, piyasa gözetimi ve denetimi makamlarını bu konuda bilgilendirmekle yükümlüdür.[157] Piyasa gözetim ve denetim makamlar bu tür bir bilgi aldıkları zaman CRA'da öngörülen prosedürleri işletmekle yükümlüdür.

E. Tanıtıcı bilgilerini paylaşma ve erişilebilir kılma yükümlülüğü

İthalatçı, adını, tescilli ticari unvanını veya tescilli ticari markasını ve posta adresini, e-posta adresini veya diğer dijital iletişim bilgilerini ve uygun olduğu hallerde kendisiyle iletişime geçilebilecek web sitesini dijital unsurlu ürünün üzerinde, ambalajında veya dijital unsurlu ürüne eşlik eden bir belgede belirtmekle yükümlüdür.[158] İletişim bilgileri, kullanıcılar ve piyasa gözetimi ve denetimi yetkilileri tarafından kolayca anlaşılabilecek bir dilde olmalıdır.

F. CRA'ya uyumsuzluğu tespit etmesi durumunda düzeltici önlemleri alma yükümlülüğü

Piyasaya sürdüğü dijital unsurlu bir ürünün CRA'ya uygun olmadığını bilen veya buna inanmak için nedeni olan ithalatçı, dijital unsurlu ürünün CRA'ya uygun hale getirilmesini sağlamak için gerekli düzeltici önlemleri derhal almak veya uygun düştüğü ölçüde ürünü geri çekmek veya geri çağırmakla yükümlüdür.[159]

Dijital unsurlu üründeki bir güvenlik açığının farkına varılması üzerine, ithalatçı bu güvenlik açığı hakkında üreticiyi gecikmeksizin bilgilendirmekle yükümlüdür.[160] Ayrıca, dijital unsurlu ürünün önemli bir siber güvenlik riski arz ettiği durumlarda, ithalatçı, dijital unsurlu ürünü piyasaya sunduğu üye devletlerin piyasa gözetimi ve denetimi makamlarını, özellikle uyumsuzluk ve alınan düzeltici önlemler hakkında ayrıntılı bilgi vererek, bu konuda derhal bilgilendirmekle yükümlüdür.

[156] CRA, Madde 18(3).
[157] CRA, Madde 18(3).
[158] CRA, Madde 18(4).
[159] CRA, Madde 18(5).
[160] CRA, Madde 18(5).

G. AB uygunluk beyanını 10 yıl boyunca bulundurma yükümlülüğü

İthalatçı, dijital unsurlu ürünün piyasaya sürülmesinden sonra en az 10 yıl boyunca veya destek süresi boyunca (hangisi daha uzunsa), AB uygunluk beyanının bir kopyasını piyasa gözetimi ve denetimi makamlarının kullanımına hazır tutmak ve teknik belgelerin talep üzerine bu makamlara sunulabilmesini sağlamakla yükümlüdür.[161]

Ğ. CRA'ya uygunluğa ilişkin piyasa gözetimi ve denetimi makamlarına bilgi ve belge verme yükümlülüğü

İthalatçı, bir piyasa gözetim ve denetim otoritesinden gelen gerekçeli bir talep üzerine, dijital unsurlu ürünün CRA'nın EK 1. Bölümünün 1. Kısmında belirtilen temel siber güvenlik gerekliliklerine uygunluğunu ve üretici tarafından CRA'nın EK 1. Bölümünün 2. Kısmında belirtilen temel siber güvenlik gerekliliklerine uygun olarak uygulanan süreçleri göstermek için gerekli tüm bilgi ve belgeleri fiziksel veya elektronik formda söz konusu otorite tarafından kolayca anlaşılabilecek bir dilde sağlamakla yükümlüdür.[162] Keza, piyasaya sürdüğü dijital unsurlu ürünün yarattığı siber güvenlik risklerini ortadan kaldırmak için alınan her türlü önlem konusunda, talebi üzerine, bu makamla işbirliği yapmakla yükümlüdür.

H. Üreticinin faaliyetlerini durdurması halinde ilgili piyasa gözetimi ve denetimi makamları ile kullanıcılara bunu duyurma yükümlülüğü

Dijital unsurlu bir ürünün ithalatçısı, söz konusu ürünün üreticisinin faaliyetlerini durdurduğunu ve sonuç olarak CRA'da belirtilen yükümlülüklere uyamayacağını öğrenmesi halinde, ilgili piyasa gözetim ve denetim makamlarını bu durum hakkında ve ayrıca mevcut herhangi bir yolla ve mümkün olduğu ölçüde, piyasaya sürülen dijital unsurlu ürünün kullanıcılarını bilgilendirmekle yükümlüdür.[163]

XI. Dağıtıcının CRA Yükümlülükleri

CRA'nın üretici ve ithatlatçı dışındaki bir diğer temel aktörü dağıtıcıdır. Dağıtıcı, tedarik zincirinde yer alan, üretici veya ithalatçı dışında, dijital unsurlu bir ürünü, özelliklerini etkilemeden AB pazarında kullanılabilir hale getiren gerçek veya tüzel kişi anlamına gelmektedir. Dağıtıcıya CRA'da getirilen yükümlülükler ithalatçıyla benzer niteliktedir.

[161] CRA, Madde 18(6).
[162] CRA, Madde 18(7).
[163] CRA, Madde 18(8).

A. CRA'ya uyumu dijital unsurlu ürünü piyasaya sürme yükümlülüğü

Dağıtıcı, dijital unsurlu bir ürünü piyasaya sunarken, CRA'da belirtilen gerekliliklerle ilgili olarak gerekli özeni göstermekle yükümlüdür.[164]

Dağıtıcı, dijital unsurlu bir ürünü piyasaya sunmadan evvel şu hususları doğrulamakla yükümlüdür:[165]

(1) Dijital unsurlu ürünün CE işareti taşıdığını kontrol yükümlülüğü,
(2) Üretici ve ithalatçının CRA'nın 13. maddesinin on beş, on altı, on yedi, on dokuz ve yirminci fıkraları ile 19. maddesinin dördüncü fıkrasında düzenlenen yükümlülüklere uyduğunu ve gerekli tüm belgeleri dağıtıcıya sağladığını kontrol yükümlülüğü.

B. CRA'ya uyumsuzluk durumunda piyasaya arzı durdurma yükümlülüğü

Bir dağıtıcı, elindeki bilgilere dayanarak, dijital unsurlu bir ürünün veya üretici tarafından uygulamaya konulan süreçlerin CRA'nın EK 1. Bölümünde belirtilen temel siber güvenlik gerekliliklerine uygun olmadığını düşündüğü veya buna inanmak için nedenlerinin olduğu durumlarda, dijital unsurlu ürünü, söz konusu ürün veya üretici tarafından uygulamaya konulan süreçler CRA ile uyumlu hale getirilene kadar piyasaya arz edemez.[166] Ayrıca, dijital unsurlu ürünün önemli bir siber güvenlik riski teşkil ettiği durumlarda, dağıtıcı gecikmeksizin imalatçıyı ve piyasa gözetimi ve denetimi otoritelerini bu konuda bilgilendirmekle yükümlüdür.

C. Dijital unsurlu üründe ciddi siber güvenlik riski tespit edilmesi durumunda üretici ve piyasa gözetimi ve denetimi makamlarını derhal bilgilendirme yükümlülüğü

Dijital unsurlu ürünün önemli bir siber güvenlik riski bulundurması durumunda dağıtıcı, üreticiyi ve piyasa gözetimi ve denetimi makamlarını bu hususta gecikmeksizin bilgilendirmekle yükümlüdür.[167]

Ç. CRA'ya uyumsuzluğu tespit etmesi durumunda düzeltici önlemler alma yükümlülüğü

Dağıtıcı, elindeki bilgilere dayanarak, piyasaya sunduğu dijital unsurlu bir ürünün veya üreticisi tarafından uygulanan süreçlerin CRA ile uyumlu olmadığını bilen veya buna inanmak için nedenleri olması halinde, dijital unsurlu ürünü veya üreticisi tarafından uygulanan süreçleri uygun hale getirmek veya gerekirse ürünü geri çekmek veya geri çağırmak için gerekli düzeltici önlemleri almakla yükümlüdür.[168]

---

[164] CRA, Madde 19(1).
[165] CRA, Madde 19(2).
[166] CRA, Madde 19(3).
[167] CRA, Madde 19(3).
[168] CRA, Madde 19(4).

D. Dijital unsurlu üründe güvenlik açığı tespit edilmesi durumunda üretici ve piyasa gözetimi ve denetimi makamlarına bildirimde bulunma yükümlülüğü

Dağıtıcı, dijital unsurlu üründe bir güvenlik açığının farkına vardığında, bu güvenlik açığını üreticiye gecikmeksizin bilgilendirmekle yükümlüdür.[169] Keza dağıtıcı, dijital unsurlu ürünün önemli bir siber güvenlik riski tespit etmesi durumunda, dijital unsurlu ürünü piyasaya sunduğu üye devletlerin piyasa gözetimi ve denetimi makamlarını, özellikle uygunsuzluk ve alınan düzeltici önlemler hakkında ayrıntılı bilgi vererek, derhal bilgilendirmekle yükümlüdür.[170]

E. CRA'ya uygunluğa ilişkin piyasa gözetimi ve denetimi makamlarına bilgi ve belge verme yükümlülüğü

Dağıtıcılar, bir piyasa gözetimi ve denetimi kuruluşunun gerekçeli talebine ek olarak, dijital unsurlu ürünün ve üreticisi tarafından uygulamaya konulan süreçlerin CRA'ya uygunluğunu göstermek için gerekli tüm bilgi ve belgeleri, söz konusu kuruluş tarafından kolayca anlaşılabilecek bir dilde, fiziksel veya elektronik ortamda sağlamakla yükümlüdür.[171] Keza, piyasaya sürdüğü dijital unsurlu ürünün yarattığı siber güvenlik risklerini ortadan kaldırmak için alınan her türlü önlem konusunda, talebi üzerine, bu makamla işbirliği yapmakla yükümlüdür.

F. Üreticinin faaliyetlerini durdurması halinde ilgili piyasa gözetimi ve denetimi makamları ile kullanıcılara bunu duyurma yükümlülüğü

Dijital unsurlu bir ürünün dağıtıcısı, söz konusu ürünün üreticisinin faaliyetlerini durdurduğunu ve sonuç olarak CRA'da belirtilen yükümlülüklere uyamayacağını öğrenmesi halinde, ilgili piyasa gözetimi ve denetimi makamlarını bu durum hakkında ve ayrıca mevcut herhangi bir yolla ve mümkün olduğu ölçüde, piyasaya sürülen dijital unsurlu ürünün kullanıcılarını bilgilendirmekle yükümlüdür.[172]

XII. Açık Kaynak Yazılım Sorumlusunun CRA Yükümlülükleri

CRA, açık kaynak yazılımların siber güvenlik ekosistemindeki önemini dikkate alarak bu alana ilişkin özel kurallar getirmektedir. Bu açıdan özel ve dar bir sorumluluk rejimi oluşturmaktadır.

CRA bağlamında açık kaynak yazılım sorumlusu (*open-source software steward*) "*özgür ve açık kaynaklı yazılım olarak nitelendirilen ve ticari faaliyetlere yönelik dijital unsurlu belirli ürünlerin geliştirilmesi için sistematik olarak sürekli destek sağlama amacı veya hedefi olan ve bu ürünlerin*

[169] CRA, Madde 19(4).
[170] CRA, Madde 19(4).
[171] CRA, Madde 19(5).
[172] CRA, Madde 19(5).

uygulanabilirliğini sağlayan, üretici dışındaki tüzel kişi" olarak tanımlanmıştır.[173] Önemle vurgulamak gerekir ki, açık kaynak yazılım sorumlusu kapsamda sadece tüzel kişiler vardır, özel kişiler yoktur. CRA gerekli risk değerlendirmesini yaparak bilinçli bir tercihle kapsamı dar tutmuştur.

A. Siber güvenlik politikası geliştirme yükümlülüğü

Açık kaynak yazılım sorumlusu, dijital unsurlu güvenli bir ürünün geliştirilmesini ve bu ürünün geliştiricileri tarafından güvenlik açıklarının etkili bir şekilde ele alınmasını desteklemek etmek için bir siber güvenlik politikası oluşturmak ve doğrulanabilir bir şekilde bunu belgelemekle yükümlüdür.[174]

Bu politika aynı zamanda söz konusu ürünün geliştiricileri tarafından güvenlik açıklarının CRA'nın 15. maddesinde düzenlendiği üzere gönüllü olarak bildirilmesini kolaylaştırıcı nitelikte olmalıdır ve açık kaynaklı yazılım sorumlusunun özel yapısını ve tabi olduğu yasal ve kurumsal düzenlemeleri dikkate almalıdır.[175] Bu politika, bilhassa güvenlik açıklarının belgelenmesi, ele alınması ve düzeltilmesi ile ilgili hususları içerecek ve keşfedilen güvenlik açıkları ile ilgili bilgilerin açık kaynak topluluğu içinde paylaşılmasını teşvik edecek nitelikte olması gerekmektedir.

B. Piyasa gözetimi ve denetimi makamlarıyla işbirliği yükümlülüğü

Açık kaynak yazılım sorumlusu, özgür ve açık kaynaklı yazılım olarak nitelendirilen dijital unsurlu ürünün yol açtığı siber güvenlik risklerini azaltmak amacıyla, talepleri üzerine, piyasa gözetimi ve denetimi otoriteleriyle işbirliği yapmakla yükümlüdür.[176] Bir piyasa gözetimi ve denetimi otoritesinden gelen gerekçeli bir talebin ardından, açık kaynaklı yazılım sorumlusu söz konusu otoriteye, söz konusu otorite tarafından kolayca anlaşılabilecek bir dilde, siber güvenliğe ilişkin belirtilen belgeleri kağıt veya elektronik formda sağlamakla yükümlüdür.

C. Siber güvenlik açıklarını bildirim yükümlülüğü

Açık kaynak yazılım sorumluları dijital unsurlu ürünlerin geliştirilmesine dahil oldukları ölçüde CRA'nın 14. maddesinin birinci fıkrasında üreticilere getirilen siber güvenlik açıklarını bildirim yükümlülüklerine tabi olacaklardır.[177] Keza, CRA'nın 14. maddesinin üçüncü fıkrası ve sekizinci fıkrasında belirtilen yükümlülükler, dijital unsurlu ürünlerin güvenliği üzerinde etkisi olan ciddi

[173] CRA, Madde 3(14).
[174] CRA, Madde 24(1).
[175] CRA, Madde 24(1).
[176] CRA, Madde 24(2).
[177] CRA, Madde 24(3).

olayların açık kaynaklı yazılım sorumluları tarafından bu tür ürünlerin geliştirilmesi için sağlanan ağ ve bilgi sistemlerini etkilediği ölçüde açık kaynaklı yazılım sorumluları için de uygulanacaktır.

