

281

Temmuz 2024

İKV DEĞERLENDİRME NOTU

AB DİJİTAL HİZMETLER YASASI'NA
TÜRKİYE'NİN UYUMU

Sema Nur Yeniıldız
İKV Uzmanı

İKTİSADİ KALKINMA VAKFI



AB Dijital Hizmetler Yasası'na Türkiye'nin Uymu

Sema Nur Yeni yıldız, İKV Uzmanı

Dijital Hizmetler Yasası (DSA), AB'nin dijital stratejisi bağlamında, Birliğin temel hak ve özgürlüklerin korunduğu ve dijital hizmet sağlayıcılarının hesap verebilirliğinin artırıldığı güvenli, öngörülebilir ve güvenilir bir çevrim içi ortam yaratma taahhüdünü AB hukukuna dâhil etmektedir. AB, DSA ile üye ülkeler arasında dijital düzenleme çerçevelerini modernize etmeyi ve azami şekilde uyumlu olmasını amaçlamaktadır. AB'ye aday ve potansiyel aday ülkelerin DSA'ya uyumu ise zorunlu olmasa da bu ülkelerde DSA'nın geliştirilmesi, uygulanması ve yürütülmesi hem çevrim içi hizmetlerinde şeffaflık ve güvenilirliği desteklemesi açısından hem de AB'ye katılım (mevzuata uyum) bağlamında oldukça önemlidir. Hâlihazırda, temel hak ve özgürlüklerin (özellikle bilgi edinme ve ifade özgürlüğünün) ve hukukun üstünlüğünün korunması için DSA'yı hayati bir gereklilik olarak gören Avrupa Komisyonu, aday ve potansiyel ülkelerde DSA'nın hazırlanması ve uygulanması için iş birliğine açık olduğunu belirtmiştir.

Aday ve potansiyel aday ülkelerin, AB'nin dijital stratejisiyle paradigma farklılıkları yaşamaması için yatay bir düzenleme olan DSA'ya ve gerekli düzenlemelere uyum sağlaması gerekmektedir. Bu ülkelerin sağlamlık, emniyet, hesap verilebilir ve şeffaflık zemininde olmayan dijital stratejilere sahip olması, AB açısından genişleme politikası altında katılımı güçlendirmenin önüne engel olabilir veya stratejik kalibrasyonun olumsuz etkilenebileceği söylenebilir. Bu bağlamda AB mevzuatına uyum açısından Türkiye'nin de dijital hizmet sağlayıcılarına, çok büyük çevrim içi platform ve arama motorlarına yönelik "hesap verebilirlik ve şeffaflık sağlayan, çevrim içi kullanıcı ve sivil toplumu güçlendiren, bağımsız düzenleyicileri belirleyerek rolünü tanımlayan, temel hakları koruyan, yasa dışı içeriğin yayılması, sivil söylem ve seçim süreçleri üzerindeki olumsuz etkileri önleyen, çevrim içi platformlardan kaynaklanan sistemik risklerin değerlendirilmesini ve azaltılmasını sağlayan hükümlere odaklanan, DSA'nın yasal bağlamına, hedeflerine, temel ilkelerine, uygulama yapısına ve yükümlülük mimarisine azami şekilde uyan" bir dijital hizmet düzenlemesi oluşturması gerekmektedir. Türkiye-AB Gümrük Birliği'nin modernizasyonu ve hizmet ticaretinin serbestleştirilmesi hedefleri kapsamında da dijital hizmetlerin düzenlenmesi konusu ön plana çıkmaktadır. Ancak DSA'nın doğasından kaynaklanan karmaşıklık ve üye ülkelerin bile DSA'ya tam uyumda zorluklarla karşılaşması göz önüne alındığında Türkiye'nin DSA'nın operasyonel hazırlığında üye ülkelere ve Komisyondan rehberlik alması -özellikle kapasite yaratmada- oldukça önemlidir. DSA ile ilgili Komisyon birimleri, uzmanları ve sivil toplum kuruluşlarından temsilciler, DSA'nın geliştirilmesi ve uygulanmasına ilişkin deneyim ve bilgilerini çeşitli perspektiflerden ve farklı kanallarla paylaşmaya hazırdır. Türkiye'nin özellikle kurumlar arası koordinasyon ve iş birliği üzerine odaklanarak yasal ve kurumsal çerçeve konusunda tavsiyeler alması gerekmektedir. Ayrıca Dijital Hizmet Koordinatörü'nün atanması, kurulması ve faaliyetleri de dâhil olmak üzere DSA'nın ulusal düzeyde uygulanması sırasında karşılaşılan zorluklarla ilgili deneyim aktarımına ihtiyacı vardır.

Dijital Platformlara İlişkin AB Perspektifi

21'inci yüzyılın en önemli yeniliklerinden biri olarak hayatımıza giren dijital platformlar, kontrolü güç, yeni bir evren oluşturmakta ve sunduğu hizmetlerle günlük hayata giderek entegre olmaktadır.¹ Sosyal medya ağlarından e-ticaret sitelerine, çevrim içi ödeme sistemlerinden eğitim ve sağlık hizmetlerine kadar geniş bir yelpazede hizmet sunarak toplumsal ve ekonomik yapıyı dönüştüren bu platformlar, küreselleşmenin de tam istediği gibi kişilerin ve işletmelerin dünyanın dört bir yanına hızlı ve kolay bir şekilde erişim sağlanmasının önünü açmaktadır. Bilgi ve eğitimin yaygın ve erişebilir olması gibi faydaların yanı sıra operasyonel verimliliği de sağlaması gibi avantajları bulunan bu platformların, kişilerden dünya ile bağlantıda olan tüm kurumlara kadar etkisi bulunmaktadır. Ancak doğası gereği dijital platformların altyapısının oldukça karmaşık ve birbiriyle bağlantılı birçok sistemden oluşması, çok sayıda kullanıcının verisine ev sahipliği yapması (kişisel ve finansal bilgiler gibi veriler), sürekli değişim dinamizminde olması, bilgilerin yanlış veya doğru olmaksızın hızlı yayılmasını sağlaması gibi özelliklerinden dolayı özellikle kişisel verilere karşı siber saldırılara maruz kalmakta, yasa dışı içeriklerin hızlı yayılmasına neden olmakta, dezenformasyonu desteklemekte ve temel hakların baltalanmasına sebep olmaktadır. Bu bağlamda, sınırları net olarak belirlenmemiş ve kuralları yeni yeni oluşturulan dijital ortamı ve bu ortamın başlıca aktörleri olan, bağımsız faaliyetlerde bulunan dijital platformları düzenlemenin önemi giderek artmaktadır.

Ulusal ve uluslararası hukuki çerçeveler, temel hakları (ifade özgürlüğü, özel yaşamın gizliliği gibi) veri gizliliğini sağladığı ve koruduğu, siber güvenlik oluşturduğu, haksız rekabeti engellediği (rekabet hukuku), tüketici haklarını desteklediği için devletlerin dijital platformları düzenleme yetkisi bulunmaktadır. Bu bağlamda devletler, dijital platformların yasalara uymasını sağlamak için gerekli yasal çerçeveyi oluşturmak ve bu çerçeveyi etkin bir şekilde uygulamakla yükümlüdür.

2030 yılına kadar Avrupa'yı insan merkezli, sürdürülebilir ve daha müreffeh bir dijital geleceğe taşımayı hedefleyen AB de oldukça kapsamlı bir dijital stratejiye sahiptir ve Birliğin bu hedeflere ulaşması için çeşitli eylem planları ve yasal altyapıyı oluşturmaya çalışmaktadır.

AB'nin, bu hedeflere hizmet edecek şekilde dijital platformları düzenlemeye dair evrensel yaklaşımı ise şu şekildedir:

- AB vatandaşlarının güvenliğinin sağlanması ve ifade özgürlüğünün geliştirilmesi,
- İnovasyonun sağlanması ve desteklenmesi,
- 27 üye ülkeli AB'nin, iç mevzuatının yasal olarak parçalanmasının önlenmesi.

