Bölüm 8

Uluslararası Hukukta Dijital Örgütler: Sınır Aşan Veri, Siber Güvenlik ve Hukuki Sorumluluk

Zeynep Deniz Altınsoy[1]

Özet

Dijitalleşme sürecinde örgütlerde gerçekleştirilen faaliyetler ve yapılan işler de dijitalleşmeye başlamıştır. Bu süreçte uluslararası hukuk alanında da dijital örgütlerin faaliyetleri, hukuki sorumlulukları ve örgütsel süreçleri farklılaşmaya başlamıştır. Uluslararası hukuk alanında dijitalleşmeyle birlikte devletlerin uluslararası alanda hukuki sorumlulukları, uymaları gereken yasal prosedürler ve kurallar, devletlerin yetkileri ve sorumluluk alanları yeniden tanımlanmaktadır. Örgütler gelenekselden dijitale doğru değiştikçe hukuksal platformda da dijitalleşme süreci karşımıza çıkmaktadır. İçinde bulunduğumuz dijital çağda örgütlerin faaliyetlerinde ve tüm süreçlerinde en temel hammaddeleri olan verinin serbestçe dolaşımı uluslararası ticaretin ve iletişimin en temel unsurudur. Bu süreçte dijital bilgi ve veri akışı kavramları karşımıza çıkmaktadır. Bu çalışma ile dijitalleşme ile birlikte uluslararası hukuk alanında yaşanan dönüşüm ve ortaya çıkan yeni hukuki sorumluluklar ele alınmıştır. Çalışmada siber güvenlik, sınır aşan veri akışları, dijital insan hakları ve uluslararası örgütlerin dijitalleşme politikaları ve uygulamaları ele alınmıştır. Çalışma ile dijitalleşme süreci ile birlikte uluslararası hukuk normlarında ortaya çıkan etkilerin ortaya konulması ve bu yönde reform önerileri sunulması amaçlanmaktadır.

1. GİRİŞ

Günümüzde dijitalleşme, devletlerin, uluslararası örgütlerin ve özel aktörlerin işleyiş biçimini kökten değiştiren, teknolojik ve toplumsal bir dönüşüm süreci olarak kavramsallaştırılmaktadır. Uluslararası hukuk alanında dijitalleşme; devlet egemenliğinin sınırlarını, hukuki sorumluluk alanlarını ve uluslararası normların uygulanabilirliğini yeniden tanımlamaktadır (Castells, 2010, 28-35). Geleneksel örgüt yapıları yerini dijital örgütlere bırakırken,

1 Dr. Ör. Üyesi, Bilecik Şeyh Edebali Üniversitesi, İİBF, email: deniz.altinsoy@bilecik.edu.tr orcid: 0000.0002.0335.3181

https://doi.org/10.58830/ozgur.pub896.c3753

hukuk da bu dönüşüme ayak uydurmak zorunda kalmaktadır. Dijitalleşen örgütler, verilerin üretildiği, işlendiği ve paylaşıldığı, mekânsal sınırları kökten esneten yapılar olarak uluslararası hukukta yeni bir düzenleme alanı yaratmıştır (Brynjolfsson & McAfee, 2014, 89-102). Beraberinde "dijital örgütlerin" uluslararası hukukta ortaya çıkardığı birçok sorununda varlığı belirginleşmiştir. Başlıca sorunlar arasında, dijitalleşmenin etkisiyle "egemenlik kavramının sınırlarının belirsizleşmesi, sınır ötesi veri akışlarının denetimi, siber güvenlik ve siber saldırıların hukuki boyutları, dijital platformların rekabet hukuku çerçevesindeki durumu, dijital insan hakları ile veri koruma ve gizlilik" konuları yer almaktadır (Kuner, 2017; Schmitt, 2017, 106-134). Ayrıca uluslararası örgütlerin bu dönüşüme uyum sağlamak için geliştirdiği politikalar ve düzenlemeler de ayrı bir çalışma konusu ve hukuki düzenlemeyi gerektiren başlık olarak öne çıkmaktadır.

1.1. Çalışmanın Amacı ve Kapsamı

Bu çalışma, dijitalleşmenin uluslararası hukukta yarattığı dönüşümü ve ortaya çıkan yeni hukuki sorumlulukları kapsamlı biçimde incelemeyi amaçlamaktadır. Sınır aşan veri akışları, siber güvenlik, dijital insan hakları ve uluslararası örgütlerin dijitalleşme politikaları başlıkları altında derinlemesine analizler yapılacaktır. Çalışmanın temel amacı, dijitalleşmenin uluslararası hukuk normlarına olan etkilerini ortaya koymak ve bu alandaki hukuki boşlukları belirleyerek reform önerileri sunmaktır.

1.2. Yöntem ve Literatür Taraması

Çalışmada nitel araştırma yöntemi benimsenmiştir. Literatür taraması kapsamında akademik makaleler, uluslararası hukuk kitapları, uluslararası örgütlerin raporları ve mevzuat metinleri detaylı şekilde incelenmiştir. Ayrıca güncel akademik kaynaklar ve uluslararası normatif belgeler ışığında teorik ve uygulamalı analizler yapılmıştır.