Ç. Açık kaynak yazılımların güvenlik onayı

Yukarıda izah edildiği üzere, CRA'nın 13. maddesinin beşinci fıkrası uyarınca üretici, siber güvenliğe ilişkin temel yükümlülükleri yerine getirmek amacıyla üçüncü taraflardan temin edilen bileşenleri entegre ederken bu tür bileşenlerin dijital unsurlu ürünlerin siber güvenliğine halel getirmediğine dair gerekli özeni göstermekle yükümlüdür. Bu özen yükümlülüğü, ticari bir faaliyetle piyasaya sunulmamış olan açık kaynak yazılım bileşenlerini de entegre ederken geçerlidir.

Peki, ücretsiz ve açık kaynak yazılımların güvenlik tasdikleri nasıl sağlanacaktır? CRA'nın 'Özgür ve açık kaynak yazılımların güvenlik tasdikleri' başlıklı 25. maddesi uyarınca özellikle açık kaynaklı yazılım bileşenlerinin dijital unsurlu ürünlere entegre eden üreticilerle ilgili olarak CRA'nın 13. maddesinin beşinci fıkrasında belirtilen durum tespiti yükümlülüğünü kolaylaştırmak amacıyla AB Komisyonu, açık kaynaklı yazılım olarak nitelendirilen dijital unsurlu ürünlerin geliştiricilerinin veya kullanıcılarının yanı sıra diğer üçüncü tarafların bu tür ürünlerin tüm veya belirli temel siber güvenlik gerekliliklerine veya CRA'da belirtilen diğer yükümlülüklere uygunluğunu değerlendirmesine olanak tanıyan gönüllü güvenlik tasdik programları oluşturmak suretiyle CRA'yı tamamlamak üzere 61. madde uyarınca yetki devrine dayalı tasarruflar kabul etme yetkisine sahiptir.

XIII. Ortak Yükümlülükler

Girişte açıklandığı üzere, CRA'da statüler geçişken şekilde ve fonksiyonel olarak tanımlanmıştır. Dijital üründe esaslı değişiklik yapılması veya kendi adıyla piyasaya arz edilmesi durumunda üretici olmayan bir aktör de üretici olarak nitelendirilerek CRA'da üreticilere getirilen tüm yükümlülüklere ve sorumluluklara tabi olacaktır.

CRA'da dijital unsurlu ürünle ilgili tüm aktörler için üst bir kavram olarak 'ticari işletmeci' (*economic operator*) kavramı kullanılmaktadır. CRA'nın tanımlar başlıklı 3. maddesinde "*üretici, yetkili temsilci, ithalatçı, dağıtıcı veya dijital unsurlu ürünlerin imalatı veya dijital unsurlu ürünlerin CRA uyarınca piyasaya sunulması ile ilgili yükümlülüklere tabi olan diğer gerçek veya tüzel kişi*" olarak tanımlanmıştır.[178]

[178] CRA, Madde 3(12).

CRA'nın 'Ticari işletmecinin belirlenmesi' başlıklı 23. maddesi uyarınca talep halinde ticari işletmeci müteakipteki bilgileri piyasa gözetimi ve denetimi makamına sunmakla yükümlüdür:

(1) Kendilerine dijital unsurlu bir ürün tedarik etmiş olan herhangi bir işletmecinin adı ve adresi,
(2) Mevcut olduğu durumlarda, dijital unsurlu bir ürünü tedarik ettikleri herhangi bir işletmecinin adı ve adresi.

Bir ticari işletmeci, bu bilgileri, dijital unsurlu ürün tedarik edildikten sonra 10 yıl boyunca ve dijital unsurlu ürün tedarik ettikten sonra 10 yıl boyunca bu bilgileri sağlamakla yükümlüdür.[179]

XIV. Temel Siber Güvenlik Yükümlülükleri (EK 1)

EK 1

TEMEL SİBER GÜVENLİK GEREKLİLİKLERİ

Kısım I - Dijital unsurlu ürünlerin özelliklerine ilişkin siber güvenlik gereklilikleri

(1) Dijital unsurlu ürünler, risklere dayalı olarak uygun bir siber güvenlik düzeyi sağlayacak şekilde tasarlanır, geliştirilir ve üretilir.
(2) CRA'nın 13. maddesinin ikinci fıkrasında atıfta bulunulan siber güvenlik risk değerlendirmesi temelinde ve uygulanabilir olduğu hallerde, dijital unsurlu ürünler:
    a. Bilinen istismar edilebilir güvenlik açıkları olmaksızın piyasaya sunulmalıdır;
    b. Özel olarak geliştirilen dijital unsurlu bir ürünle ilgili olarak üretici ve ticari kullanıcı tarafından açıkça aksinin kararlaştırıldığı haller saklı kalmak kaydıyla, ürünü orijinal durumuna sıfırlama imkânı da dahil olmak üzere, varsayılan olarak güvenli (*secure by default*) bir yapılandırmayla piyasaya sunulmalıdır.
    c. Güvenlik açıklarının güvenlik güncellemeleri yoluyla giderilebilmesini sağlamalıdır. Buna, uygun bir zaman dilimi içerisinde varsayılan ayar olarak etkinleştirilen, açık ve kullanımı kolay bir devre dışı bırakma mekanizmasına sahip otomatik güvenlik güncellemeleri, mevcut güncellemelerin kullanıcılara bildirilmesi ve bunları geçici olarak erteleme seçeneği gibi olanaklar dahildir.
    d. Kimlik doğrulama, kimlik veya erişim yönetimi sistemleri dahil ancak bunlarla sınırlı olmamak üzere uygun kontrol mekanizmalarıyla yetkisiz erişime karşı koruma sağlamalıdır ve olası yetkisiz erişimi rapor edebilmelidir.

[179] CRA, Madde 23(2).

e. İlgili saklanan verileri veya aktarım halindeki verileri son teknoloji araçlarını kullanarak şifreleyerek veya diğer teknik çözümleri kullanarak depolanan, iletilen veya başka bir şekilde işlenen kişisel veya diğer verilerin gizliliğini korumalıdır.
f. Saklanan, iletilen veya başka bir şekilde işlenen kişisel veya diğer verilerin, komutların, programların ve yapılandırmanın bütünlüğünü kullanıcı tarafından yetkilendirilmemiş herhangi bir manipülasyon veya değişikliğe karşı korumalıdır ve bozuklukları rapor edebilmelidir.
g. Yalnızca dijital unsurlu ürünün belirtilen amacına uygun, bağlantılı ve sınırlı kişisel veri işlemelidir (veri minimizasyonu).
h. Hizmet reddi saldırılarına (DoS) karşı dayanıklılık ve hafifletme önlemleri de dahil olmak üzere, bir olaydan sonra da temel ve asli işlevlerin kullanılabilirliğini korumalıdır.
i. Ürünlerin kendilerinin veya bağlı cihazların diğer cihazlar veya ağlar tarafından sağlanan hizmetlerin kullanılabilirliği üzerindeki olumsuz etkilerini en aza indirmelidir.
j. Harici arayüzler de dahil olmak üzere saldırı yüzeylerini sınırlandıracak şekilde tasarlanmalı, geliştirilmeli ve üretilmelidir.
k. Uygun istismar azaltma mekanizmaları ve teknikleri kullanılarak bir olayın etkisini azaltacak şekilde tasarlanmalı, geliştirilmeli ve üretilmelidir.
l. Kullanıcı için bir devre dışı bırakma mekanizması da sunarak, verilere, hizmetlere veya işlevlere erişim veya bunların değiştirilmesi de dahil olmak üzere ilgili dahili faaliyetleri kaydederek ve izleyerek güvenlikle ilgili bilgiler sağlamalıdır.
m. Kullanıcılara tüm verileri ve ayarları güvenli ve kolay bir şekilde kalıcı olarak kaldırma imkânı sağlamalıdır ve bu tür verilerin diğer ürünlere veya sistemlere aktarılabildiği durumlarda bunun güvenli bir şekilde yapılmasını sağlamalıdır.

Kısım II – Güvenlik açıklarını yönetme gereklilikleri

Dijital unsurlu ürünlerin üreticileri:

(1) Asgari olarak ürünlerin üst düzey bağımlılıklarını kapsayan, yaygın olarak kullanılan ve makine tarafından okunabilen bir formatta bir yazılım içerik listesi hazırlamak da dahil olmak üzere, dijital unsurlu ürünlerde bulunan güvenlik açıklarını ve bileşenleri belirlemelidir ve belgelemelidir.

(2) Dijital unsurlu ürünlerde ortaya çıkan risklerle ilgili olarak, güvenlik güncellemeleri sağlamak da dahil olmak üzere, güvenlik açıklarını gecikmeden ele almalıdır ve gidermelidir; teknik olarak

mümkün olduğunda, yeni güvenlik güncellemeleri işlevsellik güncellemelerinden ayrı olarak sağlanmalıdır.

(3) Dijital unsurlu ürünün güvenliğine ilişkin etkili ve düzenli testler ve gözden geçirmeler uygulamalıdır.

(4) Bir güvenlik güncellemesi kullanıma sunulduktan sonra, güvenlik açıklarının tanımı, kullanıcıların etkilenen dijital unsurlu ürünü tanımlamasına olanak tanıyan bilgileri, güvenlik açıklarının etkileri, ciddiyeti ve kullanıcıların güvenlik açıklarını gidermesine yardımcı olan açık ve erişilebilir bilgiler dahil olmak üzere düzeltilen güvenlik açıkları hakkındaki bilgileri paylaşmalı ve kamuya açıklamalıdır. Üreticilerin söz konusu bilgilendirmenin güvenlik risklerinin güvenlik faydalarından daha ağır bastığını düşündüğü hallerde, bunu usulüne uygun olarak gerekçelendirilmeleri kaydıyla, kullanıcılara ilgili yamayı uygulama imkânı verilene kadar düzeltilmiş bir güvenlik açığı ile ilgili bilgileri kamuya açıklamayı erteleyebilirler.

(5) Eşgüdümlü güvenlik açığı ifşasına ilişkin bir politikayı yürürlüğe koymalıdır ve uygulamalıdır.

(6) Dijital unsurlu ürünlerindeki ve bu üründe yer alan üçüncü taraf bileşenlerdeki potansiyel güvenlik açıkları hakkında bilgi paylaşımını kolaylaştırmak için, dijital unsurlu üründe keşfedilen güvenlik açıklarının bildirilmesi için bir iletişim adresi sağlamak da dahil olmak üzere gerekli önlemleri almalıdır.

(7) Güvenlik açıklarının zamanında ve güvenlik güncellemeleri için geçerli olduğu durumlarda otomatik bir şekilde düzeltilmesini veya etkilerinin hafifletilmesini sağlamak için dijital unsurlu ürünlere yönelik güncellemeleri güvenli bir şekilde dağıtacak mekanizmalar sağlamalıdır

(8) Tespit edilen güvenlik sorunlarını ele almak için güvenlik güncellemelerinin mevcut olduğu durumlarda, bunların gecikmeksizin ve dijital unsurlu özel yapım bir ürünle ilgili olarak bir üretici ve bir ticari kullanıcı arasında aksi kararlaştırılmadıkça, alınacak potansiyel önlemler de dahil olmak üzere kullanıcılara ilgili bilgileri sağlayan tavsiye mesajları eşliğinde ücretsiz olarak dağıtılmasını sağlamalıdır.

XV. Kullanıcılara Bilgi ve Talimatlar (EK 2)

EK 3

KULLANICILARA BİLGİ VE TALİMATLAR

Dijital unsuru ürüne asgari olarak aşağıdakiler eşlik etmelidir:

(1) Üreticinin adı, kayıtlı ticari adı veya tescilli ticari markası ve posta adresi, e-posta adresi veya diğer dijital iletişim bilgilerinin yanı sıra, varsa, üreticiyle iletişime geçilebilecek web sitesi.

(2) Dijital unsurlu ürünün güvenlik açıkları hakkındaki bilgilerin bildirilebileceği ve alınabileceği ve üreticinin koordineli güvenlik açığı ifşasına ilişkin politikasının bulunabileceği tek iletişim noktası.

(3) Dijital unsuru ürünün adı, türü ve benzersiz bir şekilde tanımlanmasını sağlayan her türlü ek bilgi.

(4) Üretici tarafından sağlanan güvenlik ortamının yanı sıra ürünün temel işlevleri ve güvenlik özelliklerine ilişkin bilgiler de dahil olmak üzere dijital unsurlu ürünün kullanım amacı.

(5) Dijital unsurlu ürünün amacına uygun olarak veya önemli siber güvenlik risklerine yol açabilecek makul ölçüde öngörülebilir yanlış kullanım koşulları altında kullanımıyla ilgili bilinen veya öngörülebilir her türlü durum.

(6) Uygulanabilir olduğu durumlarda, AB uygunluk beyanının erişilebileceği internet adresi.

(7) Üretici tarafından sunulan teknik güvenlik desteğinin türü ve kullanıcıların güvenlik açıklarının ele alınmasını ve güvenlik güncellemelerini almayı bekleyebilecekleri destek süresinin bitiş tarihi;

(8) Ayrıntılı talimatlar veya bu tür ayrıntılı talimatlara ve bilgilere atıfta bulunan bir internet adresi:

a. İlk devreye alma sırasında ve dijital unsurlu ürünün kullanım ömrü boyunca güvenli kullanımını sağlamak için gerekli önlemler;
b. Dijital unsurlu üründeki değişikliklerin veri güvenliğini nasıl etkileyebileceği;
c. Güvenlikle ilgili güncellemelerin nasıl yüklenebileceği;
d. Kullanıcı verilerinin nasıl güvenli bir şekilde kaldırılabileceğine dair bilgiler de dahil olmak üzere dijital unsurlu ürünün güvenli bir şekilde hizmet dışı bırakılması;
e. EK 1. Bölümün 2. maddesinin (c) bendinin gerektirdiği şekilde güvenlik güncellemelerinin otomatik olarak yüklenmesini sağlayan varsayılan ayarın nasıl kapatılabileceği;
f. Dijital unsurlu ürünün dijital unsurlu diğer ürünlere entegre edilmesinin amaçlandığı durumlarda, entegratörün EK 1. Bölümde belirtilen temel siber güvenlik gerekliliklerine ve Ek 7. Bölümde belirtilen dokümantasyon gerekliliklerine uyması için gerekli bilgiler.

(9) Üreticinin yazılım içerik listesini kullanıcıya sunmaya karar vermesi halinde, yazılım içerik listesine nereden erişilebileceğine dair bilgi.

XVI. Teknik Dokümantasyon

EK 7

TEKNİK DOKUMANTASYONUN İÇERİĞİ

CRA'nın 31. maddesinde düzenlenen teknik dokümantasyon, dijital unsurlu ilgili ürün için geçerli olduğu şekilde, en azından aşağıdaki bilgileri içermesi gerekmektedir:

(1) Dijital unsurlu ürünün aşağıdakileri de içeren genel bir tanımı:

a. Kullanım amacı;
b. Temel siber güvenlik gerekliliklerine uyumu etkileyen yazılım sürümleri;
c. Dijital unsurlu ürünün bir donanım ürünü olduğu durumlarda, dış özellikleri, işaretlemeyi ve iç düzeni gösteren fotoğraflar veya çizimler;
d. EK 2. Bölümde belirtildiği şekilde kullanıcı bilgileri ve talimatları.