¹Karen Arriaza Ibarra, 2022, "Trends and Perspectives on Digital Platforms and Digital Television in Europe", International Journal of Communication 16(2022), 457-460. Erişim Tarihi: 01.07.2024

Bu bağlamda Avrupa Dijital Stratejisi'nin² bir parçası olarak dijital piyasalardaki büyük çevrim içi platformların dijital alandaki pazar güçlerini denetim altına almayı planlayan Dijital Piyasalar Yasası (*Digital Markets Act- DMA*) ve dijital platformların sorumluluklarını belirleyerek yasa dışı içerik ve ürünlerle mücadele etmenin kurallarını belirleyen Dijital Hizmetler Yasası, (*Digital Services Act- DSA*) Aralık 2020'de Avrupa Komisyonu tarafından önerilmişti.

Dijital Hizmetler Yasası'nın Geçmiş Yasal Çerçevesi

AB'nin DSA öncesinde de dijital hizmetleri düzenleyen yasal altyapısı olsa da dijital dünyada yaşanan hızlı değişim ve bu değişimlerin getirdiği zorluklar ve gereksinimler, çevrim içi platformların artan rolü ve etkisi, mevcut düzenlemelerin yetersizliği ve dijital alanda temel hak ve özgürlüklere yönelik ihlallerin giderek artması nedeniyle AB'de DSA'ya ihtiyaç artmıştır. AB'nin dijital alandaki en önemli ve kapsamlı yasal düzenlemelerinden biri olan DSA, çevrim içi dünyada daha güvenli ve sorumlu bir ortam yaratmayı amaçlayarak 15 yılı aşkın bir süredir yürütülen kapsamlı bir çalışmanın bir sonucu olarak ortaya çıkmıştır. Geçmiş AB düzenlemelerine bakıldığında:

- 2000 E-Ticaret Tüzüğü: Bu tüzük, çevrim içi pazarlarda yasa dışı içerik ve haksız rekabete karşı Tek Pazar'a ilk koruma önlemlerini getirmiştir.³
- 2016 Çevrim İçi Platformlar Tebliği: Bu iletişimde, çevrim içi platformların yasa dışı içerik ve dezenformasyonla mücadeledeki sorumlulukları ele alınmıştır.⁴
- 2017-2018 Yasa Dışı İçerik Çalışması: Bu çalışmada, çevrim içi platformlarda yasa dışı içerikle mücadeledeki boşluklar ve eksiklikler analiz edilmiştir.
- 2020 Dijital Hizmetler Etki Değerlendirmesi: Bu değerlendirmede, DSA'nın temel haklar ve özgürlükler üzerindeki potansiyel etkileri incelenmiştir.

Bu çalışmaların yanı sıra, AB Adalet Divanı'nın (ABAD) içtihatları da DSA'nın şekillenmesinde önemli rol oynamıştır. ABAD'ın kararları, çevrim içi platformların sorumlulukları ve yasa dışı içerikle mücadeledeki yükümlülükleri konusunda önemli rehberlik sağlamıştır.

²The European Commission's Six Priorities 2019- 2024, "A Europe Fit For the Digital Age: Shaping Europe's Digital Future". https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en Erişim Tarihi: 01.07.2024

³Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), 17.07.2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32000L0031> Erişim Tarihi: 01.07.2024

⁴Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM/2016/0288 Final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0288> Erişim Tarihi: 01.07.2024

DSA'nın Yapısı ve Yükümlülüklerine Genel Bir Bakış

Aralık 2020'de Avrupa Komisyonu tarafından önerilen ve Temmuz 2022'de AP ve AB Konseyi tarafından onaylanan DSA, 25 Ağustos 2023 tarihinden itibaren büyük çevrim içi platform ve arama motorları için yürürlüğe girmiştir. 17 Şubat 2024 tarihinden itibaren ise DSA, e-ticaret pazarlarından çevrim içi uygulama mağazalarına, video paylaşım platformlarından ve arama motorlarına kadar AB pazarında hizmetlerini (mal, içerik veya hizmet) sunan tüm çevrim içi hizmet sağlayıcılarını etkilemeye başlamıştır.

Toplumsal kaygılarla mücadele etme iradesiyle oluşturulan DSA'nın uygulama alanı oldukça geniş ve her türlü dijital hizmet için kurallar belirlemektedir. DSA, platformlar için doğrudan geçerli olacak şekilde aşağıdaki yükümlülükleri ve yasakları getirmektedir:

- Yasa dışı içerik ve ürünlerle mücadele: DSA, AB içinde hizmet veren çevrim içi platformun -ana temsilciliği hangi ülkede olursa olsun- Üye Devletlerin herhangi bir yasa dışı içeriği kaldırma talebini değerlendirmesini zorunlu kılmaktadır.
- Kişilere yönelik hedefli reklamlar: DSA'da, herhangi bir çevrim içi platformun 18 yaş altını hedefleyen (özellikle çocukları) veya kişilerin hassas verileri üzerinde hedefleme yapan reklamlar sunması tamamen yasaklanmaktadır.
- Aracılık hizmetlerinin düzenlenmesi: Dijital pazar yerlerinde hizmet sağlayan bir çevrim içi platform, sunduğu tüm ürünlerden sorumlu hâle getirilmektedir. Böylece platformlarda satışa çıkan ürünlerin denetiminin artırılması -özellikle de aracılık hizmeti sağlayanların sunduğu hizmetlerin denetiminin artırılması planlanmaktadır. Kısaca bu hükümlerle, denetimi zor olan bu platformlarda aracılık yapanların yasa dışı ürün ve hizmet sağlamasının önüne geçilmesi öngörülmektedir. Ayrıca DSA, çevrim içi hizmetlerden mağdur olan tüketicilere toplu dava açma hakkı da tanımaktadır.
- Medya çoğulculuğu ve ifade özgürlüğü: DSA ile çevrim içi platform kullanıcılarının hangi kanaldan içerik önerisi alabileceğine dair kendilerinin karar verebilmesi sağlanmaktadır. DSA, bu platformların kullanıcı hesaplarını askıya alma kurallarını da AB standartları ve kriterlerine göre baz alınmasının önünü açıyor. Böylece Meta (*Facebook ve Instagram*), *X* ve *TikTok* benzeri sosyal medya platformlarının, kendi kurallarını ve standartlarını AB ile uyumlu olacak şekilde düzenlemesi gerekmektedir.
- Algoritma şeffaflığı: DSA ile çevrim içi platformlar, kullanıcılarına sahip oldukları algoritma işleyişleriyle ilgili şeffaflığı ve hesap verilebilirliği ortaya koymaları gerekmektedir. Bu doğrultuda çevrim içi platformlar, hangi içerikleri filtrelediklerine ya da önerdiklerine dair kullanıcıları bilgilendirmek zorunda kalmaktadır.
- Ana dilde içerik denetimi: DSA, üye ülkelerde faaliyet gösteren çevrim içi platformların, mevcut resmî dilde yayımlanan tüm içeriklerini denetlemesini gerektirmektedir. Bunun içinde platformlar, bu denetimi yapabilecek yeterli insan gücünü işe almakla yükümlü hâle getirmektedir. Ayrıca çevrim içi platformlarla iletişime geçmek veya bu platformlara şikâyette bulunmak isteyen kullanıcıların ana dilini bilen çalışan bulundurulması gerekmektedir.

- Kullanım koşulları: Çevrim içi hizmet sunanların hepsi, DSA ile verdikleri hizmetlere dair hüküm ve koşulları açık, erişilebilir ve anlaşılır bir dilde sunması zorunludur. Böylece çevrim içi hizmet sağlayıcılarının, özel hüküm ve koşullarını çoklu sayfalar arkasına gizlemesi yasaklanmaktadır. Bu hükümlerle birlikte, herhangi bir internet sitesine giren kullanıcının tek bir tıkla tüm çerezlere izin vermesi veya bu çerezleri reddetmesi de kolaylaşmaktadır.
- Doğrudan denetim: DSA, AB'nin özellikle büyük teknoloji (*big tech*) platformlarına temsilci atmasının önünü açmaktadır. Böylece DSA, AB'ye uzman heyetleriyle birlikte platformların veri, algoritma ve iş modelleri konusunda müdahalede bulunmasına izin vermektedir.
- Acil durum kanalları: AB'nin kriz, salgın ve savaş gibi acil durumlarında halkla iletişime geçebilmesi için çevrim içi platformların gerekli sistemi kurmasını zorunlu hâle getirmektedir.