2. DİJİTAL ÖRGÜTLER VE ULUSLARARASI HUKUKUN TEMEL KAVRAMLARI

2.1. Dijital Örgüt Kavramı ve Özellikleri

Dijital örgütler, uluslararası ilişkilerde ve hukukta klasik örgütlerden farklı olarak fiziksel mekândan bağımsız, internet ve dijital teknolojiler aracılığıyla faaliyet gösteren organizasyonlardır. Bu yapılar, hiyerarşik ve sabit sınırlar yerine esnek, ağ tabanlı ve muhtemelen de çok aktörlü sistemlerdir (Tapscott, 2014,204-267). Dijital örgütler, genellikle ellerindeki veriyi merkezi bir kaynak olarak kullanır. Bu bağlamda da coğrafi sınırlar ötesinde iş birliği

ve koordinasyon sağlar (Brynjolfsson & McAfee, 201, 67-80). Örneğin, "Google, Amazon" gibi küresel teknoloji devleri dijital örgütlerin tipik örnekleri olarak verilebilir. Bu dijital örgütlerin varlığı uluslararası hukukta ve sistemde devletin egemenlik ilkesi başta olmak üzere birçok güvenlik konularını devletlerin gündemine taşımaktadır. Uluslararası ilişkilerde "güvenlikleştirme" olarak tanımlanan ve devletin egemenliğine yönelik tehdit algılarının yeniden yazılarak önlem almak üzere geliştirdiği stratejiler kapsamında güvenlik sorunu haline dönüşmeleri de an meselesidir.

Uluslararası hukukun temel ilkeleri ekseninde ise "egemenlik, müdahale etmeme ve uluslararası iş birliği" temel ilkeler içerisinde kabul edilir (Crawford, 2012,57-63). Dijitalleşmenin bu ilkelerin uygulanmasında yeni zorluklar doğurduğu bir gerçektir.

2.2. Devletin Egemenlik İlkesi

Egemenlik ilkesi, devletlerin kendi toprakları ve halkları üzerinde tam yetkiye ve bu yetkiyi kendi başına kullanma hakkına sahip olmalarını ifade eder (Cassese, 2005,345-390). Dijital ortamda ise egemenlik; "veri merkezi altyapısına, siber savunmaya ve dijital politikaların belirlenmesine ilişkin haklarını" içine almaktadır. Ancak dijital ağların sınır tanımaması, egemenliğin uygulanmasını karmaşık bir hale getirmektedir (Schmitt, 2017,72). Diğer taraftan "müdahale etmeme ilkesi" devletin başka bir devletin egemenliğine müdahale etme yasağını ifade etmektedir ki devletlerin günümüz dijital dünyasında, dijital saldırılar ve siber casusluk bağlamında yapmış oldukları eylemler tartışmayı hukuk alanına ve güvenlik alanına taşımıştır (Kittichaisaree, 2015,78-154).

Özellikle siber saldırıların devlet kaynaklı olup olmadığının tespitinin zorluğu ve müdahale sınırlarının belirsizliği hukuki açıdan yeniden düzenlemelerin yapılması konusunu da gündeme getirir. Bu bağlamda "uluslararası iş birliği ilkesi" dijitalleşmenin sınır tanımayan yapısı nedeniyle daha çok gündeme gelmiştir. Bu haliyle dijitalleşme, devletlerin güvenlik, egemenliğe saygı gibi konularda özellikle iş birliği yapmasını zorunlu kılmaktadır. Siber güvenlik, veri koruma ve dijital ticaret alanlarında çok taraflı anlaşmaların geliştirilmesi, uluslararası iş birliğinin önemini gün geçtikçe artırmaktadır (United Nations, 2019). Dolayısıyla bu iş birliğinin en önemli ayağı "siber uzayın kullanımı" konusunda olacaktır. Bu kullanımın hukuki standartları ise konu özelinde daha da önem kazanacaktır. Buradan yola çıkarak bilinmektedir ki "siber uzayın" uluslararası hukukta açık bir tanımı ve statüsü bulunmamaktadır. Ancak Tallinn Manual 2.0[2]

2 2017 yılında yayınlanan Tallinn Elkitabı 2.0, devletlerin günlük yaşamda karşılaştıkları ancak

gibi rehber belgeler, siber operasyonların uluslararası hukuk çerçevesinde değerlendirilmesine katkı sağlamaktadır (Schmitt, 2017,98-123). Siber saldırıların silahlı saldırı olarak kabul edilip edilmeyeceği, meşru müdafaa kapsamında olup olmadığı gibi konular ise mevcut durumda tartışmalı bir alan olma özelliğini korumaktadır.