(2) Ürünün dijital unsurlarla tasarımı, geliştirilmesi ve üretimi ile güvenlik açığı işleme süreçlerinin, aşağıdakileri de içeren bir açıklaması:

a. Dijital unsuru ürünün tasarımı ve geliştirilmesine ilişkin gerekli bilgiler, uygulanabildiği yerlerde çizimler ve şemalar ve yazılım bileşenlerinin birbiri üzerine nasıl inşa edildiğini veya birbirini nasıl beslediğini ve genel işleme nasıl entegre olduğunu açıklayan sistem mimarisinin bir açıklaması;
b. Yazılım içerik listesi, koordineli güvenlik açığı ifşa politikası, güvenlik açıklarının bildirilmesi için bir iletişim adresi sağlandığına dair kanıt ve güncellemelerin güvenli dağıtımı için seçilen teknik çözümlerin açıklaması dahil olmak üzere üretici tarafından uygulamaya konulan güvenlik açığı işleme süreçlerine ilişkin gerekli bilgi ve özellikler;
c. Dijital unsurlu ürünün üretim ve izleme süreçlerine ve bu süreçlerin doğrulanmasına ilişkin gerekli bilgi ve özellikler.

(3) EK 1. Bölümde belirtilen temel siber güvenlik gerekliliklerinin nasıl uygulanabilir olduğu da dahil olmak üzere, dijital unsurlu ürünün 13. madde uyarınca tasarlandığı, geliştirildiği, üretildiği, teslim edildiği ve muhafaza edildiği siber güvenlik risklerinin bir değerlendirmesi.

(4) Dijital unsurlu ürünün 13. maddenin 8. fıkrası uyarınca destek süresinin belirlenmesinde dikkate alınan ilgili bilgiler.

(5) Referansları Avrupa Birliği Resmî Gazetesinde yayımlanmış olan tamamen veya kısmen uygulanan uyumlaştırılmış standartların bir listesi, CRA'nın 27. maddesinde düzenlenen ortak teknik şartlar veya CRA'nın 27 maddesinin sekizinci fıkrası uyarınca 2019/881/EU sayılı Tüzüğe göre kabul edilmiş Avrupa siber güvenlik sertifikasyon şemaları ve bu tür uyumlaştırılmış standartlar, ortak teknik şartlar veya Avrupa siber güvenlik sertifikasyon şemaları uygulanmadığı durumlarda uygulanan diğer teknik kuralların listesi dahil EK 1. ve 2. Bölümlerde düzenlenen temel siber güvenlik yükümlülüklerini karşılamak için alınan çözümlere ilişkin açıklamalar. Kısmen uygulanan uyumlaştırılmış standartlar, ortak teknik şartlar veya Avrupa siber güvenlik sertifikasyon planları olması durumunda, teknik dokümantasyon uygulanan kısımları belirtmelidir.

(6) Dijital unsurlu ürünün ve güvenlik açığı yönetme süreçlerinin EK 1. Bölüm ve 2. Bölümde belirtilen geçerli temel siber güvenlik gerekliliklerine uygunluğunu doğrulamak için gerçekleştirilen testlerin raporları.

(7) AB uygunluk beyanının bir kopyası.

(8) Uygulanabilir olduğu hallerde, EK 1. Bölümde belirtilen temel siber güvenlik gerekliliklerine uygunluğu kontrol edebilmesi için gerekli olması koşuluyla, bir piyasa gözetimi ve denetimi otoritesinden gelen gerekçeli bir talep üzerine yazılım içerik listesi.

XVII. Uyum Yöntemleri

CRA, düzenlediği her bir dijital unsurlu ürün kategorisine göre farklı nitelikte bir uyum yöntemi öngörmektedir. Uyumu ispat için temel olarak şu araçlar kullanılmaktadır:

(1) Uyumlaştırılmış standartlar (*harmonised standards*)

(2) Ortak teknik şartlar (*common specifications*)

(3) Avrupa siber güvenlik sertifikasyon şemaları (*European cybersecurity certification schemes*)

(4) Diğer yöntemler (*technical documentation*)

XVIII. Uygunluk Karinesi

Referansları Avrupa Birliği Resmî Gazetesinde yayınlanmış olan uyumlaştırılmış standartlara veya bunların bölümlerine uygun olan ve üretici tarafından uygulamaya konulan dijital unsurlara ve süreçlere sahip ürünlerin, bu standartlar veya bunların bölümleri kapsamında CRA'nın EK Birinci Bölümünde belirtilen temel siber güvenlik gerekliliklerine uygun olduğu varsayılacaktır.[180]

Avrupa Komisyonu, bir veya daha fazla Avrupa standardizasyon kuruluşundan, CRA'nın EK Birinci Bölümünde belirtilen temel siber güvenlik gereklilikleri için uyumlaştırılmış standartlar hazırlamasını talep etme yetkisini haizdir.[181] Komisyon, CRA için standardizasyon taleplerini hazırlarken, uyumlaştırılmış standartların geliştirilmesini kolaylaştırmak amacıyla, siber güvenliğe ilişkin mevcut veya geliştirilmekte olan Avrupa standartlarını ve uluslararası standartları dikkate almaya gayret edecektir.

[180] CRA, Madde 27(1).
[181] CRA, Madde 27(1).

Avrupa Komisyonu, CRA kapsamına giren dijital unsurlu ürünler için EK 1. Bölümde belirtilen temel siber güvenlik gerekliliklerine uymak için bir araç sağlayan teknik gereklilikleri kapsayan ortak spesifikasyonları belirleyen uygulama tasarrufları kabul etme yetkisini haizdir.[182]

Siber Güvenlik Yasası uyarınca kabul edilen bir Avrupa siber güvenlik sertifikasyon programı kapsamında bir AB uygunluk beyanı veya sertifikası verilen üretici tarafından uygulamaya konulan dijital unsurlara ve süreçlere sahip ürünlerin, AB uygunluk beyanı veya Avrupa siber güvenlik sertifikası veya bunların bazı bölümleri bu gereklilikleri kapsadığı sürece CRA'nın EK 1. Bölümünde belirtilen temel siber güvenlik gerekliliklerine uygun olduğu varsayılacaktır.[183]

XIX. AB Uygunluk Beyanı

Üretici, CRA'nın 13. maddesinin on ikinci fıkrası uyarınca EK 1. Bölümde belirtilen geçerli temel siber güvenlik gerekliliklerinin yerine getirildiğini kanıtladığını göstermek için uygunluk beyanı hazırlamakla yükümlüdür.[184]

AB uygunluk beyanı CRA'nın EK 5. Bölümünde belirtilen model yapıya sahip olmalıdır ve EK 8. Bölümde belirtilen ilgili uygunluk değerlendirme prosedürlerinde belirtilen unsurları içermelidir.[185] Böyle bir beyan uygun şekilde güncellenmesi gereklidir. Dijital unsuru ürünün piyasaya sürüldüğü veya piyasada bulundurulduğu üye devlet tarafından talep edilen dillerde hazır bulundurulması gerekmektedir.

CRA'nın 13. maddesinin yirminci fıkrasında atıfta bulunulan basitleştirilmiş AB uygunluk beyanı, EK 6. Bölümde belirtilen model yapısına sahip olması gerekmektedir.[186] Dijital unsurlu ürünün piyasaya sürüldüğü veya piyasada bulundurulduğu üye devlet tarafından talep edilen dillerde hazır bulundurulması zorunludur.

Dijital unsurlu bir ürünün AB uygunluk beyanı gerektiren birden fazla Birlik düzenlemesine tabi olması halinde, tüm AB yasal düzenlemeleri için tek bir AB uygunluk beyanı düzenlenecektir.[187] Bu beyan, yayın referansları da dahil olmak üzere ilgili Birlik yasal düzenlemelerinin tanımlanmasını içerecektir.

[182] CRA, Madde 27(2).
[183] CRA, Madde 27(3).
[184] CRA, Madde 28(1).
[185] CRA, Madde 28(2).
[186] CRA, Madde 28(2).
[187] CRA, Madde 28(3).

Üretici, AB uygunluk beyanı düzenleyerek ürünün dijital unsurlara uygunluğunun sorumluluğunu üstlenmektedir.[188]

Avrupa Komisyonu, teknolojik gelişmeleri dikkate almak amacıyla EK 5. Bölümde belirtilen AB uygunluk beyanının asgari içeriğine unsurlar eklemek suretiyle CRA'yı tamamlamak üzere 61. Madde uyarınca yetki devrine dayalı tasarruflar kabul etme yetkisine sahiptir.[189]

A. AB Uygunluk Beyanı (EK 5)

EK V

AB UYGUNLUK BEYANI

28. maddede atıfta bulunulan AB uygunluk beyanı şu bilgileri içermelidir:

(1) Dijital unsurlu ürünün benzersiz bir şekilde tanımlanmasını sağlayan ad, tür ve her türlü ek bilgi
(2) Üreticinin veya yetkili temsilcisinin adı ve adresi
(3) AB uygunluk beyanının sağlayıcının münhasıran sorumluluğu altında düzenlendiğine dair bir beyan
(4) Beyanın amacı (dijital unsurlu ürünün izlenebilirliğe izin verecek şekilde tanımlanması, uygun olduğu durumlarda fotoğraf da içerebilir)
(5) Yukarıda açıklanan beyanın amacının ilgili AB uyum mevzuatına uygun olduğuna dair bir beyan
(6) Kullanılan ilgili uyumlaştırılmış standartlara veya uygunluğun beyan edildiği diğer herhangi bir ortak spesifikasyona veya siber güvenlik sertifikasına yapılan atıflar
(7) Onaylanmış kuruluşun adı ve numarası, gerçekleştirilen uygunluk değerlendirme prosedürünün açıklaması ve verilen sertifikanın tanımı
(8) Ek bilgiler:

Adına ve hesabına imzalanmıştır:

(düzenlendiği yer ve tarih):

(isim, görev) (imza):

B. Basitleştirilmiş AB Uygunluk Beyanı (EK 6)

EK VI

BASİTLEŞTİRİLMİŞ AB UYGUNLUK BEYANI

[188] CRA, Madde 28(4).
[189] CRA, Madde 28(5).

13. maddenin yirminci fıkrasında düzenlenen basitleştirilmiş AB uygunluk beyanı şu bilgileri içermelidir:

İşbu belge ile, … [üreticinin adı], … [dijital unsurlu ürün tipinin tanımı] dijital unsurlu ürünün, (AB) 2024/2847 Tüzüğüne uygun olduğunu beyan eder.

AB uygunluk beyanının tam metni aşağıdaki internet adresinde mevcuttur:

XX. CE İşaretine İlişkin Genel Kurallar

CE işaretine ilişkin kurallar, AB'nin 765/2008 sayılı Tüzüğü'nün[190] 30. maddesinde belirlenen genel kurallara tabidir.[191]

CRA bağlamında CE işaretine ilişkin özel yükümlülükler şunlardır:

(1) CE işareti, dijital unsurlar ürüne görünür, okunaklı ve silinmeyecek şekilde iliştirilmesi gerekmektedir.[192] Dijital unsurlu ürünün niteliği nedeniyle bunun mümkün olmadığı veya garanti edilmediği durumlarda, ambalaja ve dijital unsurlu ürüne eşlik eden CRA'nın 28. maddesinde atıfta bulunulan AB uygunluk beyanına iliştirilmesi gerekmektedir. Yazılım şeklinde olan dijital unsurlu ürünler için, CE işareti ya 28. maddede atıfta bulunulan AB uygunluk beyanına ya da yazılım ürününe eşlik eden web sitesine iliştirilmesi gerekmektedir. İkinci durumda, web sitesinin ilgili bölümü tüketiciler tarafından kolayca ve doğrudan erişilebilir olmalıdır.

(2) Dijital unsurlu ürünün doğası gereği, dijital unsurlu ürüne iliştirilen CE işaretinin yüksekliği, görünür ve okunaklı kalması koşuluyla 5 mm'den daha düşük olması mümkündür.[193]

(3) CE işareti, dijital unsurlu ürün piyasaya sürülmeden önce iliştirilmesi zorunludur.[194] CE işaretini özel bir siber güvenlik riskini veya kullanımını gösteren bir piktogram veya başka bir işaret takip etmesi mümkündür.

(4) CE işareti, 32. madde uyarınca onaylanmış kuruluşun tam kalite güvencesine dayalı uygunluk değerlendirme prosedürüne dahil olduğu durumlarda, bu kuruluşun kimlik numarası takip etmelidir (modül H'ye göre).[195] Onaylanmış kuruluşun kimlik numarası, kuruluşun kendisi tarafından veya talimatları uyarınca üretici veya üreticinin yetkili temsilcisi tarafından ürüne iliştirilmelidir.

---

[190] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218, 13.8.2008.
[191] CRA, Madde 29.
[192] CRA, Madde 30(1).
[193] CRA, Madde 30(2).
[194] CRA, Madde 30(3).
[195] CRA, Madde 30(4).

Üye devletler, CE işaretini düzenleyen rejimin doğru bir şekilde uygulanmasını sağlamak için mevcut mekanizmaları geliştirmeleri beklenmektedir ve bu işaretin uygunsuz kullanımı durumunda uygun önlemleri almakla yükümlüdür.[196]

Dijital unsurlu ürün, CRA dışında da CE işaretinin iliştirilmesini de öngören AB uyum mevzuatına tabi olması halinde, CE işareti, ürünün söz konusu diğer AB uyum mevzuatında belirtilen gereklilikleri de karşıladığını belirtmelidir.

Avrupa Komisyonu, uygulama tasarrufları vasıtasıyla, dijital unsurlu ürünlerin güvenliğine ilişkin etiketler, piktogramlar veya diğer işaretler, bunların destek süreleri ve kullanımlarını teşvik edecek ve dijital unsurlar içeren ürünlerin güvenliği konusunda kamu bilincini artıracak mekanizmalar için teknik özellikler belirleme yetkisini haizdir.[197]

XXI. Siber Güvenlik Yükümlülüklerine Uyum

A. Temel Siber Güvenlik Yükümlülüklerine Uyum

CRA, dijital unsurlu ürünlerin uygunluğunun ispatı için farklı hesap verebilirlik yöntemleri öngörmektedir.[198] Üretici, EK 1. Bölümde belirlenen temel siber güvenlik yükümlülüklerinin karşılandığını ispat etmek için bir uygunluk değerlendirmesi yapmakla yükümlüdür. Üretici, temel siber güvenlik gerekliliklerine uyumu ispat etmek için müteakipteki herhangi bir prosedüre dayanması mümkündür:[199]

(1) CRA'nın EK 8. Bölümünde düzenlenen dahili kontrol prosedürü (Modül A'ya dayalı),
(2) EK 8. Bölümde düzenlenen AB-tipi inceleme prosedürü (Modül B'ye dayalı) ve ardından EK 8. Bölümde düzenlenen iç üretim kontrolüne dayalı AB-tipi uygunluk (Modül C'ye dayalı),
(3) EK 8. Bölümde düzenlenen tam kalite güvencesine dayalı bir uygunluk değerlendirmesi (modül H'ye dayalı), veya
(4) Mevcut ve uygulanabilir olduğu durumlarda, CRA'nın 27. maddesinin dokuzuncu fıkrası uyarınca bir Avrupa siber güvenlik sertifikasyon şeması.