Bu kurallarla ise AB, dijital hizmetlerdeki üye ülkeler arasındaki yasal bölünmüşlük ve düzenletici boşlukların üstesinden gelerek Tek Pazar'da dijital hizmetlerin en uygun şekilde sunulmasını sağlamayı amaçlamaktadır. Yani DSA ile AB, farklı kategorilerdeki çevrim içi hizmet sağlayıcıları için başta "risk yönetimi ve risk değerlendirme yükümlülükleri" olmak üzere net bir dizi durum tespiti yükümlülüğü getirerek "güvenli, öngörülebilir ve güvenilir" bir çevrim içi ortam için uyumlaştırılmış kurallar sağlamaktadır (Madde 1). Ancak bu hedeflere ulaşılması için ulusal yetki makamlarının DSA'yı uygulamada, hizmet sağlayıcılarının ise DSA'nın yükümlülüklerine uymakta başarılı olması gerekmektedir.

Dijital Hizmetler Yasası'nın Kapsamı

DSA kuralları, AB dışında yerleşik olup olmadığına bakılmaksızın dijital hizmetlerini (AB'de yerleşik veya AB'de bulunan gerçek veya tüzel kişi alıcılara sunan) Tek Pazar'da sunan tüm sağlayıcılar için geçerlidir. Böylece tüm dijital hizmet sağlayıcılarının AB'de hizmetlerini sunarken tek bir kurallar dizisine bağlı kalmaları sağlanmaktadır. Bu sayede, farklı ülkelerde farklı yasalara uyum sağlama yükümlülüğü ortadan kalkmakta ve platformların iş yapma şekli netleşmektedir. Bu netlik, hem hizmet sağlayıcılar hem de kullanıcılar için yasal belirlilik ve öngörülebilirlik sağlamaktadır.

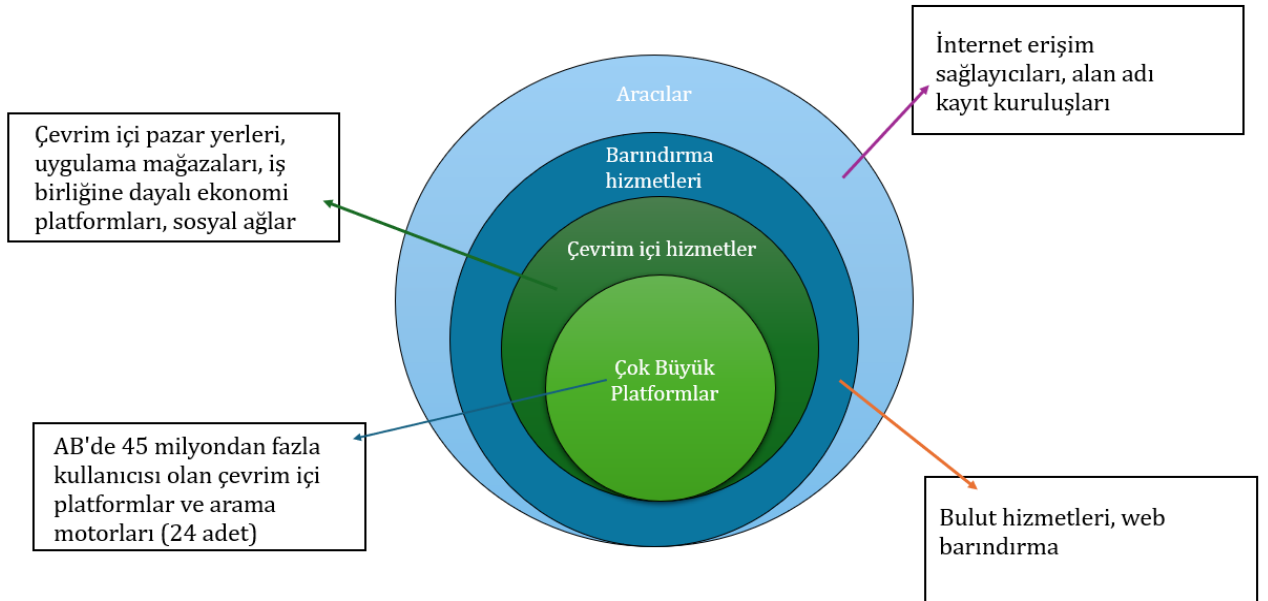
Yani DSA, internet hizmet sağlayıcıları, bulut sağlayıcıları ve web barındırma platformları, sosyal medya ağları, çevrim içi arama motorları, web tabanlı mesajlaşma hizmetleri ve e-posta hizmetleri, alan adı kayıt şirketleri, IP üzerinden ses hizmetleri ve üçüncü tarafların içeriğini depolayan veya ileten uygulama mağazaları ve çevrim içi pazar yerleri başta olmak üzere geniş bir işletme yelpazesini kapsamaktadır.

DSA, ayrıca tüm dijital sağlayıcıları tek bir kategoriye sokmak yerine sundukları hizmetlerin büyüklüğü, niteliği ve etkisine göre düzenlemeleri uyarlamak için sağlayıcıları belirli gruplara ayırmaktadır. Bu ayrımla platformlar "riske dayalı etki"den

kaynaklı olarak asimetrik yükümlülükler altına girmektedir. Bu sayede, tüm platformların sunduğu hizmetlere orantılı bir şekilde sorumluluk almaları sağlanmaktadır.

En yüksek risk potansiyeline sahip olan ve aylık kullanıcı sayısı 45 milyonu aşan Çok Büyük Çevrim İçi Platformlar (*Very Large Online Platforms-VLOPs*) ve Çok Büyük Çevrim İçi Arama Motorları (*Very Large Online Search Engines- VLOSEs*), etki alanları oldukça yüksek (bu yüzden daha çok riske sahip) olmalarından dolayı daha fazla yükümlülüğe sahiptir. Yasa dışı içerikle ve dezenformasyonla mücadelede, kullanıcıların şeffaflığı ve veri koruma gibi konularda daha kapsamlı adımlar atmaları gerekmektedir.

Şekil 1: Dijital Hizmet Sağlayıcılarının Kapsamı



Komisyon tarafından *Aliexpress, Amazon Store, Apple AppSore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, Shein, Temu, LinkedIn, Pinterest, Snapchat, TikTok, X, Wikipedia, YouTube, Zalando, Pornhub, Stripchat, Xvideos* çok büyük çevrim içi platformlar (VLOP's) olarak belirlenmiştir. *Bing* ve *Google Search* ise çok büyük çevrim içi ara motorları (VLOSE's) olarak tanımlanmıştır. Bahsedilen 24 platform sayısının ise 28'e çıkması planlanmaktadır.