3. SINIR AŞAN VERİ AKIŞLARI VE ULUSLARARASI DÜZENLEMELER

3.1. Veri Akışlarının Önemi ve Küresel Ekonomiye Etkisi

Günümüzün "Dijital Çağ" olarak anıldığı bilinmektedir. Bu çağın gereği olarak verinin serbestçe akışı, uluslararası ticaret ve iletişimin temel dinamiğidir. Bu nedenledir ki küresel ekonomide, "dijital bilgi ve veri akışları", mal ve hizmetlerin uluslararası dolaşımından daha hızlı büyüyen bir alan olarak öne çıkmaktadır (World Bank, 2021). Özellikle e-ticaret, bulut bilişim, finansal teknolojiler ve sosyal medya platformları, sınır aşan veri akışlarına dayanan alanlarda faaliyet göstermek zorundadır.

Verimlilik artışı, inovasyonun hızlanması, küçük ve orta ölçekli işletmelerin (KOBİ) küresel pazarlara erişimi ve tüketici faydasının yükselmesi (OECD, 2019) gibi verinin sınır ötesi akışının ekonomik büyüme üzerindeki pozitif etkileri de devletler açısından ön plana çıkan başka bir alan haline gelmektedir. Bu nedenlerle birçok uluslararası kuruluş, serbest veri akışını teşvik etmektedir. Ancak bu destek beraberinde "kişisel verilerin korunmasına yönelik yeni rejimlerin" ortaya çıkması beklentisini yükseltecektir. Çünkü sınır aşan veri akışları, kişisel verilerin korunması meselesini kritik hale getirmiştir. Veri güvenliği ve mahremiyet, dijital ekonominin sürdürülebilirliği için temel önceliklerden biridir. Bu kapsamda da ülkeler ve bölgeler, kişisel veri korumasına ilişkin farklı norm ve düzenlemeleri kendi iç hukuklarında geliştirmiştir.

3.2. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

Avrupa Birliği'nin 2018 yılında yürürlüğe giren GDPR[3]'si, kişisel verilerin işlenmesinde standartları belirleyerek veri sahiplerinin haklarını

güç kullanımı veya silahlı çatışma eşiklerinin altında kalan siber olayları düzenleyen uluslararası hukuk kurallarını dikkate alarak bu çalışmayı temel almıştır.

3 4 Mayıs 2016 tarihinde Avrupa Birliği (AB) Resmi Gazetesi'nde yayımlanan ve 25 Mayıs 2018 tarihinde uygulanmaya başlayan (AB) 2016/679 sayılı AB Genel Veri Koruma Tüzüğü'dür. Kişisel verileri işlenen kişilerin haklarını, veri işleme faaliyetinde bulunanların yükümlülüklerini, kurallara uyum sağlama yöntemlerini ve kurallara uymayanlar hakkında uygulanacak yaptırımları öngören Tüzük, giderek daha fazla kişisel verinin işlendiği günümüzde, veri gizliliği ve güvenliği konusunda uluslararası aktörleri ve üçüncü ülkeleri

güçlendirmiş bir metindir (Voigt & Von dem Bussche, 2017, 67-70). GDPR, sadece AB sınırları içinde değil, AB vatandaşlarının verilerini işleyen şirketleri de kapsar dolayısıyla metin küresel bir etki de yaratmaktadır.

Özellikle kişisel verilerin üçüncü ülkelere aktarımı konusunda GDPR, önemli koşullar geliştirmiştir. Metnin normları gereği veri aktarımı yapılacak ülkenin yeterli veri koruma düzeyine sahip olması ya da ek güvenceler sağlaması zorunludur (Kuner, 2017,935-962). Bu durum, AB ile diğer ülkeler arasında veri koruma alanında diplomatik görüşmelere ve karşılıklı uyum çabalarının geliştirilmesini sağlamıştır. Benzer bir veri güvenliği koruma metni Türkiye'de düzenlenmiştir.

3.2.1. Türkiye'de Kişisel Verilerin Korunması Kanunu (KVKK)

Türkiye, 2016 yılında 6698 sayılı KVKK'yı yürürlüğe koyarak GDPR benzeri bir koruma sistemi oluşturmuştur. KVKK, kişisel verilerin hukuka uygun işlenmesini, veri sahiplerinin haklarının korunmasını amaçlayan bir hukuki düzenlemedir (Kişisel Verileri Koruma Kurumu, 2016). Ancak KVKK'nın uluslararası boyutta etkisi GDPR kadar geniş değildir bu etkinin beklenmesi henüz çok erkendir. Genel görüşümüz odur ki kanun metni ne yazık ki hukuki alanın dışında kamu kuruluşlarının çalışanları tarafından dahi tam olarak anlaşılabilmiş değildir. Bu düzenlemenin yapılmasının hukuki getirileri elbette çok fazladır ancak eğitimin ve aktarımın önemi çok büyüktür. KVKK'nın özellikle kamuda eğitiminin uygulayıcılar düzeyinde sürekli hale getirilmesi gerekmektedir. Diğer taraftan Türkiye-AB arasında veri koruma uyumu konusu ise ne yazık ki halen müzakere edilmektedir ve uyum yakalanmış değildir. Diğer bölgesel ve ulusal düzenlemeler açısından bakıldığında; ABD'de, kişisel veri koruma refleksi sektör bazlı ve eyalet bazlı farklı düzenlemeler uygulama şeklinde olurken, (örneğin, California Consumer Privacy Act- CCPA) Çin'de 2021 yılında Kişisel Bilgilerin Korunması Kanunu'nu (PIPL) çıkarılarak, veri koruma alanında hızlı bir şekilde mevzuatını güçlendirmek şeklinde yansımıştır (Chander & Lê, 2015, 109-151).