[196] CRA, Madde 30(5).
[197] CRA, Madde 30(6).
[198] CRA, Madde 32.
[199] CRA, Madde 32(1).

B. Dijital Unsurlu Önemli Ürünler İçin Uyum

1. Dijital Unsurlu Önemli Ürün: Sınıf I Uyumu

EK 3. Bölümde belirtildiği üzere Sınıf I kapsamına giren dijital unsurlu önemli bir ürünün ve üreticisi tarafından uygulamaya konulan süreçlerin EK 1. Bölümde belirtilen temel siber güvenlik gerekliliklerine uygunluğunun değerlendirilmesinde, üreticinin 27. maddede atıfta bulunulduğu üzere en azından "önemli" düzeyde güvence sağlayan uyumlaştırılmış standartları, ortak spesifikasyonları veya Avrupa siber güvenlik sertifikasyon programlarını uygulamadığı veya sadece kısmen uyguladığı hallerde veya bu tür uyumlaştırılmış standartların, ortak teknik şartların veya Avrupa siber güvenlik sertifikasyon programlarının mevcut olmadığı durumlarda, ilgili dijital unsurlu ürün ve üretici tarafından uygulamaya konulan süreçler, söz konusu temel siber güvenlik gerekliliklerine ilişkin olarak aşağıdaki prosedürlerden birine sunulacaktır:

(1) EK 8. Bölümde düzenlenen AB-tipi inceleme prosedürü (Modül B'ye dayalı) ve ardından EK 8. Bölümde düzenlenen iç üretim kontrolüne dayalı AB-tipi uygunluk (Modül C'ye dayalı); veya

(2) EK 8. Bölümde düzenlenen tam kalite güvencesine dayalı bir uygunluk değerlendirmesi (modül H'ye dayalı).

2. Dijital Unsurlu Önemli Ürün: Sınıf II Uyumu

Ürün, CRA'nın EK 3. Bölümündeki Sınıf II kapsamına giren bir dijital unsurlara sahip önemli bir ürün olması durumunda, üretici, aşağıdaki prosedürlerden herhangi birini kullanarak EK 1. Bölümde belirtilen temel siber güvenlik gerekliliklerine uygunluğunu göstermekle yükümlüdür:[200]

(1) EK 8. Bölümde düzenlenen AB-tipi inceleme prosedürü (Modül B'ye dayalı) ve ardından EK 8. Bölümde düzenlenen iç üretim kontrolüne dayalı AB-tipi uygunluk (Modül C'ye dayalı);

(2) EK 8. Bölümde düzenlenen tam kalite güvencesine dayalı bir uygunluk değerlendirmesi (modül H'ye dayalı); veya,

(3) Mevcut ve uygulanabilir olduğu durumlarda, 2019/881/EU sayılı Tüzük uyarınca asgari olarak 'önemli' güvence seviyesini sağlayan CRA'nın 27. maddesinin dokuzuncu fıkrası uyarınca bir Avrupa siber güvenlik sertifikasyon programı.

[200] CRA, Madde 32(3).

C. Dijital Unsurlu Kritik Ürünler İçin Uyum

Ürün, CRA'nın 4. Bölümünde listelenen dijital unsurlara sahip kritik ürün olması durumunda, üretici aşağıdaki prosedürlerden birini kullanarak Ek 1. Bölümde belirtilen temel siber güvenlik gerekliliklerine uygunluğunu göstermekle yükümlüdür:[201]

(1) 8. maddenin birinci fıkrası kapsamında bir Avrupa siber güvenlik sertifikasyon programı; veya
(2) 8. maddenin birinci fıkrasındaki koşullar sağlanmazsa "Dijital Unsurlu Önemli Ürün: Sınıf II Uyumu" için öngörülen prosedürler uygulanmalıdır.

Ç. Açık Kaynak Kodlu Yazılımlar İçin Uyum

Yukarıda izah edildiği üzere, açık kaynak kodlu yazılım geliştiricileri de belirli koşullarda CRA yükümlülüklerine tabi hale gelebilmektedir. CRA; kapsamına giren açık kaynak kodlu yazılım üreticilerinin CRA'ya uyumlarını ispatı için genel bir kural getirmektedir. Şöyle ki, CRA'nın Ek 3. Bölümü kapsamına giren açık kaynak kodlu yazılım olarak nitelendirilen dijital unsurlu ürünlerin üreticileri, diğer bir deyişle dijital unsurlu önemli ürünlerin üreticisi olan açık kaynak yazılım geliştiricileri, CRA'nın EK 1. Bölümünde yer alan temel siber güvenlik yükümlülüklerine uyumu "Temel Siber Güvenlik Yükümlülüklerine Uyum" için öngörülen prosedürlerden birisini kullanarak sağlamaları gerekmektedir.[202] Bu durumda, CRA'nın 31. maddesinde atıfta bulunulan teknik dokümantasyon, bu tür ürünlerin piyasaya sürülmesi sırasında kamuya açık hale getirilmesi zorunludur.

D. Mikro İşletmeler ile KOBİ'lere İlişkin Ücret Kuralları

Uyum için sertifikasyon süreçleri maliyetli süreçlerdir. Bu hususu göze alan CRA, uygunluk değerlendirme prosedürleri için ücretler belirlenirken, yeni kurulan işletmeler de dahil olmak üzere, mikro işletmelerin ve küçük ve orta ölçekli işletmelerin özel çıkarları ve ihtiyaçlarının dikkate alınmasını zorunlu kılmaktadır ve bu ücretlerin, bu tür işletmelerin özel menfaatleri ve ihtiyaçları ile orantılı olarak azaltılması gerektiğini öngörmektedir.[203]

XXII. Üçüncü Ülkelerle Uyum Bağlamında İlişki

CRA uyarınca, Avrupa Birliği, üçüncü bir ülkenin teknik gelişmişlik düzeyini ve uygunluk değerlendirmesine ilişkin yaklaşımını dikkate alarak, uluslararası ticareti teşvik etmek ve

[201] CRA, Madde 32(4).
[202] CRA, Madde 32(5).
[203] CRA, Madde 32(6).

kolaylaştırmak amacıyla, Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın 218. maddesi uyarınca üçüncü ülkelerle karşılıklı tanıma anlaşmaları akdetme yetkisini haizdir.[204]

XXIII. Yaptırımlar

A. İdari Para Cezaları

Üye devletler, CRA'nın ihlallerine uygulanacak cezalara ilişkin kuralları belirlemek ve bunların uygulanmasını sağlamak için gerekli tüm tedbirleri almakla yükümlüdür.[205] CRA'ya aykırılıklar için öngörülen cezalar etkili, orantılı ve caydırıcı olmalıdır.

1. Kategori I: Ağır İhlaller

CRA'nın EK 1. Bölümünde düzenlenen temel siber güvenlik yükümlülükleri ile 13. maddesinde düzenlenen üreticinin yükümlülükleri ve 14. maddede düzenlenen üreticinin yükümlülükleri hükümlerine aykırılık durumunda:[206]

(1) 15.000.000 Euro'ya kadar idari para cezası,

(2) İhlali gerçekleştiren bir şirket ise, önceki mali yıl için dünya çapında toplam yıllık cirosunun %2.5'ına kadar, hangisi daha yüksekse, idari para cezası.

2. Kategori II: Orta İhlaller

CRA'nın 18-23 arasındaki maddeleri, 28. maddesi, 30. maddesinin birinci fıkrasından dördüncü fırkasına kadar, 32. maddenin birinci, ikinci ve üçüncü fıkrası, 33. maddenin beşinci fıkrası, 39. madde, 41. madde, 47. madde, 49. madde ve 53. maddelerine aykırılık durumunda:[207]

(1) 10.000.000 Euro'ya kadar idari para cezası,

(2) İhlali gerçekleştiren bir şirket ise, önceki mali yıl için dünya çapındaki toplam cirosunun %2'sine kadar, hangisi daha yüksekse, idari para cezası.

İdari para cezasına konu olacak söz konusu hükümler şu şekildedir:

> Madde 18 - Yetkili temsilciler
>
> Madde 19 - İthalatçıların yükümlülükleri
>
> Madde 20 - Dağıtıcıların yükümlülükleri

[204] CRA, Madde 34.
[205] CRA, Madde 64.
[206] CRA, Madde 64(2).
[207] CRA, Madde 64(3).

Madde 21 – Üreticilerin yükümlülüklerinin ithalatçılara ve dağıtıcılara uygulandığı durumlar

Madde 22 - Üreticilerin yükümlülüklerinin geçerli olduğu diğer durumlar

Madde 23 - Ekonomik operatörlerin tanımlanması

Madde 28 - AB uygunluk beyanı

Madde 30 - CE işaretinin iliştirilmesine ilişkin kurallar ve koşullar (Birinci, ikinci, üçüncü ve dördüncü fıkralar)

Madde 31 - Teknik dokümantasyon (Birinci, ikinci, üçüncü ve dördüncü fıkralar)

Madde 32 - Dijital unsurlu ürünler için uygunluk değerlendirme prosedürleri (Birinci, ikinci ve üçüncü fıkralar)

Madde 33 - Yeni kurulan işletmeler de dahil olmak üzere mikro işletmeler ve küçük ve orta ölçekli işletmeler için destek tedbirleri (Beşinci fıkra)

Madde 39 - Onaylanmış kuruluşlara ilişkin gereklilikler

Madde 41 - Onaylanmış kuruluşların iştirakleri ve onaylanmış kuruluşlar tarafından alt yüklenicilik

Madde 47 - Onaylanmış kuruluşların operasyonel yükümlülükleri

Madde 49 - Onaylanmış kuruluşlara ilişkin bilgi yükümlülüğü

Madde 53 - Veri ve belgelere erişim

3. Kategori III: Temel İhlaller

Bir talebe cevaben, bildirilmiş kuruluşlara ve piyasa gözetimi ve denetimi makamlarına yanlış, eksik veya yanıltıcı bilgi verilmesi durumunda:[208]

(1) 5.000.000 Euro'ya kadar idari para cezası;

(2) İhlali gerçekleştiren bir şirket ise, önceki mali yıl için dünya çapındaki toplam cirosunun %1'sine kadar, hangisi daha yüksekse, idari para cezası.

[208] CRA, Madde 64(4).

B. İdari Para Cezası Verilmesine İlişkin Esaslar

İdari para cezasının miktarı belirlenirken, her münferit olayda somut olayın ilgili tüm koşulları dikkate alınacak ve bilhassa aşağıdaki hususlar gözetilecektir:[209]

(1) İhlalin ve sonuçlarının niteliği, ağırlığı ve süresi;
(2) Benzer bir ihlal için aynı müteşebbise aynı veya diğer piyasa gözetimi ve denetimi makamları tarafından daha önce idari para cezaları uygulanıp uygulanmadığı;
(3) Bilhassa mikro işletmeler ve yeni kurulan işletmeler de dahil olmak üzere küçük ve orta ölçekli işletmeler açısından büyüklük ve ihlali gerçekleştiren müteşebbisin pazar payı.

İdari para cezaları, her bir somut olayın koşullarına bağlı olarak, aynı ihlal için piyasa gözetimi ve denetimi makamları tarafından uygulanan diğer düzeltici veya kısıtlayıcı tedbirlere ek olarak uygulanması mümkündür.[210]

İdari para cezalarını uygulayan piyasa gözetimi ve denetimi makamları, uyguladıkları idari para cezasını 2019/1020/EU sayılı Tüzüğün 34. maddesinde düzenlenen bilgi ve iletişim sistemi aracılığıyla diğer üye devletlerin piyasa gözetimi ve denetimi makamlarına bildirmekle yükümlüdür.[211]

Kamu kurum ve kuruluşlarına idari para cezası kesilebilir mi? CRA, bu konuda takdir yetkisini üye devletlere bırakmaktadır. Her üye devlet, söz konusu üye devlette yerleşik kamu makamlarına ve kamu kuruluşlarına idari para cezası verilip verilemeyeceğine ve ne ölçüde verilebileceğine ilişkin kuralları belirleyecektir.[212]

Keza, üye devletlerin hukuk sistemine bağlı olarak, idari para cezalarına ilişkin kurallar, para cezalarının yetkili ulusal mahkemeler veya diğer organlar tarafından söz konusu üye devletlerde ulusal düzeyde belirlenmiş yetkilere göre verileceği şekilde uygulanacaktır.[213] Bu üye devletlerde bu tür kuralların uygulanması eşdeğer bir etkiye sahip kabul edilecektir.

C. İdari Para Cezalarına İlişkin İstisna

CRA, idari para cezalarına özel bir istisna tanımaktadır. Müteakipteki durumlarda idari para cezaları uygulanmayacaktır:

[209] CRA, Madde 64(5).
[210] CRA, Madde 64(9).
[211] CRA, Madde 64(6).
[212] CRA, Madde 64(7).
[213] CRA, Madde 64(8).

(1) Mikro işletme veya küçük işletme olarak nitelendirilen üreticilerin CRA'nın 14. maddesinin ikinci fıkrasının (a) bendi veya 14. maddesinin dördüncü fıkrasının (a) bendinde yer alan sürelere uymamasına ilişkin ihlaller;
(2) Açık kaynak yazılım geliştiricileri tarafından CRA'nın herhangi bir şekilde ihlali.

XXIV. Uyum Maliyetleri, Riskler ve Diğer Eleştiriler

CRA, AB'nin son dönemdeki diğer dijital düzenlemeleri gibi kazuistik bir yaklaşımla kapsamına giren konuları düzenlemiştir. AB mevzuatına tam uyumun belirli riskleri de barındıracağı noktasında tereddüt etmemek gerekecektir. Nitekim, yasama süreçlerinde tıpkı Veri Yasası ve Veri Yönetişimi Yasası gibi birçok eleştiriye maruz kalmış ve hala eleştirilmektedir. Bu yasaların Türk hukukuna aktarılması, bu çerçevede yaşanan belirsizliklerin de aynı şekilde ülkemiz hukukuna aktarılması sonucunu beraberinde getirecektir.

CRA'nın hazırlanması sırasında kapsamlı bir etki analizi yapılmış ve özellikle uyum maliyeti üzerine değinilmiştir. Önemle vurgulamak gerekir ki, kapsamlı tartışmalar neticesinde CRA'nın mevcut düzenleme yöntemi (yatay düzlemde müdahale) tercih edilmiştir. CRA'ya yönelik yapılan etki değerlendirmesinde dört düzenleme yöntemi değerlendirilmiş ve mevcut yöntemde karar kılınmıştır.[214]

Etki analizinde ele alınan düzenleme yöntemleri şunlardır:

1) Yumuşak hukuk (*soft law*) yaklaşımı ve gönüllü tedbirler
2) Dijital unsurlara ve ilgili gömülü yazılımlara sahip somut ürünlerin siber güvenliği için ürüne özel geçici düzenleyici müdahale
3) Dijital unsurlara ve ilgili gömülü yazılımlara sahip somut ürünlerin siber güvenliği için yatay zorunlu kurallar ve gömülü olmayan yazılımlar için uygunluk değerlendirmesi için iki alt seçenekli kademeli bir yaklaşım içeren karma yaklaşım;
4) Gömülü olmayan yazılımlar da dahil olmak üzere dijital unsurlara sahip geniş kapsamlı ürünler için siber güvenlik gereklilikleri getiren, kapsam ve uygunluk değerlendirmesine ilişkin alt seçeneklere sahip yatay bir düzenleyici müdahale.[215]

[214] European Commission, 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, 15.9.2022 SWD(2022) 282 final PART 1/3, s. 28 vd.
[215] "A horizontal regulatory intervention introducing cybersecurity requirements for a broad scope of tangible and non-tangible products with digital elements, including non- embedded software"

AB tarafından yapılan etki değerlendirmesinde, tercih edilen seçeneğin dijital unsurları olan tüm ürünleri kapsayan ve kritik ürünler için zorunlu üçüncü taraf değerlendirmesini öngören 4. seçenek olduğu sonucuna varmıştır.