Tablo 1: Gruplarına Göre Dijital Sağlayıcıların Kümülatif DSA Yükümlülükleri

	Aracılık Hizmetleri	Barındırma Hizmetleri	Çevrim İçi Platformlar	Çok Büyük Platformlar ve Arama Motorları
	Kümülatif Yükümlülük	Kümülatif Yükümlülük	Kümülatif Yükümlülük	Kümülatif Yükümlülük
Şeffaflık Raporları	●	●	●	●
Temel Haklara ve Hizmet Şartlarına İlişkin Gereklilikler	●	●	●	●
Ulusal Makamlarla Talimatlara Uygun İş Birliği	●	●	●	●
İrtibat Merkezi ve Gerektiğinde Yasal Temsilci Atama	●	●	●	●
Kullanıcılara Bildirim, Eylem ve Bilgi Sağlama Yükümlüğü		●	●	●
Cezai Suçların Raporlanması ve Bildirilmesi		●	●	●
Şikâyet ve Telafi Mekanizması ile Mahkeme Dışı Uyuşmazlık Çözümü			●	●
Güvenilir İşaretçiler			●	●
Kötü Niyetli İhbarlara Karşı Önlemler			●	●
Pazar Yerleri için Özel Yükümlülükler, Rastgele Kontroller			●	●
Çocuklara Yönelik Hedefli Reklamların ve Kullanıcıların Özel Niteliklerine Dayalı Reklamların Yasaklanması			●	●
Tavsiye Sistemlerinin Şeffaflığı			●	●
Çevrim İçi Reklamcılığın Kullanıcıya Yönelik Şeffaflığı			●	●
Risk Yönetimi Yükümlülükleri ve Krize Müdahale				●
İç ve Dış Bağımsız Denetim, İç Uyum Fonksiyonu ve Kamu Hesap Verilebilirliği				●
Kullanıcı Verilerine Dayalı Önerilerin Alınmaması Seçimi (Kullanıcı Profillemeyi Devre Dışı Bırakabilir)				●
Yetkililerle ve Araştırmacılarla Veri Paylaşımı				●
Davranış Kuralları				●
Krize Müdahalede İş Birliği				●

İletişim ve bağlantısallık alanında yeni bir dünya olan çevrim içi -ve yeni yeni keşfettiğimiz bu- dünyada, aktörlerin belirsizliği-çeşitliliği, şeffaflık ve hesap verilebilirlik eksikliği ve sınırlarının aynı zamanda insan hakları ihlalleri, dezenformasyon kampanyaları, nefret söylemi, ayrımcılık ve yasa dışı içeriğin yayılmasında da DSA, çevrim içi platformlar için düzenleyici bir çerçeve olarak çerçevelenmiş olsa da DSA, yeni bir çevrim içi insan hakları dönemi için bir köşe taşı görevi görmektedir. Çünkü, yukarıdaki tabloda da görüldüğü üzere DSA;

- İçerik denetleme uygulamalarını ve veri kullanımını detaylandıran şeffaflık raporlarını zorunlu kılmaktadır.
- İçerik modülasyonunun ötesine geçmektedir. Kullanıcıları, platformları sorumlu tutmaları için güçlendirmektedir. İçerik kaldırma kararlarına itiraz etme ve net gerekçe beyanları gerekliliği, kullanıcıların deneyimledikleri çevrim içi şekillendirme konusunda söz sahibi olmalarını sağlamaktadır. Ayrıca, üye ülkeleri platform eylemlerinden tazmin etmeye yönelik çerçeve geliştirmeye teşvik etmekte ve etkili bir çözüm bulma hakkını desteklemektedir.
- Tasarım yoluyla güvenlik vurgusu, platformları hizmetleriyle ilişkili riskleri proaktif olarak azaltmaya teşvik etmektedir. Ayrıca bu vurgu, uluslararası insan hakları hukuku kapsamında korunan ifade özgürlüğü hakkı ile de uyumlu olmasının yanı sıra bu özgürlüğün şiddeti, nefret söylemini veya ayrımcılığı teşvik etmeden kullanılmasını sağlamaktadır.

DSA, dijital alandaki aktörleri şeffaflık ve içerik denetimi ile yükümlü kılarken, kullanıcıların güçlendirilmesine yaptığı vurgu ile temel insan hakları ilkeleriyle yakından uyumlu ve daha adil, eşitlikçi, güvenli, öngörülebilir ve güvenilir bir dijital alan için önemli bir plan olarak karşımıza çıkmaktadır.

İcra Yapıları ve Yetkileri

DSA, dijital sağlayıcılara yönelik sadece yeni uyumlaştırılmış yasal yükümlülükler getirmekle sınırlı değildir. Üye ülkelerde de AB yasa koyucusunun bu yükümlülüklerin uygulanacağı ve icra edileceği yapılandırılmış kurumsal bir sistem kurması gerekmektedir.

DSA, çok büyük çevrim içi platformları ve çok büyük çevrimiçi arama motorlarını denetleme görevi Avrupa Komisyonuna vermektedir (Madde 56(2)). Diğer tüm çevrim içi hizmet sağlayıcıları, Üye Devletler tarafından kurulan veya belirlenen bir ya da daha fazla yetkili makam tarafından denetlenmektedir (Madde 56(1)). DSA, Üye Devletlere DSA'nın uygulanmasında hangi makamların yer alacağını seçme konusunda önemli ölçüde özgürlük tanımakta ve yeni veya özel bir makamın kurulmasını zorunlu kılmamaktadır. Sonuç olarak, Üye Devletler DSA'nın (bazı bölümlerinin) uygulanması için birden fazla yeni ya da mevcut yetkili makamı görevlendirebilmektedir (Madde 49(1)). Üye ülkelerin hepsi, yeni veya özel bir makamın kurulması zorunlu olmasa da Dijital Hizmetler

Koordinatörü görevini icra edecek kurumlarını 17 Şubat 2024 tarihine kadar belirlemiştir (Madde 49(3)). Dijital Hizmetler Koordinatörleri, Avrupa Komisyonu ile, üye ülkeler arasında ve ilgili üye ülke içinde DSA uygulamasını koordine etmeyi amaçlayan bir ağ olan Avrupa Dijital Hizmetler Kurulu'nun faaliyetlerine katılmaktadır (Madde 61).

Özetleyecek olursak DSA'nın icra yapıları ve yetkileri şu şekildedir:

- **Dijital Hizmet Koordinatörleri:** Her üye ülkenin belirlediği bu koordinatörler, kendi yetki alanları dâhilindeki dijital hizmetlerin uyumluluğunu gözden geçirmekte, değerlendirmekte ve dijital hizmetleri ulusal düzeyde denetlemektedir. Ancak, diğer koordinatörlerle de iş birliği yapabilmektedir. Soruşturma yetkilerine bakıldığında, koordinatörler dijital hizmet sağlayıcılarından bilgi talep edebilir, yerinde incelemeler yapabilir ve bu sağlayıcılardan gelen verilere erişebilmektedir. Düzeltici tedbirlerine bakıldığında yasa dışı içeriğin kaldırılmasını talep edebilir ve DSA'ya uyumsuzluk durumunda idari ve para cezaları uygulayabilir.
- **Avrupa Dijital Hizmetler Kurulu:** Üye ülkeler arasında iş birliğini ve bilgi alışverişini destekleyen bu kurul, bir nevi koordinatörler için danışma görevi görmekte ve DSA'nın tutarlı bir şekilde uygulanması konusunda rehberlik etmekte ve tavsiyelerde bulunmaktadır.
- **Avrupa Komisyonu:** Denetim ve yaptırım yetkisi, sağlayıcının ana kuruluşunun bulunduğu üye ülkeye aittir. Ancak bu kurala istisna olarak DSA, Avrupa düzeyini temsil eden Avrupa Komisyonuna münhasır yetki vermektedir. Bu istisna ise şu şekildedir: Komisyon, özellikle VLOP ve VLOSE'ler için denetim-soruşturma otoritesi görevi görmekte, bu sağlayıcıları doğrudan denetleyebilmekte, DSA'ya uyum için bilgi talep edebilmekte, platformların verilerine ve algoritmalarına erişim emri çıkarabilmektedir. Komisyon, denetimde Avrupa Algoritmik Şeffaflık Merkezi'nin uzmanlığından yararlanmaktadır. İçerik denetimi konusunda şeffaflık raporlaması, tüketicinin korunması, şeffaflığın ve hesap verilebilirliğin sağlanması gibi DSA yükümlülüklerinin yerine getirilmemesi durumunda DSA VLOP ve VLOSE'ler için caydırıcı cezalar ortaya koymaktadır. DSA'daki yükümlülükleri yerine getirmeyen, geçici tedbirlere uyumaya ve taahhütlerine uymayan çevrim içi platformların yıllık küresel gelirlerinin %6'sına kadar idari para cezası getirebilmektedir. Çözüm yollarına, geçici tedbirlere ve taahhütlere uyulmasında gecikilen her gün için dünya çapındaki ortalama günlük cironun %5'ine kadar periyodik cezalar uygulanabilmektedir. Son çare olarak, ihlalin devam etmesi ve kullanıcılara ciddi zarar vermesi ve kişilerin hayatını veya güvenliğini tehdit eden cezai suçlar içermesi durumunda, Komisyon belirli bir prosedürü izleyerek hizmetin geçici olarak askıya alınmasını talep edebilmektedir: Komisyon ilgili taraflardan 14 iş gününden az olmayacak bir süre içinde, talep etmeyi düşündüğü önlemleri açıklayan ve amaçlanan muhatap veya muhatapları tanımlayan yazılı rapor sunmalarını talep edebilmektedir. Komisyon, üye ülkenin dijital hizmet koordinatöründen üye ülkenin yetkili adli makamından ihlalle ilgili hizmete erişimin geçici olarak kısıtlanması için bir emir talep etmesini isteyebilmektedir. Ancak emirin, üye ülkedeki bir hâkim tarafından verilmesi