3.2. Veri Yerelleştirme Politikaları ve Tartışmalar

Bazı devletler, milli güvenlik ve ekonomik egemenlik gerekçesiyle verilerin kendi sınırları içinde depolanmasını zorunlu kılmaktadır. Bu "veri yerelleştirme" politikaları, devlet egemenliğini dijital alana taşımayı

---

de etkileyen bir düzenlemedir. GDPR, AB'de ve Avrupa Ekonomik Alanı'nda (AEA) kurulu bulunan veri sorumluları ile veri işleyenlerin yanı sıra, belirli koşullar altında AB ve AEA dışındaki veri sorumluları ve veri işleyenler hakkında da uygulanabilmektedir.

amaçlar (Bradshaw, Millard & Walden, 2011, 187-223). Devletlerin bu tutumu güvenlik algıları kapsamında anlaşılabilir bir reflekstir. Ancak veri yerelleştirmenin eleştirilen yönleri vardır. Bunlar arasında verilerin paylaşımının devlet tarafından önlenmesi uluslararası ticaretin önünde engel oluşturma gibi bir sonuca neden olmaktadır. Bu haliyle küresel veri ekonomisinin bölünmesi riski, maliyetlerin artması ve inovasyonun yavaşlamasına yolaçacaktır (Chander & Lê, 2015,677-739). Örneğin Rusya ve Çin, veri yerelleştirme konusunda katı uygulamalara sahipken, AB bu konuda daha esnek ama koruyucu yaklaşımlar sergilemektedir. Diğer taraftan uluslararası ticaret anlaşmalarında veri serbestisinin uygulanmaya çalışıldığı da bilinmektedir.

Dünya Ticaret Örgütü (DTÖ) ve bölgesel ticaret anlaşmaları, veri akışının serbestliği ve dijital ticaretin gelişimi için önemli düzenlemeler içermektedir. Yakın zamanda DTÖ, dijital ekonominin düzenlenmesi için yeni müzakereler başlatmıştır. Özellikle e-ticaret ve sınır aşan veri akışı konuları Örgütün gündemindedir (WTO, 2020). Ancak, DTÖ'nün veri koruma alanındaki düzenlemelerinin bütün bu çalışmalarına rağmen halen sınırlı olduğunu belirtmekte fayda var. Örgüte üye devletler arasında veri akışının paylaşılması ve e-ticaret kaynağı olarak kullanılması konusunda görüş ayrılıkları bulunmaktadır. Bu durum Örgüt açısından yeni düzenlemelerin yapılması konusunda elini daraltmaktadır.

Diğer bir örgüt yapısı olan Kapsamlı ve İlerlemeci Trans-Pasifik Ortaklığı (CPTPP) ise sınır aşan veri akışına ilişkin daha liberal hükümler içermektedir. Örgüte üye ülkeler, veri akışını gereksiz yere engellememeyi taahhüt etmektedir (CPTPP, 2018). Bu tür anlaşmalar, küresel veri ekonomisinin gelişimini görece desteklemektedir. Avrupa Birliği Dijital Tek Pazar Politikası ekseninde ise AB, Dijital Tek Pazar stratejisiyle veri ekonomisini entegre etmeyi amaçlayan adımlar atmaktadır. Bu politika, veri akışının serbest bırakılması ile kişisel veri koruma beraberinde güvenliğinin de sağlanmasını hedeflemektedir (European Commission, 2020).

Bütün bu veri paylaşımına dair düzenleme örnekleri ve gelişmeler göstermektedir ki "sınır aşan veri akışları", dijital ekonominin temel taşıdır ve uluslararası hukukta düzenlenmesi zorunlu bir alan haline gelmektedir. Ancak veri koruma, yerelleştirme ve ticaret politikaları arasında uyum sağlanması karmaşık ve hassas bir konudur. Çok taraflı iş birliği ve karşılıklı uyum, sürdürülebilir dijitalleşme için kritik önemdedir. Ancak devletlerin güvenlik algıları ile beraber hukuki düzenlemelerinin de uluslararası iş birliği konusunda engeller yarattığı bir gerçektir. Devletlerin güvenlik kaygıları anlaşılabilir durumdadır ancak hukuki düzenlemenin özellikle uluslararası

alanda yapılmasından ziyade uygulanabilir olması elzemdir. Devletin "egemen erki kullanma yetkisine sahip tek aktör" olma kabulü ise bu düzenlemelerin etkinliğine ayrıca sorun teşkil etmektedir.