AB tarafından yapılan etki analizinde doğrudan uyum maliyetlerinin en çok yazılım ve donanım üreticilerini etkileyeceği belirtilmiştir. Uyumdaki temel maliyet unsurları şu şekilde belirlenmiştir:[216]

a) **Yeni yükümlülüklere aşinalık (bir defaya mahsus):** Girişim kapsamındaki üreticiler, dağıtıcılar ve ithalatçılar, yeni mevzuat kapsamındaki yükümlülüklere aşina olmak ve uyum stratejileri geliştirmek için uyum maliyetlerine katlanmak zorunda kalacaklardır (uygulama maliyetleri).

b) **Destek ve güvenlik güncellemelerinin yanı sıra güvenlik açığının ele alınmasıyla ilgili gereksinimler de dahil olmak üzere yaşam döngüsü boyunca güvenli ürün geliştirme (bir defaya mahsus ve tekrarlayan):** Uyum maliyetleri, güvenlik kontrollerinin ve özelliklerinin ürün tasarımına ve geliştirilmesine uygulanmasından (uyumluluğun düzenli olarak kontrol edilmesi ve güncellemelerin uygulanması için bir defaya mahsus ve tekrarlayan), vasıflı insan kaynaklarının işe alınmasından ve potansiyel ekipman ve malzeme maliyetlerinden (örneğin yeni güvenlik yazılımı) kaynaklanacaktır. Güvenlik kontrolleri ve özellikleri ayrıca son kullanıcılarla ürünün kullanım ömrü hakkında iletişim kurma ve onları bilgilendirme ve güvenlik desteği sağlama yükümlülüklerini de içerecektir.

c) **Güvenli ürün özellikleri ve kullanım talimatları hakkında son kullanıcılara yönelik bilgi ve şeffaflık gereklilikleri (bir defaya mahsus ve tekrarlayan):** Uyum maliyetleri, dijital ürünün güvenlik özellikleri ve kullanımına ilişkin bilgi yükümlülüklerinden kaynaklanacaktır.

d) **Uygunluk değerlendirmesi:** dahili ürün testi/öz değerlendirme, dahili testler için laboratuvar ve test ekipmanlarının satın alınması gibi bir defaya mahsus maliyetler ve test ekipmanlarının yeniden kalibrasyonu ve raporlama gibi tekrarlayan maliyetler ile üçüncü taraf ürün testi ve sertifikasyonu (sertifikasyon ücretleri için bir defaya mahsus ve sertifikasyonun sürdürülmesi için tekrarlayan maliyetler, örneğin düzenli denetimler).

e) **Diğer uygunluk maliyetleri ve raporlama yükümlülükleri:** Şirketlerin teknik dokümantasyon ve uygunluk beyanı geliştirmeleri, ürünlere işaretleme yapıştırmaları ve yetkililerin talebi üzerine ürünlerin uygunluğu hakkında raporlama yapmalarının yanı sıra

[216] European Commission, Commission Staff Working Document, Impact Assessment Report, s. 41.

istismar edilen güvenlik açıklarını ve olayları ENISA'ya bildirmeleri gerekecektir. Teknik belgelerin ve uygunluk beyanının düzenli olarak güncellenmesini sağlamak için iç sistemlerin ve prosedürlerin uygulamaya konulması gerekmektedir. Ayrıca, güvenlik açığı ve olay raporlama gereklilikleri işletmeler için hem bir defaya mahsus hem de tekrarlayan maliyetleri temsil edecektir (örneğin, raporlama sistemlerinin kurulması ve olayların düzenli olarak raporlanması).

CRA'ya uyumu çok fazla parametrenin dikkate alınmasını gerektirdiği için kesin bir uyum maliyeti hesabı yapmak mümkün değildir. Belirli modellere göre varsayımlara göre hareket edilmektedir. CRA etki değerlendirmesine göre donanım üreticileri uyum maliyetini yazılım üreticilerine göre daha düşük görmektedir.[217] Düzeltme maliyetleriyle ilgili olarak, güvenli ürün geliştirme maliyetlerinin tahmin edilmesine ilişkin şu şekilde bir yaklaşım benimsenmiştir: kapsamlı siber güvenlik önlemlerinin alınmaması durumunda ortalama %30,5 ek ürün geliştirme maliyeti öngörülmektedir.[218] Bu da dijital unsurlar içeren ortalama bir ürün (140.000 EUR) için 42.700 EUR ek ürün geliştirme maliyetine yol açmaktadır. Üreticilerin %50'sinin halihazırda yeterli güvenlik gerekliliklerini uyguladığı varsayılmıştır.

Görüldüğü üzere CRA esaslı bir uyum maliyeti getirmektedir. Bu maliyet KOBİ'ler için daha fazladır. KOBİ'ler hem maliyetler hem de faydalar açısından CRA'dan önemli ölçüde etkilenecektir. Etki analizi aşamasında AB geliştirme maliyetinin artmasının büyük şirketler ve üçüncü ülkeler karşısında rekabet dezavantajına neden olabileceği yönündeki endişeler olduğunu tespit etmiştir.[219] Öyle ki, uyum maliyetlerinin bazı KOBİ'ler tarafından karşılanamayacağı ve bunların piyasadan kaybolabileceği korkusu dahi dile getirilmiştir. Rapordan alıntılar yapmak gerekirse:

"*Maliyetler açısından, üreticiler olarak KOBİ'ler, çeşitli nedenlerden dolayı prensipte büyük şirketlerden daha fazla etkilenecektir. Daha büyük şirketler yeni düzenlemeye alışmanın bir defaya mahsus maliyetlerini daha kolay dağıtması mümkündür. Ayrıca, büyük şirketler genellikle daha geniş bir müşteri tabanına sahiptir ve bu nedenle sabit maliyetleri daha fazla müşteriye dağıtabilir (ölçek ekonomileri). En önemlisi, KOBİ'lerin sabit maliyetleri karşılayabilecek mali kapasiteleri çok daha sınırlıdır. İlk olarak, KOBİ'ler genel olarak siber güvenlik konusunda farkındalık ve bilgi eksikliği yaşayabilir, bu nedenle yeni güvenlik gereklilikleri hakkında bilgi toplamak ve bunları uygulamak onlar için daha maliyetli olabilir. Şirket içi teknik ve hukuki uzmanlığın sınırlı olması nedeniyle KOBİ'ler*

[217] European Commission, Commission Staff Working Document, Impact Assessment Report, s. 48.
[218] European Commission, Commission Staff Working Document, Impact Assessment Report, s. 49.
[219] European Commission, Commission Staff Working Document, Impact Assessment Report, s. 55.

dışarıdan danışmanlara başvurma eğilimindedir ve bu da toplam maliyetleri artırmaktadır. Ayrıca, laboratuvarlarının sınırlı kapasitesi nedeniyle - hem ekonomik kaynaklar hem de yetkinlikler açısından – KOBİ'ler yürürlükteki mevzuata uygunluğu sağlamak için harici test laboratuvarlarını veya onaylanmış kuruluşları kullanmak zorundadır. KOBİ'leri temsil eden ulusal bir ticaret birliğine göre, KOBİ'lerin %61'i siber güvenliklerini sağlamada engellerle karşılaştıklarını bildirmektedir; en büyük zorluklar yetersiz beceriler ve siber güvenlik maliyetleridir. ENISA anketine göre, KOBİ'lerin yaklaşık %12,3'ü bilgi güvenliği performanslarının "endüstri standartlarının altında" veya "çok altında" olduğuna inanırken, bu oran büyük işletmeler için sadece %2,1'dir. Bu rakamlar daha yüksek ek uyum maliyetlerine işaret ederken, aynı zamanda KOBİ'ler tarafından üretilen ürünlerin güvenlik seviyesinin yeterli bir güvenlik seviyesine getirilmesi ihtiyacına da işaret etmektedir."

İşlem maliyetleri dışında CRA için yapılan diğer eleştiriler şu şekildedir:[220]

- Siber kaynaklar hem endüstri hem de hükümetler için kıt olduğundan, tüm yazılımların CRA'nın kapsamına alınmış olması aşırı ve erken bir adım niteliğindedir.
- Ağa bağlı makineler ve sistemler için tüm temel bileşenlerin kritik ürünler olarak sınıflandırılması, üreticiler için bürokrasiye yol açma riski taşımaktadır. Zira, birçok endüstriyel bileşen yalnızca kritik olmayan amaçlar için kullanılmaktadır.
- CRA kapsamının geniş olması, üreticilerin ürünlerini üçüncü taraf sertifikasyon kuruluşları aracılığıyla sertifikalandırma zorunluluğunun yarattığı darboğazlar nedeniyle AB tedarik zincirlerinde COVID-19 tarzı aksaklıklara yol açması söz konusu olabilecektir.
- Ürün geliştiricileri dışında üçüncü kişilerin uygunluk değerlendirmesi yapılması yerinde görülmektedir. Risk, CRA'ya tabi dijital ürünlerin %90'ının hala üreticileri tarafından değerlendirilecek olması ve bunun da tüketicilerin emniyeti ve güvenliği için risk oluşturabilecek belirli miktarda ürünü piyasada bırakacak olmasıdır.
- Uygun standartların bulunmaması, onaylı ürünlerin tesliminde gecikmelere neden olabilecektir.
- Siber güvenlik olaylarını farklı makamlara bildirmenin şirketler üzerindeki yük oluşturma riski bulunmaktadır. ENISA'nın herhangi bir olayın bildirilmesi gereken merkezi raporlama kuruluşu olması gerektiği belirtilmiştir.
- Güvenlik açıkları ile ilgili bilgilerin kötüye kullanılmasını önlemek için güvenlik açığı açıklama gerekliliklerinin ele alınmasında güvenlik önlemlerinin dahil edilmemesi risk olarak görülmektedir.

[220] Bkz. European Parliament, EU Cyber Resilience Act, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf

- CRA çok katı bildirim yükümlülüğü getirmektedir ve yamalanmamış güvenlik açıklarının bildirilmesine ilişkin yükümlülüğün kaldırılması ve bunun yalnızca hafifletme eylemlerinin mevcut olduğu güvenlik açıklarının ifşa edilmesiyle sınırlandırılması gerekmektedir.

Peki hem büyük şirketler hem de KOBİ'ler açısından bu kadar maliyet getirmesine rağmen CRA'nın sağlayacağı temel faydalar nelerdir? Etki analizinde tespit edilen faydalar şunlardır:[221]

1) Hem yazılım hem de donanım üreticileri, ürünlerini etkileyen %33'lük siber güvenlik olaylarının sayısındaki azalmanın ardından itibar kaybının azalmasından fayda sağlayacaktır. Ayrıca, dijital unsurlu ürünlerin kullanıcıları olarak işletmeler de gelişmiş tedarik zinciri güvenliğinden faydalanacaktır. CE işaretli yazılım ve donanım ürünlerinin AB'de ve küresel çapta yaygınlaşması ve AB'nin teknolojik liderliğini güçlendirmesi muhtemeldir. Ayrıca hem yazılım hem de donanım üreticileri iç pazarın parçalanmasının önlenmesinden fayda sağlayacaktır.
2) CRA, siber güvenlik olaylarının %11 ila %18 oranında azalmasına ve olaylarla ilgili maliyetlerin de benzer oranda düşmesine yol açabilecektir. CRA'nın şirketleri etkileyen olaylardan kaynaklanan maliyetlerde AB çapında yıllık 97 Milyar Euro ila 158 Milyar Euro arasında bir azalmaya yol açabileceği tahmin edilmektedir.
3) Sadece donanımı değil yazılımı da kapsayacak olan CRA, siber güvenlik olaylarının %20 ila %33 arasında azalmasını sağlayabilir ve olayla ilgili maliyetleri de benzer oranda düşürebilir. Örneğin, tüm güvenlik olaylarının sadece küçük bir alt kümesini temsil eden veri ihlalleri ve DDoS saldırılarıyla ilişkili yıllık maliyetler sırasıyla 2.0 Milyar Euro ila 3.3 Milyar Euro ve 13 Milyar Euro ila 21.45 Milyar Euro azaltılabilir. CRA, şirketleri etkileyen olaylardan kaynaklanan maliyetlerde AB çapında yılda yaklaşık 180 milyar Euro ila 290 milyar Euro arasında bir azalmaya yol açabilir.
4) Sadece 290 milyar Euro'luk üst sınır faydasının uyum maliyetlerinden yaklaşık on kat daha yüksek olduğu tahmin edilmektedir. Söz konusu faydalar şu şekildedir: kullanıcılar için risk azaltma maliyetlerindeki düşüş; modern teknolojilere olan güvenin artması sonucunda dijital çözümlerin daha fazla benimsenmesi gibi ölçülebilir olmayan diğer faydaları hesaba katmamaktadır; dijital unsurlar içeren ürünlerin genel saldırı yüzeyindeki azalmanın bir sonucu olarak risk azaltma maliyetlerinde (siber güvenlik sigortası gibi) azalma; ürünlerindeki güvenlik açıklarını içeren daha az olaydan kaynaklanan üreticilere daha az itibar zararı; güvenlik açısından üreticilerin verimliliğinin artması; ve üye devletlerin markaya müdahale etmeye karar vermesi halinde üreticilerin karşı karşıya kalacağı potansiyel pazar parçalanması maliyetlerinin önlenmesi.

[221] European Commission, Commission Staff Working Document, Impact Assessment Report, s. 51 vd.

Peki bu fırsatlar için bu kadar katı bir düzenleme yapılması yerinde midir? AB'nin dijital alanda son dönemde gerçekleştirdiği yasama faaliyetlerine ilişkin getirilen en önemli eleştirilerden birisi de aşırı düzenleme (*overregluation*) sorunudur. Draghi raporunda da belirtildiği üzere AB içerisinde dijital alana ilişkin çok fazla regülasyon, çok fazla denetleyici ve düzenleyici otorite mevcuttur.[222] Dijital alanda faaliyet göstermek isteyen şirketler aynı zamanda birden fazla regülasyona tabi tutulmakta, birden çok otoriteyle muhatap olmaktadır. CRA, ürünlerin standardizasyonundan sertifikasyonuna ihlal bildiriminden denetimine kadar birçok kamu otoritesine ve kuruluşa yetki vermektedir. Diğer AB dijital düzenlemelerine yönelik getirilen eleştiriler CRA için de geçerlidir.