gerekmektedir. Getirilen ceza kararına karşı AB mahkemelerinde itirazın da önü açılmıştır. Ayrıca bu platformların DSA'ya yönelik ihlallerinin devamlı olması durumunda ise AB içinde yasaklanmasının da önünü açmaktadır. Sınır ötesi konuları koordine eden Komisyon, DSA'nın yeknesak bir şekilde uygulanmasını da sağlamayı hedeflemektedir. DSA ile ilgili uyumsuzluk sorunlarının soruşturulması esnasında ise zararları önlemek için de Komisyon geçici tedbirler (belirli anahtar veya etiketlerin daha fazla izlenmesi, iddia edilen ihlalleri sonlandırma veya düzeltme emirleri) almaktadır.

DSA ve Özen Yükümlülüğü

DSA'nın hesap verilebilirlik çerçevesi ile platform şeffaflığı ve sorumluluğu arasında bir denge yaratılmaktadır. Şöyle ki DSA, gözden geçirilmiş bir "**dijital hizmet sağlayıcı sorumluluk rejimi**" getirmektedir. Bu sorumluluk rejimi ise platformlara hesap verilebilirlik çerçevesini zorunlu kılmaktadır. Ayrıca DSA, yasa dışı içeriğin yayılmasını önlemek için platformları "özen yükümlülüğü" ile donatmaktadır. Bu özen yükümlülüğü ise şunları içermektedir:

- Genel Gözetim Yasağı: Platformlar tüm içeriği izlemekle yükümlü tutulmamaktadır, ancak kullanıcıların yasa dışı içeriği bildirmeleri için platformların açık prosedürler oluşturmasını gerektirmektedir. Bu yasa ile amaç, kullanıcıların mahremiyetini ve ifade özgürlüğünü korumaktır.
- Durum Tespiti Kavramı (*Concept of Due Diligence*): DSA kapsamındaki durum tespiti, platformların yasa dışı içeriği ve sistemik riskleri önlemek, tespit etmek ve ele almak için proaktif önlemler almasını içermektedir. Bu, yasa dışı içeriğin bildirilmesi ve kaldırılması için mekanizmaların uygulanmasını, risk değerlendirmelerinin yapılmasını ve içerik moderasyon süreçlerinde şeffaflığın sağlanmasını içermektedir.
- Açık hüküm ve koşullar: Platformların tutarlı ve özenli bir şekilde uygulanan açık, şeffaf hüküm ve koşullara sahip olması gerekmektedir. Bu şartlar, ifade özgürlüğü ve keyfi içerik kaldırmaya karşı koruma dâhil olmak üzere temel haklara saygı göstermesi zorunludur.
- Harekete Geçme Emri: Yetkililer, platformlara yasa dışı içeriğin kaldırılmasını emredebilir. Platformlar bu emirlere derhal uymak için mekanizmalar oluşturmalı ve yasa dışı içeriğin etkili bir şekilde ele alınmasını sağlamalıdır.
- Güvenliğe Yönelik Tasarım ve Risk Yönetimi: Platformlar özellikle küçükler için hizmetleriyle ilişkili riskleri proaktif olarak değerlendirmeli ve azaltmalıdır. Bu bağlamda platformlar içerik denetleme sistemi oluşturmalı, nefret söylemi ve dezenformasyona neden olan içerikler gibi zararlı içerikleri güçlendirmeyen algoritmalar tasarlamalı, reşit olmayanları zararlı içerikten korumak için yaş doğrulama mekanizmaları kurmalı, kullanıcılara reklam deneyimleri üzerinde kontrol verme ve sponsorlu içeriğin açık bir şekilde sağlanması yoluyla reklamcılıkla şeffaflığı sağlamalı, özellikle VLOP'lar düzenli olarak risk değerlendirme ve azaltma yükümlülüklerini yerine getirmelidir.

DSA Hesap Verebilirlik Çerçevesi: Sorumluluk Muafiyeti ve Durum Tespiti

Dijital Hizmetler Yasası, E-Ticaret Yönergesi'nin (2000/31/EC) tarafından oluşturulan mevcut dijital hizmetleri düzenleme çerçevesinin üzerine inşa edilmiştir. Bu yönerge, aracı hizmetler için kritik sorumluluk muafiyetleri sağlayarak onları bir kullanıcının talebi üzerine iletilen veya depolanan içerik için sorumluluktan korumuştur.

DSA, çevrim içi servis sağlayıcılarının (*internet services providers-ISP*) çevrim içi etkileşimi kolaylaştırmadaki temel rolünü kabul ederek bu temel muafiyetleri büyük ölçüde korumaktadır. Madde 3,4 ve 5'te ayrıntıları verilen "sorumluluk muafiyeti hükümleri" hizmet sağlayıcıları için belirli koşullar altında üçüncü taraf içeriğine ilişkin sorumluluktan muaf tutulmaya devam etmektedir. Örneğin, e-posta sağlayıcıları gibi verileri değiştirmeden veya seçmeden ileten hizmetler (sadece kanal hizmetleri) iletimi başlatmadıkları, alıcıyı seçmedikleri veya iletilen bilgiyi değiştirmedikleri sürece bilgi iletiminden sorumlu değildir (Madde 3). Önbellek hizmetleri, bilgiyi değiştirmedikleri, erişim koşullarına uydukları ve yasa dışı niteliği hakkında gerçek bilgi edindikten sonra bilgiye erişimi kaldırmak veya devre dışı bırakmak için derhâl harekete geçtikleri takdirde sorumluluktan muaftır (Madde 4). Barındırma hizmetleri ise yasa dışı faaliyet veya bilgiler hakkında fiili bilgiye sahip olmamaları veya haberdar olduktan sonra erişimi kaldırmak veya devre dışı bırakmak için hızlı hareket etmeleri koşuluyla, bir alıcının talebi üzerine depolanan bilgilerden sorumlu değildir (Madde 5).

Madde 6, barındırma hizmetlerine yönelik koşullu muafiyetlerin ana hatlarını çizerek, bu hizmetlerin yasa dışı içerik şüphesi hakkında yetkilileri bilgilendirmelerini, kolluk kuvvetleriyle iş birliği yapmalarını ve yasa dışı içeriğin yayılmasını önlemek için tedbirler almalarını gerektirmektedir. Bu, platformların sorumluluktan korunurken, yine de sorumlu bir şekilde hareket etmelerini sağlamaktadır.