4. SİBER GÜVENLİK VE ULUSLARARASI HUKUK

Siber güvenlik kavramı bilgi ve iletişim teknolojileri sistemlerinin gizliliğini, bütünlüğünü ve erişilebilirliğini koruma amacıyla alınan teknik, hukuki ve organizasyonel önlemler bütünü şeklinde tanımlanır (ENISA, 2020). Günümüz dünyasında devletler, özel sektör ve bireyler için siber güvenlik kritik bir strateji alanı haline gelmiştir. Dijitalleşmenin dünya genelinde hızlı gelişimi ile birlikte, siber saldırılar devletler ve uluslararası şirketler için daha karmaşık, yaygın ve yıkıcı hale gelmiştir (Lewis, 2018, 112-124). Bu doğrultuda hukuki düzenlemelerin ve yazılı normların hızla düzenlenmesi ve hukukun doğası gereği güncel şartlara ayak uydurması gerekliliği ortaya çıktı.

4.1. Uluslararası Hukukta Siber Saldırılar ve Hukuki Değerlendirmesi

Uluslararası hukukta siber saldırıların tanımı henüz tam olarak netleşmiş değildir. Ancak genel olarak, bir devlet ya da diğer aktörlerin bilgi sistemlerine yönelik "kasıtlı ve zararlı eylemleri" siber saldırı olarak kabul edilmektedir (Schmitt, 2017, 67-68). Bu saldırılar, veri hırsızlığı, hizmet engelleme (DDoS), altyapı sabotajı, casusluk gibi çeşitli biçimlerde olabilmektedir. Belirtmek gerekir ki uluslararası hukukta "saldırı" kavramına yönelik en net tanım "silahlı çatışma hukuku" kapsamında yapılmaktadır ve "meşru müdafaa hakkı" kavramı ile beraber okunmaktadır. Bu doğrultuda bir siber saldırının "silahlı saldırı" olarak kabul edilmesi, Birleşmiş Milletler Şartı'nın 51. maddesi uyarınca meşru müdafaa hakkını doğurabilir mi sorusu gündeme geldi (United Nations, 1945).

Tallinn Manual 2.0'a göre, ciddi ve yıkıcı sonuçlar doğuran siber operasyonlar silahlı saldırı sayılabilir (Schmitt, 2017, 203-204). Ancak zararın derecesinin tespiti ve saldırının kapsamı konuları uluslararası hukukta hâlen tartışmalıdır. Konu başlığına dair bir diğer sorun "devletin sorumluluğu ve atıf sorunudur". Siber saldırılarda devletlerin sorumluluğu önemli bir hukuki mesele halindedir. Devletin birçok eylem gibi siber saldırı konusunda da sorumluluğu tartışmalı ve sonuca ulaştırılabilen bir konu değildir. Devletlerin doğrudan ya da vekil aktörler aracılığıyla gerçekleştirilen siber operasyonlardan sorumlu tutulması maddi delile ulaşmanın zorluğu nedeniyle tartışmalı hal almaktadır (Crootof, 2015,183-220).

Özellikle anonimlik ve dijital kanıt eksikliği, sorumluluk tespitini zorlaştırmaktadır. Uluslararası teamül hukuku ve BM Çalışmaları ekseninde değerlendirilecek olursa mevcut konu; devletlerin siber uzayda uyması gereken davranış kurallarını uluslararası teamül hukuku şekillendirmektedir (Hathaway et al., 2012,817-885). Dolayısıyla uluslararası hukukun doğası gereği devlet uygulamaları kodifiye edilerek yazılı hukuk metinleri haline getirilmiştir. Aynı uygulama siber güvenlik hukuku her ne kadar yeni bir alan olsa da uygulamalar bu alanda hukuki düzenlemeler konusunda başta Birleşmiş Milletler olmak üzere ulus üstü yapılara rehber olmuştur. Bu bağlamda BM Siber Hukuku Çalışma Grubu, devletlerin siber alanda sorumlulukları ve uluslararası hukuka uyumları konusunda raporlar hazırlamaktadır (United Nations, 2015).