Öte yandan, aşırı düzenlemenin yerinde olduğu da ileri sürülebilir. Siber güvenlik gibi kıt insan kaynağının olduğu bir alanda, kazusitik düzenleme yapılmak suretiyle sistemin insana dayalı olmasına yönelik riskler azaltılabilecektir. Her ülkenin bu açıdan durumu *sui generis* niteliktedir. Genelleme yapmak doğru değildir.

XXV. Fırsatlar

A. AB ile Uyum, Mal ve Hizmet İhracatında Kolaylık

Veri Yasası ve Veri Yönetişimi Yasası'na yönelik fırsatlar CRA için de geçerlidir. AB'nin dijital alanda getirdiği birçok düzenleme, aynı zamanda bir pazara giriş engeli niteliği taşımaktadır. Bu husus, özellikle düzenlemelerin uygulama alanına bakıldığında daha da çarpıcı bir şekilde ortaya çıkmaktadır. Nitekim rekabet hukuku ve sermaye piyasası hukukundan esinlenerek benimsenen pazar yeri ilkesine göre bir pazara yönelik faaliyet gösteren, o pazarı hedefleyen her aktör, söz konusu pazarın şartlarına da riayet etmekle yükümlüdür. Bu açıdan bakıldığında GDPR ile başlayan dijital alandaki düzenlemeler, aktörün nerede kurulduğu ve faaliyet merkezinin nerede olduğundan bağımsız olarak AB pazarında faaliyet gösterilmesinin amaçlandığı takdirde AB mevzuatına uyum sağlanması zorunluluğunu öngörmektedir. Dolayısıyla AB dışında bulunan ve AB pazarında faaliyet göstermek isteyen aktörlerin de bu yükümlülüklere riayet etmesi gerekmektedir. AB mevzuatına uyum göstermeyen aktörler ise kural olarak AB pazarından dışlanacaktır.

Türkiye'de yerleşik veri ekonomisi aktörleri de bu durumdan doğrudan etkilenecektir. AB'de mevcut yasal düzenlemelere uyum sağlamayan aktörler açısından yukarıda etraflıca incelenen mevzuat hükümleri bir pazara giriş engeli teşkil edecektir. Dolayısıyla Türk hukukunun AB mevzuatına

[222] Mario Draghi tarafından hazırlanan ve AB'nin rekabet edebilirliğine ilişkin rapor: The future of European competitiveness – A competitiveness strategy for Europe, https://commission.europa.eu/topics/strengthening-european-competitiveness/eu- competitiveness-looking-ahead_en#paragraph_47059.

uyumlaştırılması, Türkiye'de yerleşik veri ekonomisi aktörleri açısından hem Türk hem de AB mevzuatına uyum anlamına gelecek, bu çerçevede gerçekleştirilecek olan mal ve hizmet ihracatında yasal engeller gündeme gelmeyecektir.

B. Çifte Standart Sorunu ve Rekabet Açısından Dezavantajlar

AB mevzuatına uyum sağlamamanın bir diğer sonucu ise, AB pazarına ürün ya da hizmet sunmak isteyen Türk üreticinin, AB'ye mal satabilmek için oradaki mevzuata uyum için veri paylaşımı ve siber güvenlik için belirli gereksinimleri yerine getirecek olması, ancak aynı ürünü Türk piyasasına arz ettiğinde Türk kullanıcıyı bu haklardan mahrum bırakmasıdır. Veri Yasası ve Veri Yönetişimi Yasası'na yönelik analizde de belirtildiği üzere uyum hem çifte standardın önlenmesine hem de rekabet avantajının sağlanmasına hizmet edebilecektir.

C. Türkiye'nin Kendi Standartlarını Oluşturması, Üreticinin Öncelikle Bu Standartlar Çerçevesinde Hareket Edebilmesi

Önem arz eden bir diğer husus, AB pazarında faaliyet göstermek isteyen Türk aktörlerin AB standartlarına uyum sağlamak zorunda olmalarına ilişkindir. Şöyle ki AB'ye mal veya hizmet ihracında bulunmak isteyen aktörler, AB tarafından geliştirilen standartları öncelikle esas alacak ve ürün ve hizmetlerini bu standartlara göre belirleyecektir. Bu durumda ise Türkiye'nin kendi ülkesinde kendi muhatapları üzerindeki hakimiyeti zayıflayacaktır. Nitekim Türk üretici ya da hizmet sunucu, Türk standartlarına göre değil AB standartlarına göre hareket edecektir. Ancak Türkiye'nin AB standartlarıyla uyumlu olacak şekilde kendi standartlarına sahip olması, bu standartları hızlı bir şekilde hayata geçirmesi, bir taraftan Türk veri ekonomisi açısından son derece faydalı olacak, diğer yandan AB ile uyum ve özellikle denetim hakimiyeti açısından önem taşıyacaktır. Nitekim söz konusu standartlara uyumu öncelikle Türk otoriteleri denetleyecek, bu sayede Türkiye'nin denetim hakimiyeti de tesis edilmiş olacaktır. Aksi takdirde dijital alandaki standart koyma hakimiyeti bütünüyle AB'ye devredilmiş olacaktır.

Ç. Siber Güvenlik Standartlarının Yükseltilmesi ve Rekabet Avantajları

Siber güvenliğin sağlanması, birçok hakkın korunmasına hizmet etmektedir. CRA gibi düzenlemelerle ulaşılmaya çalışılan nihai amaç bireylerin dijital araçları güvenle kullanmaları ve dijital ortamda başta mahremiyetleri olmak üzere temel hak ve hürriyetlerinin en etkin şekilde korunmasıdır. Anayasa Mahkemesinin bir kararında vurguladığı üzere "*Bireylerin güven içinde yaşamalarının sağlanmasında devlete yüklenen ödevler arasında şüphesiz siber güvenliğin sağlanması da yer almaktadır. Dolayısıyla*

siber güvenliğin sağlanmasının kamu güvenliğinin korunmasına yönelik olduğu anlaşılmaktadır.".[223] Dolayısıyla, siber güvenliğin sağlanmasında devletlerin aktif görevleri bulunmaktadır.

CRA gibi kapsamlı bir siber güvenlik düzenlemesine uyulması, her şeyden evvel temel hakların korunması açısından katkı sağlayacak niteliktedir. Dijital unsurlu ürün hangi amaçla kullanılıyorsa o alandaki hakların korunmasına hizmet edecektir.

Öte yandan, GDPR başta olmak üzere kişisel verilerle ilgili düzenlemelerin veri güvenliğini sağlamak için teknolojin geldiği son noktayı esas alması ve hesap verebilirlik üzerine sorumluluğu inşa etmeleri sebebiyle dijital unsurlu ürünler kullanırken CRA'nın ortaya koyduğu metodoloji pratiklik sağlayacaktır. Diğer bir deyişle, GDPR ve CRA arasında yakın bir ilişki vardır ve GDPR uyumu için de CRA'ya uyum sağlamak gerekecektir. GDPR uyumunun AB pazarına mal ve hizmet ihracı için önemli bir kısıt oluşturduğu dikkate alındığında, CRA'ya tam uyumun etkisi daha da belirginleşmektedir. Bu açıdan, AB'nin dijital alandaki mevzuatlardaki çapraz-atıflar sebebiyle AB pazarına mal ve hizmet satışı için bütüncül bir uyum kaçınılmaz hale gelmektedir.

CRA, doğrudan dijital unsurlu ürünün üreticisi, ithalatçısı ve dağıtıcısına uygulanıyor olsa da yazılım ve donanım tedarik zincirine yönelik getirdiği kurallar ile veri işleme sistemlerine yönelik getirdiği kurallar sebebiyle dolaylı olarak üçüncü ülkedeki taraflara da uygulanmaktadır. Dolayısıyla, Türkiye'deki bir yazılım veya donanım geliştiricisi şirket, doğrudan AB pazarına yönelik faaliyette bulunmuyor olsa da geliştirdiği donanım veya yazılım CRA'ya tabi bir üretici, ithalatçı veya dağıtıcı tarafından kullanılıyorsa, CRA kurallarıyla muhatap olacaktır.

İlgili bölümde incelendiği üzere Avrupa Birliği, üçüncü bir ülkenin teknik gelişmişlik düzeyini ve uygunluk değerlendirmesine ilişkin yaklaşımını dikkate alarak, uluslararası ticareti teşvik etmek ve kolaylaştırmak amacıyla, Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın 218. maddesi uyarınca üçüncü ülkelerle karşılıklı tanıma anlaşmaları akdetme yetkisini haizdir.

Türkiye'nin AB ile arasındaki Gümrük Birliği anlaşmasının bir neticesi olarak bu karşılıklı tanıma sürecinden muaftır. Türkiye, bu açıdan üçüncü ülkelere karşı avantajlı durumdadır. Bu durum, Türkiye'nin üçüncü ülkelerle olan ilişkisini de olumlu etkileyecektir. Şöyle ki, siber güvenlik alanında hem ürünler hem de insan kaynağı açısından ciddi açıklar vardır. Türkiye, AB pazarına doğrudan girmek isteyen üçüncü ülkelerdeki siber güvenlik ürün geliştiricilerini ülkeye gelmesini teşvik ederek siber güvenlik ekosistemini zenginleştirmesi mümkün olacaktır.

[223] Anayasa Mahkemesi, E. 2017/16 K. 2019/64 K.T. 24.07.2019.

Bu şekilde Türkiye'nin bir siber güvenlik açısından köprü haline gelmesi pekâlâ mümkündür. Bilhassa, Türkiye'nin AB aday ülkesi olması ve mevzuatını önemli ölçüde AB ile uyumlu hale getirmesi, bu tür bir yakınsama içerisinde olmayan üçüncü ülkeler için cezbedici nitelikte olacaktır. Türkiye'nin CRA uyumuna ilişkin tecrübesi önemli bir dijital diplomasi konusu haline getirilebilecektir.

Öte yandan, siber güvenliğe yönelik kaynakların kısıtlı ve maliyetli olması sebebiyle, Türk şirketleri AB'ye muhtelif donanım ve yazılım desteği sunmaktadır. Türk şirketlerinin AB pazarına mal ve hizmet sunumunu devam ettirebilmesi için CRA uyumluluğu önemli bir zorunluluktur.

Keza siber güvenlik alanında kapsamlı düzenleme yapan, detaylı dökümantasyon gereklilikleri olan, siber açık ve ihlal bildirimi talep eden tek düzenleme CRA değildir. Japonya, Çin, Brezilya gibi ülkeler genel siber güvenlik sertifikasyon kuralları getirirken ABD yazılım tedarik zincirine ilişkin şeffaflık kuralları getirmektedir.[224] Brüksel etkisi farklı coğrafyalarda görülmektedir.

Kaldı ki, belirli sektörlerde siber güvenlik konusu uluslararası düzenlemelere konu edilebilmektedir. En önemli örnek bu bağlamda otomotiv sektörüdür. Otomotiv sektöründe en önemli iki siber güvenlik düzenlemesi Birleşmiş Milletler ("BM") tarafından düzenlenmektedir. BM'nin 155 ve 156 numaralı kararları, araçlarda kullanılan yazılımların geliştirilmesi, güncellenmesi ve siber güvenlik ile siber güvenlik yönetim sistemlerinin kontrolüne ilişkin kapsamlı kurallar getirmektedir.[225]

CRA, bu açıdan atipik bir düzenleme niteliğinde değildir. Siber güvenliğe ilişkin düzenlemelerde önemli ölçüde benzerlikler bulunmaktadır. CRA'ya uyum bu açıdan farklı pazarlara giriş açısından da kolaylıklar sağlayacaktır.

CRA'nın kapsadığı kritik ve önemli nitelikte olmayan dijital unsurlu ürünlerde uygunluk denetimi özdenetim (*self-assessment*) yöntemiyle gerçekleştiği dikkate alındığında CRA kendine özgü bir siber güvenlik kültürü oluşturacaktır. Özdenetime tabi olacak ürünlerin dijital unsurlu ürünlerin %90'ını oluşturacağı öngörülmektedir. Bu açıdan bakıldığında CRA uyumu Türk şirketleri için aşırı külfetli ve yüksek maliyetli bir süreç olmayacaktır. AB'nin yaptığı etki analizinin sonuçları dikkate alındığında CRA'ya uyum maliyeti karşısında önemli kazanımlar elde edilmektedir. Bu bağlamda maliyet açısından en çok etkilenen KOBİ'lerin özel olarak desteklenmesi önem kazanmaktadır.

[224] Bkz. Executive Order on Improving the Nation's Cybersecurity https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[225] Bkz. UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system; UN Regulation No. 156 – Software update and software update management system.

XXVI. Değerlendirmeler

CRA'nın uygulanması için donanım ve yazılımın (I) AB iç pazarına yönelik arzı ve (II) herhangi bir veri bağlantısı unsuru içermesi gerekmektedir. Önemle vurgulamak gerekir ki, CRA'da NIS 2 gibi kişi bakımından uygulama açısından istisna yoktur. CRA, sadece özel sektörü değil kamu ihale pazarını da doğrudan etkilemektedir. Veri işleme bağlamında uzaktaki bulut bilişim altyapısı da kapsama girmektedir. Keza, NIS 2 Direktifi kapsamına giren tüm kuruluşlar için de CRA asgari siber güvenlik referansı haline gelmektedir.

CRA, AB pazarına sunulan dijital unsurlu ürünlerin daha az güvenlik açığına sahip olmasını ve üreticilerin bir ürünün yaşam döngüsü boyunca siber güvenlikten sorumlu kalmasını, donanım ve yazılım ürünlerinin güvenliği konusunda şeffaflığın artırılmasını ve iş kullanıcılarına ve tüketicilere daha iyi koruma ile fayda sağlamayı amaçlamaktadır.

CRA ile birlikte dijital unsurlu ürünlerin siber güvenliğine ilişkin yeni bir dönem başlayacaktır. Bir üretici, sadece kendi geliştirdiği donanım veya yazılım kısmı için değil üçüncü taraflara ait bileşenler için de yükümlülükler altına girmektedir.

CRA, dijital unsurlu ürün bir kez AB pazarına sunulduysa en az 5 yıllık süreç boyunca güvenlik bağlamında yükümlük getirmektedir. Hem piyasaya girişte hem de piyasadan çıkışta kurallar getirmektedir. İthalatçı ve dağıtıcıya yönelik yükümlülükler ile üçüncü taraf bileşen geliştiricilere ilişkin yükümlülükler dikkate alındığında kapsamlı CRA bir eko sistem kurmaktadır. Bu ekosistemde herkes müstakil şekilde yetkili makamlarla bilhassa piyasa gözetimi ve denetimi makamlarıyla zorunlu iletişim ve bilgi paylaşım yükümlülüğü altına girmektedir.