DSA, muafiyetlerin ötesine geçerek platformların yasa dışı içerik ve diğer toplumsal riskleri ele almak ve proaktif adımlar atması için durum tespiti (*concept of due diligence*) yükümlülüklerini getirmektedir. Belirtmek gerekir ki DSA, neyin yasa dışı olduğunu tanımlamamaktadır. Bir içeriğin yasa dışılığı ulusal veya AB kuralları ile tanımlanmaktadır. Durum tespiti ile DSA, çevrim içi hizmet sağlayıcılarını:

- Kullanıcıların yasa dışı içeriği bildirmeleri için prosedür oluşturmak,
- Hizmetlerinde barındırılan yasa dışı içerikle ilgili soruşturmalarda yetkililerle iş birliği yapmak,
- Yasa dışı içeriğin farkına vardıklarında hızlı bir şekilde hareket etmek,
- Yasa dışı içeriğin yasa dışı olduğu bilgisini aldıktan sonra bu içeriği kaldırmak veya erişimini engellemek,
- Kullanıcıların içerik kaldırma kararlarını bildirmeleri ve bunlara itiraz etmeleri için prosedürler oluşturmak,

- Yıllık şeffaflık raporlarının hazırlanması,
- Dezenformasyon veya nefret söyleminin yayılması gibi hizmetleriyle ilişkili potansiyel riskleri belirlemek için düzenli değerlendirmeler yapmak (risk değerlendirmeleri, tüm çevrim içi platformlar),
- Yasa dışı içerik ve diğer zararlı faaliyetlerle ilgili potansiyel riskleri belirlemek (tüm çevrim içi platformlar),
- Risk değerlendirmelerine dayanarak, uygun azaltma önlemlerinin uygulanması (tüm çevrim içi platformlar)
- Yasadışı veya zararlı içeriği tespit etmek ve kaldırmak için etkili sistemlere sahip içerik moderasyon uygulamaları oluşturmak (tüm çevrim içi platformlar),
- Kullanıcıların yasa dışı içeriği bildirmeleri ve içerik kaldırma kararlarına itiraz etmeleri için açık yönergeler içeren bildirim ve kaldırma prosedürleri oluşturmak (tüm çevrim içi platformlar),
- Özellikle bu tür içeriğin yaygın olduğu platformlarda, reşit olmayanları zararlı içerikten korumak için yaş doğrulama mekanizmaları oluşturmak (çevrim içi platformlar),
- Reklamcılıkta şeffaflık, sponsorlu içeriğin açık bir şekilde etiketlenmesinin sağlanması ve kullanıcılara reklamcılık deneyimleri üzerinde kontrol sağlamak (çevrim içi platformlar),
- Kriz zamanlarında, bir kriz müdahale mekanizması oluşturmak ve bu mekanizma için Avrupa Komisyonunun özel tedbirler almasına olanak tanımakla yükümlüdür (tüm çevrim içi platformlar).

Ayrıca detaylara bakıldığında, barındırma hizmetleri barındırdıkları tüm içeriği aktif olarak izlemekle yükümlü tutulmamaktadır. Özellikle sosyal medya ve çevrim içi pazar yerleri gibi platformların, daha sıkı durum tespiti yükümlülükleriyle karşı karşıya kaldığını da belirtmek gerekmektedir (Madde 25).

Dijital Hizmetlerde DSA'nın Şeffaflık Özellikleri

Çevrim içi hizmet sağlayıcıların uygulamalarına ışık tutarak aslında yeni bir denetim yöntemi getiren DSA, bu sağlayıcılar için zorunlu bir uygulama olan “şeffaflık raporlaması” hazırlanmasını gerektirmektedir (Madde 15). Şeffaflık raporları, platformların içerik moderasyonunu, reklam uygulamalarını ve kullanıcı verilerini nasıl ele aldıklarına dair bilgileri içermesi zorunludur. Raporlar, kaldırılan içeriğin hacmi ve türlerinin yanı sıra kaldırılma nedenlerini detaylandırmalıdır. Bu sayede denetim otoriteleri, araştırmacılar ve kullanıcıların, bu sağlayıcıların içerik denetleme politikalarının etkinliğini ölçebilmelerinin yolu açılmaktadır. Ayrıca bu raporlar, reklamcılıkta kullanılan hedefleme yöntemleri ve reklam kişiselleştirme için toplanan veri türleri hakkında da bilgi vermesi gerekmektedir. Özellikle platformların reklamcılıkta şeffaflığı tercih etmesi, kullanıcıların verilerinin nasıl kullanıldığını anlamaları ve çevrim içi reklamcılık konusunda bilinçli seçimler yapmasını sağlamaktadır. Ayrıca platformlar, hazırlayacakları şeffaflık raporlarında belirli içerik

denetleme kararları için gerekçe beyanları sunmaları gerekmektedir. Bu beyanlar, belirli içeriklerin neden kaldırıldığını veya kısıtlandığını açıklayabilir.

DSA ayrıca, sağlayıcılardan şeffaflık raporlarını içeren kamuya açık bir şeffaflık veri tabanının da oluşturulmasını istemektedir (Madde 24). Bu veri tabanının, AB genelindeki platform uygulamaları hakkında merkezi bir bilgi deposu olarak hizmet etmesi beklenmektedir. Araştırmacılar, politika yapımcılar ve sivil toplum kuruluşları, bu veri tabanları ile dijital hizmetlerdeki eğilimleri analiz edebilmekte, potansiyel riskleri belirleyebilmekte ve platformları sorumlu tutabilmektedir.

Kullanıcıların güçlendirilmesi için ise DSA, kullanıcılara, içerik moderasyon kararları konusunda platformlarla aktif olarak etkileşime geçebilme yetkisi vermektedir. Bu bağlamda platformlar, kullanıcıların yasa dışı içeriği bildirmeleri için açık ve erişilebilir prosedürler oluşturması gerekmektedir. Bu prosedürlerin de yanıt için belirli bir süreye sahip olması ve açık geri bildirim mekanizmalarını içermesi tavsiye edilmiştir. Kullanıcıların ayrıca, içeriklerinin kaldırılması kararlarına ilişkin itiraz etme hakkına da sahip olduğu belirtilmelidir. Ayrıca platformlar, kullanıcıların itirazına yanıt vermek üzere net zaman çizelgeleri ile adil ve şeffaf itiraz süreçleri oluşturmakla yükümlü olduğu görülmektedir. Kullanıcıların güçlendirildiği bir diğer konu ise karşı bildirimlerle ilgilidir. Kullanıcılar, platform kararlarına itiraz etme hakkı ile donatılırken, platformların işaretlenen içeriği yeniden değerlendirmesini gerektiren karşı bildirimler göndermesinin de yolu açılmıştır.

Reklam şeffaflığıyla ilgili endişeleri gidermek için Madde 39, platformların kamuya açık bir reklam kütüphanesi bulundurmasını zorunlu kılmaktadır. Bu kütüphane, reklam verenin kimliği, reklam için ödenen tutar ve kullanılan hedefleme parametreleri de dahil olmak üzere platformda barındırılan reklamlar hakkında ayrıntılı bilgiler içermelidir.

DSA, VLOP'ların ve VLOSE'lerin algoritmik sistemleriyle ilgili kapsamlı risk değerlendirmeleri yapmalarını gerektirmektedir. Madde 14, bu platformların algoritmalarının tasarımı, işleyişi ve kullanımı ile ilgili sistemik riskleri analiz etmelerini zorunlu kılmaktadır. Bu, temel haklar, kamu sağlığı ve kamu güvenliğine yönelik risklerin değerlendirilmesini de içermektedir. Bu risk değerlendirmeleri belgelenmeli ve ilgili makamlara raporlanarak algoritmik sistemlerin potansiyel etkileri konusunda şeffaflık sağlanması gerekmektedir. Platformlar bu riskleri belirleyerek ve ele alarak zararı azaltmayı ve sistemlerinin adil ve sorumlu bir şekilde çalışmasını sağlamayı hedeflemelidir.

Açık ve şeffaf hüküm ve koşullarla ilgili olarak kullanıcıların platform kullanımını düzenleyen kuralları ve ihlallerin sonuçlarını anlamalarını sağlamak için gereklidir. Madde 14, hüküm ve koşullarda açık ve anlaşılır bir dil kullanılmasının önemini vurgulamaktadır. Platformların, kullanıcıların geçmişteki değişikliklere kolayca erişebilmelerini ve bunları inceleyebilmelerini sağlamak için hüküm ve koşullarının

sürümlü bir koleksiyonunu sunmaları gerekmektedir. Bu gereklilik, kullanıcılara platformdan ne bekleyebileceklerini ve kendilerinden ne beklendiğini açık hâle getirerek şeffaflığı ve hesap verebilirliği teşvik etmektedir.