4.2. Uluslararası Örgütlerin Siber Güvenlik Politikaları

Ulusüstü örgütlerin siber güvenlik konusuna ilgileri dünyanın gelmiş olduğu dijital ortamla paralel olarak artmıştır. Bu kapsamda örgütlerin düzenlemeleri yalnız BM raporları ile sınırlı kalmamıştır. NATO, AB gibi örgütler de konuya ilgi göstermiştir. NATO siber savunmayı kolektif savunma kapsamında ele almakta ve siber saldırıları ittifakın güvenliğine yönelik bir tehdit olarak tanımlamaktadır (NATO, 2016). NATO Üye Devletleri, bilgi paylaşımı, ortak tatbikatlar ve siber saldırılara karşı koordinasyon mekanizmaları geliştirme konusunda teşvik etmektedir BM, siber güvenlik alanında uluslararası iş birliğini artırmak için çalışmalar yürütmektedir. BM Siber Güvenlik Çalışma Grubu ve Gençlik Siber Farkındalık Programları, küresel anlamda normların geliştirilmesi mevcut olanların yeniden reforme edilmesi ve devletler arası diyalog için platformlar sağlanması şeklinde faaliyetler geliştirmektedir (United Nations, 2020). AB ise "Dijital Tek Pazar" stratejisinin önemli bir parçası olarak siber güvenlik alanında mevzuat ve altyapı çalışmalarını yürütme gereği duymuştur. 2016 yılında kabul edilen Siber Güvenlik Direktifi ve Avrupa Siber Güvenlik Ajansı (ENISA), AB ülkeleri kapsamında koordinasyonu sağlamaktadır (European Commission, 2016). ASEAN ve Afrika Birliği gibi diğer bölgesel örgütler de dijitalleşme ve siber güvenlik alanlarında stratejiler geliştirmektedir. ASEAN Siber Güvenlik İş birliği Planı ve Afrika Birliği Dijital Ekonomi Stratejisi, bölgesel iş birliğinin dijital dönüşümle uyumlu hale getirilmesi yönünde atılan önemli adımlardır (ASEAN, 2020; African Union, 2021).

Dijitalleşmenin uluslararası örgütlerin kurumsal yapısına etkisinin olduğu da görülmektedir. Klasik uluslararası örgütler anlayışından çıkmak zorunda kalacakları bir durum söz konusu olduğu için bu örgütlerin dijitalleşme yönünde etmiş oldukları adımlar da kendileri için kurumsal yapılarına bir

tehdit olarak algılanmaktadır. Dijitalleşme, uluslararası örgütlerin karar alma süreçleri, bilgi yönetimi ve şeffaflık uygulamalarını etkileyecektir. Dijital araçlar, üye ülkeler arasındaki koordinasyonu güçlendirmekte, kamuoyuyla iletişimde yeni kanallar açmakta ve bürokratik süreçlerin hızlanmasına olanak sağlamaktadır (Weiss, 2013,243). Ancak bu gelişmeler kurumsal yapının yeniden şekillenmesine sebep olacağı için tehdit olarak algılanabilecektir.

Hukukun dijital gelişmelere bağlı olarak açıklama ve norm yaratma konusunda hızla adım atması gereken diğer alan ise "siber savaş" kavramıdır. Siber savaş, dijital verilere yönelik saldırıların askeri amaçla devletler arasında kullanılmasıdır. Bu bağlamda, uluslararası insancıl hukuk ilkeleri (jus in bello), siber savaşta uygulanabilirliği tartışılan diğer başlık olarak ortaya çıkmaktadır. Çalışmanın kapsamının "silahlı çatışma hukuku" alanına kaymaması ve bu alanın daha özel bir çalışma ile ele alınması gerekliliği gerçeğinden yola çıkarak bu konuyu sınırlı tutmak uygun olacaktır. Ancak konuya dair devletlerin risk alanı olarak görmüş oldukları noktaları özellikle "sivil altyapının korunması ve orantılılık ilkeleri" olduğunu belirtmeden geçmemek gerekir (Schmitt, 2013, 204-208).

Siber güvenlik, dijitalleşen dünyada uluslararası hukukun en önemli ve dinamik alanlarından biri haline gelmeye adaydır. Siber saldırıların tanımı, devlet sorumluluğu, meşru müdafaa hakkı gibi konular uluslararası hukukun geleceğini bu alanda önemli ölçüde etkileyecektir. Uluslararası iş birliği ve çok taraflı mekanizmaların güçlendirilmesi, siber uzayın hukuki güvenliğinin sağlanmasında kritik öneme sahiptir. Ancak iş birlikleri hukukun düzenlenmesinde ya da yeni normların oluşturulmasında yeterli bir girişim olmayacaktır. Hukuk organik bir yapıdır. Dolayısıyla devletlerin ve kişilerin ya da hukukun öznesi olan diğer aktörlerin deneyimleri ile ve bu deneyimlerin gerektirdiği ihtiyaçlar doğrultusunda gelişecektir.