CRA, dijital unsurlu ürünlerle ilgili özetle şu yükümlülükleri getirmektedir:

- Ürünler, bilinen herhangi bir istismar edilebilir güvenlik açığı olmadan piyasaya arz edilmelidir.
- Ürünler erişim kontrol mekanizmalarına sahip olmalıdır.
- Ürünler kişisel veri koruması sağlamalıdır.
- Ürünler siber saldırılara karşı dayanıklı olmalıdır.
- Ürünler güvenlik güncellemelerinin (otomatik) dağıtımını içermelidir.
- Ürünler gerekli bilgileri ve talimatları içerecek şekilde piyasaya arz edilmelidir.

Süreçlerle ilgili olarak özetle şu gerekliliklerin yerine getirilmesi gerekmektedir:

- Ürünle ilgili siber güvenlik risklerinin belirlenmesi ve belgelenmesi
- Bir yazılım içerik listesinin (SBOM) muhafaza edilmesi

- Bir ürünün beklenen kullanım ömrünü kapsayan önceden tanımlanmış bir destek süresi boyunca güvenlik açıklarının (güncellemeler dahil) etkin bir şekilde ele alınması
- Yamanmış güvenlik açıkları hakkındaki bilgilerin kamuya açıklanması
- Üçüncü tarafların kullanabileceği bir güvenlik açığı raporlama mekanizmasının oluşturulması
- Güvenlik değerlendirmeleri ve testleri gerçekleştirmesi
- Ürünleri uygun şekilde geri çağrılması
- Yetkili makamları (24 saat içinde) ve kullanıcıları güvenlik olayları hakkında bilgilendirilmesi

CRA'nın Türkiye'ye farklı açılardan etkisi vardır:

(1) AB'ye satılan dijital unsurlu ürünler açısından Türkiye'ye doğrudan etkisi vardır.

(2) Yazılım ve donanım tedarik zinciri içerisinde AB paydaşları bulunan ürünler açısından Türkiye'ye dolaylı etkisi vardır.

(3) Brüksel etkisi ve küresel rekabette güven unsuru sebebiyle Türkiye'ye genel olarak örnek teşkil etmektedir. Yeni pazarlar için de önemli bir kalite güvencesi oluşturmaktadır.

(4) Siber güvenlik ekosistemini güçlendirmesi ve hesap verebilirlik kalitesinin artırılması sebebiyle AB sürecinden bağımsız olarak Türkiye için fırsatlar barındırmaktadır. Temel hak ve hürriyetleri daha güvenceli hale getirmeye katkı sunmaktadır.

(5) Türkiye, gümrük birliği sebebiyle AB pazarına açılmak isteyen üçüncü ülke hizmet sağlayıcılar için de önemli bir çekim merkezi olacaktır.

(6) Hesap verebilirlik kalitesinin artırılması açısından fırsatlar sunmaktadır.

Siber güvenlik temelli dönüşüm çok boyutlu bir süreçtir. Mevzuat bu sürecin sadece bir parçasıdır. Siber güvenliğin temini için bir siber güvenlik ekosistemi ve kültürü oluşturulmalıdır.

CRA temel çerçeveyi çizmektedir. Teknik gerekliliklere ilişkin olarak Avrupa Komisyonu yetki devrine dayalı olarak muhtelif düzenleme yapacaktır. Türkiye için de ilkeleri belirleyen ve aktörlerin sorumluluklarını ortaya koyan temel bir çerçeve hazırlanmalı, teknik hususlar ikincil düzenlemelere bırakılmalıdır. Diğer bir deyişle, ilkeler temel, teknik kurallar kazuistik şekilde ele alınmalıdır.

Sonuç

Dijital dönüşüm çağında hem ekonomik hem hukuki yapının en önemli gündem maddelerinden biri haline gelen "veri", günümüzde giderek artan bir stratejik öneme sahip olmakla birlikte, birçok riski de barındırmaktadır. Veri hukuku, ürün sorumluluğu hukuku ve siber güvenlik hukuku ekseninde Avrupa Birliği'nin (AB) son yıllarda yapmış olduğu düzenlemeler, bu stratejik yaklaşımın en somut göstergelerinden biri olarak görülmektedir. Özellikle "Avrupa Veri Stratejisi Belgesi" ile birlikte gündeme gelen ve devamında hayata geçirilen Veri Yönetişimi Yasası (Data Governance Act), Veri Yasası (Data Act), Ürün Sorumluluğu Direktifi'nde yapılan yenilikler ve Siber Dayanıklılık Yasası (Cyber Resilience Act), AB üyesi olmayan, fakat AB pazarında faaliyet gösteren ya da faaliyet göstermeyi amaçlayan ülkeler açısından da büyük önem taşımaktadır. Zira bu düzenlemeler, sadece Birlik iç hukukunu değil, aynı zamanda uluslararası ticaret ilişkilerini ve hukukun küresel ölçekteki dönüşümünü derinden etkilemektedir. Türkiye gibi, Gümrük Birliği çerçevesinde AB ile uzun zamandır ticari entegrasyona sahip bir ülkenin, bu düzenlemelere kayıtsız kalması söz konusu olmayacağı gibi, Türkiye'deki kurumların ve özel teşebbüslerin söz konusu düzenlemeleri incelemesi ve mevcut olan hukuki düzenlemeleri bu çerçevede gözden geçirmesi; hem ekonomik fırsatlar yakalamak hem de muhtemel yaptırımlardan kaçınmak adına önem arz etmektedir.

Öncelikle veri hukuku bağlamında, AB'nin kişisel verilerin korunmasındaki güçlü hukuki çerçevesi artık neredeyse küresel bir standart hâline gelmiştir. Ancak son yıllarda, verinin ekonomik değeri ve ticari kullanımı açısından yeni bir paradigma geliştirilmiştir. Buna göre veri, yalnızca korunması gereken bir varlık olmaktan çıkıp, "paylaşımcı" ve "ekonomik değer yaratıcı" bir perspektifle ele alınmaya başlamıştır. Ancak verinin paylaşımı, aynı zamanda fikrî ve sınai haklar, ticari sırlar gibi halihazırda korunan menfaatler açısından da sorunlara sebebiyet verdiği için bu çatışan menfaatler arasında bir denge kurulmaya çalışılmaktadır. Veri Yönetişimi Yasası ve Veri Yasası, bu mantığa hizmet etmek üzere düzenlenmiş; bir yandan AB'nin küresel rekabet gücünü artırırken, diğer yandan kullanıcı ve tüketicilerin haklarını koruyan bir yaklaşım benimsemeye çalışmıştır.

Burada dikkat çekilmesi gereken birinci husus, "bağlantılı ürünler" ve "bağlantılı hizmetler" kavramlarının artık çok daha somut yükümlülük ve haklar doğurmasıdır. Birlik hukukunda öngörülen çerçeve içerisinde Nesnelerin İnterneti (IoT) olarak nitelendirilen cihazlar, sensörler ve yazılımlar, veri üretimi ve paylaşımı noktasında temel altyapıyı oluşturmaktadır. Örneğin, bir otomobil üreticisi tarafından tasarlanan otonom araç; içindeki sensörleri ve yapay zekâ sistemlerini kullanarak sürüş esnasında çok sayıda veri toplar. Bu veriler, aracın donanımına gömülü yazılım ile kullanıcı, üretici ve

hatta üçüncü taraflar (örneğin bakım veya telematik hizmeti sunan firmalar) arasında paylaşılabilir. Veri Yasası, bu bağlantılı cihazlar tarafından üretilen verilerin kime ait olduğu, hangi koşullar altında paylaşılması gerektiği ve bu verilerin ekonomik değerinden kimlerin yararlanabileceği konusunda yeni düzenlemeler getirmektedir. Buna göre, AB sınırları içinde piyasaya sürülen bir bağlantılı ürün veya ilgili hizmet, kullanıcının talebi hâlinde elde edilen verileri, haksız rekabeti ve tekelleşmeyi engelleyici biçimde paylaşmak zorundadır. İşte bu yaklaşım, büyük teknoloji şirketlerinin elinde yoğunlaşan veri tekeline bir cevap olarak görülmekte ve KOBİ'lere, yeni girişimcilere daha eşit şartlarda inovasyon fırsatı sunmayı amaçlamaktadır.

Türkiye'deki şirketler için bu durum, hem fırsat hem de riskler barındırmaktadır. Zira AB pazarına mal veya hizmet ihraç eden Türk firmalarının, söz konusu yasal düzenlemelerde belirlenen veri paylaşım ilkelerine uygun davranmaları beklenmektedir. Bu yükümlülükler arasında veriye erişim taleplerine cevap verme, kullanıcıların haklarını gözetme ve veri işleme hizmetlerinde birlikte çalışabilirlik (interoperability) gibi oldukça teknik ve operasyonel noktalar da yer almaktadır. Yükümlülüklere uyulmaması durumunda AB ülkelerinde ciddi yaptırımlar ve ticari kısıtlamalarla karşılaşmak mümkündür. Ancak diğer taraftan, AB'nin veri stratejisi çerçevesinde oluşturduğu ortak veri alanları ve öngörülen mali teşvikler, AR-GE çalışmalarında ve yeni ürün geliştirmede Türk firmalarına da katkı sağlayabilir. Kapsamlı veri setlerine erişim ve belli ölçülerde kamuya açık veri kaynaklarından yararlanma fırsatı, yenilikçi uygulamalar geliştirmeyi mümkün kılmaktadır. Özellikle yapay zekâ ve ileri analitik teknolojilerinin günden güne yaygınlaştığı bir ortamda, veri zenginliği en önemli girdilerden biridir. Dolayısıyla AB düzenlemeleriyle uyum sağlamak, uzun vadede rekabet avantajı da sağlayabilir.

İkinci önemli husus, ürün sorumluluğunun giderek yazılım ve veri kaynaklı hataları da kapsamına alacak şekilde genişlemesidir. Geleneksel ürün sorumluluğu rejimlerinde, bir ürünün "kusurlu" sayılması, genellikle fiziksel tasarımdan veya üretim hatasından kaynaklanırdı. Oysa modern dünyada, bir ürünün kusuru yazılımdan kaynaklanabilir veya ürüne entegre bir yapay zekâ modülü yanlış veri işlediği için ciddi hatalara neden olabilir. Örneğin, bir endüstriyel robot kolunun kontrol yazılımı, senkronizasyonu doğru yapamazsa üretim tesisinde kazalara yol açabilir. AB, bu gerçeği dikkate alarak Ürün Sorumluluğu Direktifi'nde kapsamlı reformlara gitmiş ve yazılımın da ürün kavramına dahil edilebileceğini açıkça vurgulamıştır. Böylece, üreticiler sadece fiziki parçaların kalitesinden değil, dijital unsurların güvenlik ve doğruluğundan da sorumlu olacaktır. Türkiye'de de 7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanunu, 6502 sayılı Tüketicinin Korunması Hakkında Kanun ve 6098 sayılı Türk Borçlar Kanunu gibi yasalarda yer alan sorumluluk düzenlemelerinin, bu yeni

gerçekliğe cevap verecek şekilde güncellenmesi gerekebilir. Aksi takdirde, AB pazarına ürün ihraç eden şirketler, yurtiçinde sorunsuz görünen bir üründen dolayı AB'de mali sorumlulukla karşı karşıya kalabilecektir.

Üçüncü bir husus, siber güvenlik konusunun artık sadece teknik bir mesele değil, aynı zamanda hukuki bir sorumluluk ve yaptırım rejimiyle de desteklenmesidir. AB'nin NIS (Ağ ve Bilgi Sistemleri) Direktifi, üye devletler arasında temel hizmet operatörlerinin ve dijital hizmet sağlayıcılarının asgari güvenlik standartlarına uyumunu öngörmektedir. NIS 2 Direktifi ise bu standartları genişleterek daha fazla sektörü ve kuruluşu kapsam altına almış; "kritik altyapı" kavramını enerji, ulaşım, sağlık, bankacılık ve diğer alanları da içine alacak biçimde genişletmiştir. Siber Dayanıklılık Yasası (Cyber Resilience Act) ise doğrudan "dijital unsurlu ürünleri" hedef alarak, tasarımdan piyasaya sürmeye kadar her aşamada siber güvenlik tedbirlerinin alınmasını şart koşmuştur. Bu kapsamda üreticiler, dağıtıcılar ve ithalatçılar, sadece ürünün anlık güvenliğinden değil, kullanımdaki tüm güncellemelerinden ve teknik açıklarının yamalanmasından da sorumlu tutulmaktadır. Ayrıca güvenlik açığı ortaya çıktığında, tüketicileri ve ilgili otoriteleri derhal bilgilendirmek, düzeltici eylemlere başvurmak ve gerekiyorsa ürünü geri çağırmak gibi yükümlülükler söz konusudur.

Türkiye'de siber güvenlik alanında bazı kurumlar ve çerçeve düzenlemeler vardır; ancak AB'nin siber güvenlik yaklaşımı, gerek kapsam gerekse yaptırım mekanizmaları bakımından çok daha ileri düzeydedir. Eğer Türk yazılım ve donanım üreticileri, AB'de piyasaya ürün sunmak istiyorsa, bu kurallara tam uyum sağlamaları şarttır. Bu uyum, sadece cezai müeyyidelerden kaçınmak adına değil, aynı zamanda Türkiye'nin kendi dijital ekosistemini güçlendirmek için de önem arz etmektedir. Zira siber saldırıların küresel boyutta artış gösterdiği, her gün yeni saldırı vektörlerinin ortaya çıktığı günümüzde, yerel firmaların da güvenlik açıklarını kapatmaları ve sistemlerini daha dirençli hâle getirmeleri elzemdir. AB ile entegre bir siber güvenlik standardı benimsemek, orta ve uzun vadede işletmelerin uluslararası arenada daha itibarlı görülmesine yardımcı olabilecektir.

Buradan hareketle, Türkiye'nin AB veri hukuku, ürün sorumluluğu ve siber güvenlik düzenlemeleri karşısında benimsemesi gereken strateji "aşırı regülasyon" riski ile "rekabet avantajı" arasında ince bir denge kurmayı gerektirir. Her şeyden önce, AB'nin veri hukuku ve siber güvenlik düzenlemeleri oldukça ayrıntılıdır ve mikro işletmelerden çokuluslu şirketlere kadar geniş bir etki alanı mevcuttur. Özellikle KOBİ'ler için, Veri Yasası gibi düzenlemelerin getirdiği teknik gereklilikleri yerine getirmek ya da siber dayanıklılık standardını sağlamak, ciddi maliyetler yaratabilir. Bu noktada, bir yandan Veri Yasası'nda olduğu gibi KOBİ'leri yükümlülüklerden muaf tutmak, diğer yandan Türkiye'deki ilgili

bakanlıklar ve düzenleyici kurumların, KOBİ'lere yönelik rehberlik, eğitim ve finansal teşvik programları tasarlamaları düşünülebilecektir. Örneğin, veri paylaşım altyapısı kuracak işletmelerin desteklenmesi ya da bulut bilişim standartlarını yakalamak isteyen firmalar için hibeler verilmesi, girişimcilerin ağır regülasyon yükünü hafifletebilecektir.