DSA yükümlülüklerine uyumu sağlamak için Madde 37, VLOP'ların ve VLOSE'lerin bağımsız denetimlerden geçmesini gerektirmektedir. Bu denetimler, platformların DSA'da belirtilen şeffaflık, hesap verebilirlik ve güvenlik gerekliliklerine uygunluğunu değerlendirmektedir. Denetçiler, platformların içerik moderasyon uygulamalarının, algoritmik sistemlerinin ve risk azaltma önlemlerinin (Madde 34) etkinliğini değerlendirmekle görevlidir. Bağımsız denetimler, platform faaliyetleri üzerinde harici bir kontrol sağlayarak uyumluluğun yalnızca dâhili değerlendirmelere bağlı olmamasını sağlamaktadır. Bu denetimlerin sonuçları kamuya açık hâl olması ve platformların eylemlerinden sorumlu tutulduğu şeffaf bir düzenleyici ortama katkıda bulunması gerekmektedir.

DSA, sistemik risklerin anlaşılması ve ele alınmasında araştırmacılar için veri erişiminin önemini kabul etmektedir. Madde 40, düzenli ve onaylanmış araştırmacılar için veri erişimi sağlayarak, Birlik'teki sistemik risklerin tespit edilmesi, tanımlanması ve anlaşılmasına katkıda bulunan araştırmalar yapmalarına olanak tanımaktadır. Bu bağlamda DSA'ya göre araştırmacılar, gizlilik ve güvenlik güvencelerine tabi olarak belirli araştırma amaçları için verilere erişim talep edebilirler. Özellikle belirli kriterleri karşılayan uzman araştırmacılar (Vetted araştırmacılar), sistemik riskler üzerinde derinlemesine çalışmalar yapmak için daha hassas verilere erişebilmelidir. Bu erişimle değerli araştırmaları teşvik edilmesi, veri kullanımının gizlilik ve güvenlik standartlarına uygun olmasını sağlamak için düzenlenmesi planlanmaktadır. Kapsamlı gözetim ve yaptırım sağlamak için Madde 67, düzenleyici makamların şüpheli ihlalleri takiben platformlardan ek bilgi talep etmesine izin vermektedir. Bu hüküm, düzenleyicilerin olası ihlalleri etkili bir şekilde araştırmak ve ele almak için gerekli araçlara sahip olmasını sağlamaktadır. Ayrıca, platformların düzenleyici soruşturmalara karşı duyarlı ve iş birlikçi olmalarını gerektirerek şeffaflık ve hesap verebilirlik çerçevesini güçlendirmektedir.

AB Üye Devletlerinde Dijital Hizmetler Koordinatörlerinin Belirlenmesi

AB'de çevrim içi yönetişimin önemli bir revizyonunu temsil eden DSA'nın uygulama çerçevesinin önemli bir ayağı, her üye ülkede kurulan veya belirlenen Dijital Hizmetler Koordinatörleri'dir (*Digital Services Coordinator-DSC*). AB üye ülkelerinin DSA'yı ulusal yasalarına aktarmak için iki yıllık süreleri olmakla birlikte (17 Şubat 2024 tarihine kadar), bu süre zarfına kadar üye ülkelerin DSA'nın hükümlerini yansıtan ve uygulanması için gerekli yasal çerçeveyi oluşturan ulusal bir mevzuata sahip olması gerekmektedir. Üye ülkelerin ulusal Dijital Hizmetler Koordinatörü atama süreci ise DSA'yı uygulayan üye ülkenin ulusal mevzuatı bağlamında gerçekleşmektedir. Belirlenen ulusal DSC, DSA kapsamındaki tüm yetkilerini kullanabilmek için Komisyondan yetki alması

gerekmektedir. Bu yetkilendirme sürecinde Komisyon, makamın, DSA'yı AB çapında etkili bir şekilde uygulamak için gerekli kapasiteye ve bağımsızlığa sahip olup olmadığını değerlendirmektedir. Özellikle DSA, DSC'lerin yetkilerinin korunması için bağımsız ve tarafsız DSC'lerin şu özelliklerine dikkat etmektedir: DSC'lerin çevrim içi platformların tasarımı, geliştirilmesi veya işletilmesinde yer alan herhangi bir kuruluştan işlevsel olarak ayrı olması, DSA kapsamındaki yaptırım eylemlerine ilişkin bağımsız kararlar alma özerkliğine sahip olması, şeffaf ve hesap verebilirlik üzerine kurulması ve etkin denetim için uzmanlık ile donatılması (dijital hukuk, içerik moderasyonu, algoritmik önyargı ve veri koruma gibi çeşitli alanlarda uzmanlığa sahip insan kaynakları, teknik altyapı, bağımsız finansman) gerekmektedir.

Yatay Bir Düzenleme Olarak DSA

Oldukça geniş bir düzenleyici ortamın bir parçası olan DSA, yatay bir düzenlemedir. DSA'yı çevreleyen düzenleyici ortam kapsamlı ve çok yönlü olup dijital alandaki belirli konuları ele alan çok çeşitli yönerge ve tüzükleri kapsamaktadır. Şöyle ki DSA, içerik denetimi ve veri gizliliğinden piyasa adaleti ve tüketicinin korunmasına kadar dijital ortamı düzenleme ekosisteminin farklı yönlerini ele almayı amaçlayan çeşitli diğer AB düzenlemeleri ile kesişmektedir. Bu düzenlemelere uyum sadece yasal bir zorunluluk değil, aynı zamanda AB genelinde AB temel değerleri ve ilkeleriyle uyumu teşvik etmek için önemli bir unsurdur. DSA'ya uyum sağlarken ayrıca diğer düzenlemelere uyum yasal bir gerekliliktir. DSA'nın daha geniş düzenleyici manzarasında aşağıdaki AB düzenlemelerine de uyum gerekmektedir:

- Dijital On Yıl Stratejisi: Dijital On Yıl Stratejisi, 2030 yılına kadar AB'nin dijital dönüşümü için hedefler belirlemektedir. Bu strateji, AB'nin dijital yeteneklerinin geliştirilmesinden güçlü, güvenli ve sürdürülebilir bir dijital altyapı sağlamaya kadar AB'nin dijital dönüşüm vizyonunu yaratmaktadır. Bu bağlamda AB, DSA da dâhil olmak üzere Dijital On Yıl hedeflerine yönelik düzenlemeler oluşturmuştur.
- Terör İçeriği Tüzüğü: Terörü destekleyen içeriklerin çevrim içi olarak yayılmasının önüne geçilmesine odaklanmaktadır.
- Kadına Yönelik Şiddetle Mücadele Yönergesi: Kadınlara yönelik çevrim içi şiddet, nefret söylemi ve tacizi engellemeyi amaçlamaktadır.
- Telif Hakkı Yönergesi: Dijital alanda fikrî mülkiyet haklarının korunmasını ele almaktadır.
- Platformdan İşletmeye (P2B) Yönergesi: Çevrim içi platformlarda ticaret yapan kullanıcılar için adalet ve şeffaflık sağlamayı hedeflemektedir.
- Dezenformasyona Karşı Uygulama Kuralları: Özellikle seçim dönemleri başta olmak üzere çevrim içi alanda yanlış bilgilerin yayılmasıyla mücadele edebilmek için kılavuz ilkeler belirlemektedir.
- Dijital Hizmetler Yasası (DMA): Çevrim içi pazar yerleri başta olmak üzere adil rekabetin sağlanması ve VLOP ve VLOSE'lerin adil olmayan rekabete izin veren hâkimiyetinin önüne geçilmesi hedeflenmektedir.

- Görsel-İşitsel Medya Hizmetleri Yönergesi (AVMSD): Görsel-ışitsel medya hizmetlerini Avrupa değer ve ilkelerine halel getirmeyecek şekilde düzenlemektedir.
- Medya Özgürlüğü Yasası: Medyada ifade özgürlüğünü ve çoğulculuğu korumayı hedeflemektedir.
- Çocuklar için Daha İyi İnternet: Çocuklar adına daha güvenli bir çevrim içi ortam yaratmaya odaklanmaktadır.
- Genel Ürün Güvenliği Tüzüğü (GPSR): Çevrim içi satılan ürünlerin güvenliğini ve sağlamlığına, tüketici haklarına odaklanmaktadır.
- Yasa Dışı Nefret Söylemine İlişkin Davranış Kuralları: Çevrim içinde yayılan yasa dışı nefret söyleminin önüne geçmeye odaklanmaktadır.
- Veri Yasası ve Veri Yönetişimi Yasası: Veri Yasası AB içinde kişisel olmayan verilerin dolaşımına odaklanarak, işletmelerin verilere erişimini ve paylaşımını kolaylaştırırken kullanıcıların veri gizliliğini sağlamayı amaçlamaktadır. Veri yönetişimi yasası ise veri sağlayıcıları ile kullanıcılar arasında bağlantı görevi gören veri araçları için düzenleyici bir çerçeve oluşturmaktadır.
- Yapay Zekâ Yasası: AB'nin rekabet gücünü artıracakı öngörülen yapay zekâ sistemlerinin geliştirilmesi ve kullanımı için yasal bir çerçeve oluşturmayı amaçlamaktadır.
- AB Dijital Kimlik Cüzdanı: AB vatandaşların doğrulanmış kimlik belgelerini ve diğer kişisel özelliklerini mobil cihazlarında güvenli bir şekilde saklamalarına ve yönetmelerine olanak tanıyan AB genelinde standartlaştırılmış bir dijital cüzdan oluşturmayı amaçlamaktadır.
- Rekabet Hukuku: AB rekabet hukuku, AB Tek Pazarı'nda adil rekabete engel olan anlaşmaları ve uygulamaları yasaklamaktadır. Rekabet hukuku, dijital platformlar ve çevrim içi hizmetler için de geçerlidir, işletmeler için eşit ve adil bir alanı desteklemekte ve hâkim oyuncuların Pazar güçlerini kötüye kullanmalarını engellemektedir.
- Kripto Varlık Piyasaları: AB içinde kripto varlıklar için uyumlaştırılmış bir düzenleyici çerçeve oluşturmayı amaçlamaktadır. Kripto piyasasında finansal istikrarı ve yatırımcı korumasını teşvik etmektedir.
- Coğrafi Engelleme Tüzüğü: AB içinde haksız coğrafi engellemeyi yasaklamaktadır. Düzenleme, tüketicilerin diğer AB üye ülkelerinde sunulan mal ve hizmetlere erişebilmelerini sağlayarak daha entegre bir dijital pazarı teşvik etmektedir.

Türkiye'nin DSA'ya Uyumu için Önerilen Adımlar

DSA'ya uyum, AB'ye aday ve potansiyel aday ülkeler için bir zorunluluk olmasa da -AB'ye katılım sürecinde müktesebata uyum dikkate alındığında- AB'nin dijital ekosistemiyle bütünleşme açısından aday ve potansiyel aday ülkelerin DSA'ya hazırlıklı olması gerekmektedir. Özellikle DSA ilkelerinin erken benimsenmesi, aday ve potansiyel aday ülkeler için daha sorunsuz bir entegrasyonu destekleyeceği ve müktesebata uyum

yüklerini azaltacağı için Komisyon tarafından da desteklenmektedir. Bu bağlamda Türkiye'nin de aday bir ülke olarak AB ile uyumlu bir dijital strateji çatısı altında DSA ilkelerini benimsemesi, Türkiye'nin dijital hizmetler sektörünü güçlendirirken, AB ile bütünleşme sürecinde önemli bir avantaj sağlayacaktır.

Türkiye'nin DSA'ya uyum sağlaması, dijital hizmetlerin düzenlenmesi ve denetlenmesinde AB standartlarını benimsemesi anlamına gelmektedir. Bu uyum, Türkiye'nin dijital hizmetler sektöründe daha güvenli, şeffaf ve adil rekabeti gözeten bir ortam oluşturmaya katkı sağlayacaktır. Bu bağlamda Türkiye'nin, ilk olarak DSA ile ilgili alanlarda mevcut ve muhtemelen gerekli yasaları (DSA, yasal bir düzenleme olması); ulusal yargı alanında faaliyet gösteren dijital hizmetleri; teyit kontrol ağlarını, potansiyel güvenilir işaretçilerini, araştırma kurumlarını ve ilgili STK'ları; potansiyel bağımsız denetçileri, medya okuryazarlığı politikalarını ve ilgili STK'lara mali desteği haritalandırması gerekmektedir. Bu haritalandırmanın ardından başta düzenleyiciler (kamu), dijital hizmet sağlayıcıları ve bu hizmetlerden etkilenenler (işletmeler, vatandaşlar ve sivil toplum) olmak üzere kendi yaratacağı ulusal dijital hizmetler düzenlemesi için bir paydaş katılımı sağlaması gerekmektedir. Paydaşların görüş ve önerilerine dayalı bir ulusal düzenleme oluşturmak, bu düzenlemenin daha etkili ve uygulanabilir olmasını sağlayacaktır. Paydaşların görüş ve önerilerine ve uluslararası standartlara dayalı ve de DSA ilkelerini etkinleştiren ulusal düzenlemeyi oluşturması, kabul etmesi ve uygulamaya başlaması gerekmektedir. Türkiye'nin DSA'ya uyum temelinde, kendi anayasal düzenine göre dijital hizmet sağlayıcılarına ek yükümlülükler getirebileceği de belirtilmelidir. Ayrıca, Türkiye'nin yasa dışı içerikle ve dezenformasyonla mücadelede kendi özel ihtiyaçlarını ve bağlamlarını göz önünde bulundurması muhtemeldir.

Ulusal sınırları içerisinde belirlediği dijital hizmetler düzenlemesine uymayan dijital hizmet sağlayıcıları ve VLOP/VLOSE'lerin denetimi ve yaptırımını için bağımsız düzenleyici kapasiteyi geliştirmesi, DSC'sini tanımlaması, DSC'nin yetkilendirilmesi için çabalaması ve finansman kaynağı sağlaması gerekmektedir. Ayrıca Türkiye, medya okuryazarlığı politikalarını geliştirerek ve bu alanda faaliyet gösteren STK'lara mali destek sağlayarak kullanıcıları geliştirmeyi hedeflemelidir. Bu hedefle Türkiye, DSA'nın hedefleri doğrultusunda, yasa dışı içerikle mücadele ve dezenformasyonun önlenmesine önemli bir katkı sağlayacaktır.

Türkiye-AB Gümrük Birliği'nin modernizasyonu ve hizmet ticaretinin serbestleştirilmesi hedefleri kapsamında da dijital hizmetlerin düzenlenmesi konusu ön plana çıkmaktadır. DSA'ya uyum ve içerdiği kural ve standartlara yönelik yakınlaştırma çabaları Türkiye-AB ilişkilerinin pozitif gündem ve Borrell-Várhelyi Raporu tavsiyeleri doğrultusunda canlandırılması sürecine hazırlık açısından da önem taşımaktadır. 8 Temmuz 2024 tarihinde ilk kez yapılan Türkiye-AB Ticaret Konulu Yüksek Düzeyli Diyalog toplantısı ve Ticaret Bakanlığımız ve Komisyon arasındaki teknik görüşmeler, DSA'ya uyum ve hizmet ticareti konularında ivme kazanılmasına imkân sağlayacaktır.

DSA doęası gereęi (dijital ortamın sınırlarının ve aktörlerinin belirli olmaması) oldukça karmaşık ve çok yönlü bir düzenlemedir. Bu bağlamda DSA'ya uyum, bilgi deneyimi ve kapasite gerektirdiğinden, Türkiye'nin üye ülkelerin ve Komisyonun iş birlięi ve kılavuzluęuna başvurması, DSA'ya uyumu ve uygulama kapasitesinin geliştirilmesine -ve de hızlanmasına- yardımcı olacaktır.