Öte yandan, aşırı regülasyon kaygıları da dikkate alınarak, Türkiye'nin kendi dijital ekonomik öncelikleriyle AB düzenlemeleri arasındaki "kısmi" veya "dengeli" bir uyum politikası da düşünülebilecektir. Özellikle yerel veri merkezlerinin kurulmasını teşvik eden ve veri egemenliği konusunda hassasiyet gösterip "güvenli liman" veya "bulut sertifikasyon" sistemleri gibi mekanizmalarla AB standartlarına yakın çözümler oluşturabilecektir. Böylece, hem AB'deki düzenlemelerden ayrışılmayacak, hem de ulusal menfaatler dikkate alınmış olacaktır. Yine de AB ile "uyum anlaşmaları" veya "çapraz tanıma" esasına dayalı protokollerin geliştirilmesi, ihracatın ve dijital hizmet tedarikinin aksamaması açısından büyük önem taşımaktadır.

Raporda ele alınan bir başka boyut da, kamu sektörünün, verinin yeniden kullanımını sağlamak üzere nasıl bir hukuki çerçeve geliştirebileceği meselesidir. Veri Yönetişimi Yasası, kamunun elindeki veri setlerinin yalnızca gizlilik kaygıları ekseninde saklanmaması; kamu menfaati doğrultusunda ve belirli kurallara riayet etmek suretiyle inovasyon ekosisteminin kullanımına açılması gerektiğini savunmaktadır. Özellikle sağlık, ulaşım, enerji ve çevre gibi alanlarda kamu kurumları muazzam miktarda veri toplamaktadır; bunların belirli koşullarda özel sektörle veya araştırma kurumlarıyla paylaşılması, toplumsal faydayı artıracak buluşların ve çözümlerin geliştirilebilmesini sağlayacaktır. Türkiye'de de benzer inisiyatifler görülmekle birlikte, kurumsal kapasitenin geliştirilmesi ve veri paylaşımının standartlarının netleştirilmesi konusunda adımlar atılması isabetli olarak değerlendirilmektedir. Aksi hâlde, verinin potansiyeli yeterince değerlendirilemeyecek, mahremiyet ile kamu yararı arasında dengenin kurulması zorlaşacaktır.

Geniş perspektiften bakıldığında, AB'deki bu düzenleyici çerçeve, verinin küresel ölçekte nasıl yönetileceğine dair "Avrupa modelini" yansıtmaktadır. Bu model, ABD merkezli büyük teknoloji şirketlerinin veriye hükmetme yaklaşımından farklı olduğu gibi, Çin'in katı devlet kontrolünü öngören veri politikalarından da farklılaşmaktadır. AB, hem bireylerin temel haklarını hem de serbest rekabet ve inovasyonu korumaya çalışmaktadır. Bununla birlikte bu dengenin ne kadar isabetli kurulduğu da tartışma konusudur. Her halükarda Birlik pazarında faaliyet göstermek isteyen Türk teşebbüslerinin bu düzenlemelere uyum sağlaması stratejik bir öneme sahiptir.

Raporda değinilen ve geleceğe yönelik strateji önerilerinden biri de, Türkiye'nin bu yeni dünya düzenine hazırlanmak üzere kurumsal kapasitesini güçlendirmesi gerektiğidir. Siber güvenlik bağlamında, ulusal çapta bir koordinasyon mekanizması oluşturularak hem kamu kurumları hem de özel sektör arasındaki işbirliği artırılabilir. Böylece, NIS 2 Direktifi ve Siber Dayanıklılık Yasası türü düzenlemelere benzer standartlar, yerel düzeyde de benimsenmiş olur. Bu, AB'ye ihracat yapan şirketler için bir kolaylık sağlayacağı gibi, Türkiye iç pazarında faaliyet gösteren firmaların da siber saldırılara karşı daha korunaklı hâle gelmesini mümkün kılar. Veri hukuku bağlamında ise, Kişisel Verileri Koruma Kurumu (KVKK) benzeri bağımsız otoriteler ya da halihazırda faaliyet gösteren kamu kurumları, kişisel olmayan verilerin paylaşımı ve ticari kullanımını gözeten ek çerçeveler oluşturabilecektir. Veri paylaşımının rekabeti bozmayacak, haksız sözleşme şartları doğurmayacak şekilde gerçekleşmesi için denetleyici kurumlar harekete geçebilecektir.

Ayrıca, AB düzenlemeleri kapsamında belirtilen "istisnai durumlarda kamu yararının gerektirdiği ölçüde özel sektörden veri talep edilebilmesi" uygulaması, COVID-19 gibi kriz dönemlerinde verinin ne kadar kritik olduğunu gözler önüne sermiştir. Salgın sürecinde hastalık takip sistemleri, mobil uygulamalar ve platformlar aracılığıyla toplanan veriler, salgının yayılımını kontrol altına almak açısından büyük önem taşımıştır. AB düzenlemeleri, bu tür olağanüstü hâllerde kamu otoritesinin özel sektörden veri talep edebilmesini, ancak talebin gerekliliği ve ölçülülüğü ilkeleriyle sınırlı kalmasını benimsemektedir. Türkiye'de de benzer hâller için yasal çerçevelerin belirlenmesi; kamunun ihtiyaç duyduğu verileri özel sektörden hangi koşullarda talep edebileceğini tanımlamak bakımından faydalı olacaktır.

Bu noktada, veri egemenliği meselesi de önem kazanmaktadır. AB, verilerin AB sınırları dışında işlenmesi veya depolanması konusunda üçüncü ülke mevzuatının AB standartlarına uygunluğunu esas almaktadır. Örneğin, Türkiye'deki bir kamu kurumu, AB içinde tutulan verileri talep etmek istediğinde, AB düzenlemeleri gereği belirli prosedürleri yerine getirmek veya ilgili verilerin aktarımına yönelik uluslararası anlaşmalara dayanmak zorunda kalabilir. Dolayısıyla, Türkiye'nin siber güvenlik, kişisel verilerin koruması ve kişisel olmayan verinin işlenmesi konularındaki mevzuatı, AB seviyesine ne kadar yaklaşırsa, veri akışları da o kadar sorunsuz gerçekleşecektir. Aksi takdirde, veri transferinin engellenmesi ya da sıkı denetime tabi tutulması gibi durumlar, ekonomik ilişkileri ve ticari faaliyetleri sekteye uğratabilecektir.

Tüm bu unsurlar birlikte değerlendirildiğinde, AB'nin veri hukuku, ürün sorumluluğu ve siber güvenlik düzenlemelerinin Türkiye'ye etkisi yalnızca "uyum maliyeti" odağında ele alınmamalıdır. Orta ve uzun

vadede, bu düzenlemeler Türkiye'nin dijitalleşme sürecinde kurumsal ve teknolojik altyapısını güçlendirmesine katkı sağlayabilir. Özellikle ileri teknoloji ürün ihracatında, veri güvenliği ve birlikte çalışabilirlik kriterlerini karşılayan sistemler, küresel piyasalarda rekabet üstünlüğü elde edebilir. Örneğin, bir akıllı ev sistemini tasarlayan Türk firması, hem veri paylaşımında adil ilkeleri benimseyen hem de siber güvenlik standartlarını sağlayan bir çözüme imza attığında, AB pazarına rahatlıkla erişebilir ve büyük teknoloji şirketleriyle ortaklıklar kurabilir. Bu, ülke ekonomisine de katma değer yaratacak bir gelişme olarak değerlendirilebilecektir. Ancak bunun için belirtildiği üzere elde edilecek olan kazancın uyum maliyetlerinin çok daha üstünde olması gerekecektir.

Öte yandan, raporun belirgin kıldığı bir gerçek de, "dijital okuryazarlık" seviyesinin önemidir. Zira teşebbüsler, verinin hangi koşullarda paylaşılması gerektiğini, hangi durumlarda kamu kuruluşlarına veri sağlama zorunluluğu olduğunu, hangi siber güvenlik açıklarının bildiriminin zorunlu tutulduğunu yeterince bilmezlerse, büyük cezalarla ya da telafisi güç zararlarla karşı karşıya kalabilecektir. Bu nedenle, sektörel bazda eğitimler, üniversite-sanayi işbirlikleri ve meslek odalarının düzenleyeceği seminerler yoluyla bilgi eksikliği giderilmelidir. Aynı zamanda yazılım mühendisleri, uyum uzmanları ve veri koruma görevlileri (DPO'lar) gibi profesyonellerin yetiştirilmesi, Türkiye'nin dijital dönüşüm yolculuğunda kritik bir ihtiyaçtır.

Raporda yer alan "riskler ve fırsatlar" bölümü, Türkiye'deki mevzuata uyum senaryolarını tartışarak, "tam uyum" ve "kısmi uyum" seçeneklerini ele almıştır. Tam uyum senaryosunda, AB'nin ilgili tüm düzenlemelerinin Türk hukuk sistemine entegre edilmesi, ithalat ve ihracat süreçlerinde ortak bir zeminin oluşmasını sağlayabilir. Fakat tam uyum, özellikle yerel işletmeler açısından yüksek maliyetli olabilir. Kısmi uyum senaryosu ise, öncelik sırasına göre bazı alanlarda AB standartlarının yakalanmasını, diğer alanlarda ise daha esnek bir çerçevenin sürdürülmesini öngörür. Bu yaklaşım, kısa vadede işletmelerin uyum maliyetlerini düşürse de uzun vadede rekabet dezavantajlarına yol açabilir. En nihayetinde, küresel dijital ekosisteme entegre olmak isteyen bir ülkenin, "ayrıksı" regülasyonlarla uluslararası ticaret ve yatırım açısından elverişli görünmesi güçtür.

Geleceğe yönelik değerlendirildiğinde, AB'nin dijital dönüşümün regülasyonu konusunda lider roller üstlenmeye devam edeceği açıktır. Veri, siber güvenlik ve yapay zekâ ile ilgili pek çok düzenleme ve direktifin revize edilmesi veya yenilerinin çıkarılması beklenmektedir. Teknoloji çok hızlı değiştiği için, hukukun da bu değişime ayak uydurması gerekmektedir. Bu süreçte, Türkiye gibi AB dışındaki ülkeler, hem kendi ulusal çıkarlarını gözetmek hem de uluslararası ticaretin gerekliliklerini yerine getirmek zorundadır. Dolayısıyla "çok boyutlu" bir strateji geliştirilmesi gerekir.

Sonuç olarak, Türkiye'nin AB düzeyinde yapılan veri hukuku, ürün sorumluluğu ve siber güvenlik düzenlemelerine yaklaşımı, salt bir "uyum" perspektifini değil, aynı zamanda "yenilikçilik" ve "rekabet gücü" boyutlarını da gözetmelidir. Düzenlemelerin getirdiği bazı katı zorunluluklar, özellikle ilk etapta mali külfetler yaratabilir. Ancak bu zorunluluklar, orta ve uzun vadede yerli firmaların küresel piyasalarda güvenilir ve yüksek standartlı ürünler sunabilmesinin yolunu açtığı takdirde kanaatimizce kabul edilebilir nitelikte olacaktır.

Dijitalleşme sürecinin temel dayanağını oluşturan veriyi doğru yönetmek, bu veriyi işleyen ürünlerin sorumluluğunu üstlenmek ve bu ürünleri siber tehditlere karşı dayanıklı hâle getirmek, kaçınılmaz bir gereklilik hâline gelmiştir. Bu nedenledir ki, söz konusu düzenlemeler, Türkiye'de hukuk politikasından endüstriyel strateji planlarına kadar geniş bir yelpazede temel belirleyici unsurlardan biri olmaya adaydır. Veri, "21. yüzyılın petrolü" olarak nitelendirilmeye devam ettiği sürece, veriye dair düzenlemeler de ülkelerin küresel rekabetteki konumunu doğrudan etkileyecektir. Burada hem kamunun hem de özel sektörün yeterli altyapı ve insan kaynağına sahip olması, dijital dönüşüm süreçlerini hızlandıracak, ihracatta ve uluslararası projelerde Türkiye'nin elini güçlendirecektir. Ne var ki, bu dönüşüm sürecinde sadece hukuki metinlerin benimsenmesi yeterli değildir; doğru yönetişim mekanizmalarının hayata geçirilmesi, denetim kapasitesinin oluşturulması ve süreklilik arz eden bir farkındalık çalışması da gereklidir.

Avrupa Birliği'nin veri hukuku, ürün sorumluluğu hukuku ve siber güvenlik hukuku alanındaki düzenlemeleri, Türkiye'ye "dışsal" bir baskı veya "teknik engel" gibi değerlendirilebilecektir. Ancak bu yaklaşım kanaatimizce eksiktir. Bilakis dijital çağın standartlarını belirleyen bu düzenlemeler, Türkiye'nin dijitalleşme sürecini hızlandırması ve böylece uluslararası arenada rekabetçi kalması için önemli bir fırsat olarak da değerlendirilebilecektir. Bu perspektiften bakıldığında, "uyum" süreci aslında "dönüşüm" ve "yatırım" sürecinin de bir parçası olarak değerlendirilebilecektir. Gerçekten de AB'nin veri ve siber güvenlik politikaları bağlamında, Türkiye'nin gerek mevzuat düzeyinde gerekse kurumsal uygulamalarda atacağı adımlar, ülkenin iç piyasasında da dijitalleşmenin kalitesini artırabilir, KOBİ'lerden büyük ölçekli şirketlere kadar tüm aktörlere yeni ufuklar açabilir.

Dolayısıyla bu raporun en önemli bulgularından birisi, dijital dünyada ayakta kalabilmek ve büyümeyi sürdürebilmek için sadece teknoloji geliştirme çabasının yeterli olmadığıdır. Aynı zamanda, verinin korunması, doğru işlenmesi, adil biçimde paylaşılması, güvenlik açıklarının kapatılması ve kullanıcı haklarının korunması gibi çok boyutlu kaygıları içeren hukuki çerçevenin de titizlikle kurgulanması gerekmektedir. Türkiye, bu çerçevede kendi stratejik hedeflerini belirlerken, AB standartlarını sadece

bir “zorunluluk” olarak değil, bir “fırsat” olarak da değerlendirebilir. Uzun dönemde, veri yönetimi ve siber dayanıklılık gibi konularda güçlü bir zemine sahip olmak, hem uluslararası itibar kazanma hem de iç pazarda güven ortamı yaratma açısından belirleyici olacaktır.

Özetle, veri hukuku, ürün sorumluluğu ve siber güvenlik alanlarında Avrupa Birliği düzenlemeleri; şirketlerin, kamu kurumlarının ve tüketicilerin dijital dünya içindeki hak ve yükümlülüklerini güncelleyerek onları daha ileri bir seviyeye taşımaktadır. Türkiye’nin bu düzenlemelerle uyum konusundaki çalışmaları, yalnızca ekonomik veya hukuki bir gereklilik değil, aynı zamanda dijital çağdaki rekabet gücünü koruyabilmek için stratejik bir adımdır. KOBİ’lerden çokuluslu şirketlere kadar geniş bir kesimin bu değişime hazırlanması, örgün eğitim programları, kurumsal yetiştirme programları ve mevzuat düzenlemeleriyle mümkün olacaktır. Mevcut eğilimler, veri ve siber güvenliğin önümüzdeki dönemde çok daha önemli hale geleceğine işaret ettiğinden, bu alana yapılacak her türlü yatırım, Türkiye’yi geleceğin dijital ekonomisinde daha avantajlı konuma yerleştirecektir.