5. DİJİTAL TİCARET VE HUKUKİ DÜZENLEMELER

Dijital ticaret, mal ve hizmetlerin dijital platformlar aracılığıyla alınıp satıldığı ekonomik faaliyetleri ifade eder (UNCTAD, 2019). İnternetin yaygınlaşması, mobil teknolojilerin gelişimi ve dijital ödeme sistemlerinin kullanımı ile dijital ticaret hızla büyümüştür. Elektronik ticaretin sınırları aşan doğası, geleneksel ticaret hukukunda yeni düzenlemeler yapılmasını zorunlu kılmıştır (Wilson, 2017,107). DTÖ, dijital ticaretle ilgili müzakereleri son yıllarda önceliği haline getirmiştir. Dijital ticarette tarifelerin olmaması ve veri akışının serbestliği gibi ilkeler üzerinde çalışmaları geliştirmek zorunluluğu örgütü harekete geçirmiştir (WTO, 2021). Ancak üye ülkeler arasında veri koruma ve yerelleştirme politikaları daha önce de bahsedildiği

üzere uyumsuzluklar yaratmaktadır. Diğer taraftan bölgesel dijital ticaret eylemleri "Kapsamlı ve İlerlemeci Trans-Pasifik Ortaklığı (CPTPP), AB-Kanada Kapsamlı Ekonomik ve Ticaret Anlaşması (CETA)" gibi bölgesel anlaşmalar ile kolaylaştırılmaya çalışılmıştır. Bu kolaylığın sağlanması için ilgili anlaşmaların etkili hükümler içerdiğini söylemek doğru olacaktır. Bu anlaşmalar, veri akışının serbestliği, elektronik imza ve tüketici koruması gibi konuları düzenlemektedir (Meltzer, 2018, 28).

Uluslararası ticaret hukukunun tek düzenlenmesi gereken alanı yukarıda bahsettiğimiz çerçeve ile sınırlı kalmamaktadır. Rekabet hukuku kapsamında dijital platformların değerlendirilmesi ve kontrolünün sağlanması da milletler arası özel hukuk alanında yapılması gerekli görülen diğer revizyonlar olacaktır. Dijital platformlar (ör. Amazon, Google, Alibaba), küresel ticarette merkezi aktörler haline gelmiştir. Bu durum, rekabet hukukunda yeni sorunları gündeme getirmiştir. Tekelleşme, piyasa gücünün kötüye kullanımı ve veri tabanlı rekabet engelleri, uluslararası ve ulusal düzeyde tartışılan konular olarak kendini göstermektedir (Khan, 2017,710-805).

Tartışmalı konular olarak tanımlanan en önemli kalem dijital ürünlerin (yazılım, müzik, video, veri setleri) fikri mülkiyet hakları olarak belirlenmektedir. Bu bağlamda uluslararası anlaşmalar fikri mülkiyet haklarının korunması için de düzenlemeler yapmaktadır. Dünya Fikri Mülkiyet Örgütü (WIPO) sözleşmeleri, dijital ürünlerin sınır aşan korunmasında temel rol oynamaktadır (WIPO, 2020). Ancak dijital kopyalama ve korsanlık sorunları hukukî uygulamada yaşanan diğer zorluklardır. Dijital imza teknolojilerinin elektronik sözleşmelerin de uluslararası hukuk sistemi ve ülkelerin yerel hukuklarına bütünleştirme çalışmaları da bu kapsamda genişletilmiştir. UNCITRAL Elektronik Ticaret Model Yasası ve Model Hukuku, bu alanda uluslararası standartlar belirlemektedir (UNCITRAL, 2017). Türkiye'de de aynı hukuki düzenleme kapsamında Elektronik İmza Kanunu, elektronik sözleşmelerin geçerliliğini düzenlemektedir.

Dijital ticaretin hukuki altyapısı, uluslararası ve ulusal düzenlemelerin uyumunu gerektirmektedir. Veri akışının serbestliği, tüketici haklarının korunması, fikri mülkiyetin güvence altına alınması gibi önemli konuların dijital ticaretin sürdürülebilirliğinde kilit öneme sahip olduğu bir gerçektir. Çok taraflı iş birlikleri ve mevzuat reformları, dijital ekonominin büyümesini destekleyecek öneme sahip adımlardır. Hukuk bir bütün halindedir ve yeni düzenlemeler tek başlıklar üzerinde değerlendirilemez. Yeni gelişmelerin doğurmuş olduğu ihtiyaçlar insan yaşamının her alanında etkiye sahiptir. O nedenledir ki hukukun asıl öznesi olan insanın yeni gelişmeler kapsamında haklarının korunması da hukukun asli görevidir. Dijital insan hakları konusu

tüm bu gelişmeler ekseninde ortaya çıkmaktadır ve bu bağlamda da yeni düzenlemelere ihtiyaç duyulacaktır.

6. DİJİTAL İNSAN HAKLARI VE ULUSLARARASI HUKUK

Dijitalleşme ve insan hakları arasında bir ilişki vardır. Dijitalleşme, insan hakları alanında hem fırsatlar hem de tehditler yaratmaktadır. İnternet ve dijital teknolojilerin, bilgiye erişim, ifade özgürlüğü ve katılım gibi temel hakların gerçekleştirilmesini kolaylaştırdığı bir gerçektir. Ancak bu kolaylıklar aynı zamanda mahremiyet ihlalleri, gözetim, dezenformasyon ve dijital ayrımcılık gibi risklerin ortaya çıkmasını da beraberinde getirmektedir (De Hert & Papakonstantinou, 2016,179-194).

Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi (1948) ve Medeni ve Siyasal Haklar Uluslararası Sözleşmesi (1966) gibi uluslararası temel belgeler, dijital çağda da geçerliliğini koruyan belgelerdir. BM İnsan Hakları Konseyi, internet özgürlüğü ve dijital haklar konusunda özel raporlar yayınlayarak uluslararası standartların gelişimine öncülük etmektedir (United Nations, 2018). İnsan hakları ilkelerinden en önemlisi olan "ifade özgürlüğü" dijital ortamın tartışma konuları içinde kabul görmektedir.

İnternetin, kişilere düşüncelerini geniş kitlelere iletme imkânı veren bir araç olduğu söylenebilir. Bu bağlamda hukukça ve güvenlik ekseninde dezenformasyon ve nefret söylemi gibi sorunlarla da mücadele gerektirmektedir (UN Special Rapporteur on Freedom of Opinion and Expression, 2011). Devletlerin internet üzerindeki düzenleme yetkisi, insan haklarının birincil belirteci olan "ifade özgürlüğü" ile dengeleyici şekilde kullanılması sağlanmalıdır.

Bir diğer konu, "dijital çağda mahremiyet hakkıdır". Kişilerin mahremiyetinin korunması devlet ve hukuki düzenlemelerle gerçekleştirilmesi gereken bir alandır. Bu hak kişisel verilerin korunması ile doğrudan bağlantılıdır. Kitlesel gözetim uygulamaları, dijital izleme ve veri toplama faaliyetleri, bireylerin özel hayatının gizliliğini tehdit edebilecek alanlardır (Greenleaf, 2018,1-8). GDPR ve KVKK gibi mevzuatlar bu hakların korunmasında önemli araçlar olarak sıralanabilir (GDPRL,2017,10-13). Ayrımcılık yasağı kapsamında dijital alandaki sosyal ve ekonomik eşitsizlikleri derinleştirebilmektedir. İnternete olan erişimdeki farklılıklar, dijital okuryazarlık eksikliği ve dijital önyargılar, ayrımcılık riskini beklenenden çok arttırmaktadır (Noble, 2018,117-120). Uluslararası hukuk, bu eşitsizlikleri gidermeye yönelik politikaların geliştirilmesini desteklemelidir.

Dijital insan hakları, uluslararası hukukun önemli bir alanı olarak gelişmektedir. İnternet ve dijital teknolojilerin sunduğu fırsatların korunması

ve risklerin minimize edilmesi için çok taraflı iş birliği ve norm geliştirme faaliyetleri kritik önemdedir. İnsan haklarının dijital ortamda etkin biçimde korunması, demokratik toplumların sürdürülebilirliği için gereklidir.

7. DİJİTAL ÖRGÜTLERİN HUKUKİ STATÜSÜ VE SORUMLULUKLARI

Dijital örgütler, fiziksel sınırları aşan, internet tabanlı platformlar, şirketler ve uluslararası ağlar olarak tanımlanabilir yapılardır. Bu yapılar, geleneksel örgütlerden farklı olarak daha esnek, hızlı uyum sağlayabilen, veriye dayalı ve çok aktörlü sistemler şeklinde organize olmuşlardır (Tapscott, 2014,59-103). Örneğin, küresel teknoloji devleri, sosyal medya platformları ve uluslararası dijital ticaret ağları bu kapsama giren oluşumlardır. Bu oluşumları bugün "dijital örgütler" olarak tanımlıyor olsak da hukuki statülerinin bir belirsizlik içinde olduğunu da söylemek gerekir.

Dijital örgütlerin uluslararası hukukta ve çoğu ülke hukukunda açık ve standart bir hukuki statüsü ya da pozisyonu sağlanamamıştır. Geleneksel örgütler, şirketler veya devletler gibi hukuki olarak somut tanımları olan aktörlerden farklı olarak, dijital örgütler mekânsal sınırları aşan yapıları ve karmaşık yapılandırılmaları nedeniyle hukuki tanımlamada zorluk yaratmaktadır (Kuner, 2017,935-962).

Bu belirsizlik, özellikle dijital örgütlerin uluslararası sorumluluklarının ve yükümlülüklerinin belirlenmesinde hukuki sorunların ortaya çıkmasına neden olmaktadır. Örneğin, yukarıda da değinildiği üzere dijital platformların veri koruma, tüketici hakları ve rekabet hukuku kapsamındaki sorumlulukları ülkeden ülkeye farklılık gösterebilmektedir (Bradshaw, Millard & Walden, 2011,187-223).

Uluslararası hukukta devletlerin egemenliği, dijital alanda da geçerlidir ancak dijital örgütlerin sınır tanımayan yapısı bu egemenlik kavramını zorlamaktadır (Schmitt, 2017,396). Devletler, sınırları içindeki dijital faaliyetleri düzenleme hakkına sahip olmakla birlikte, dijital örgütlerin uluslararası faaliyetleri kontrolü zorlaştırmaktadır. Ancak bu durum dijital platformların hukuki sorumluluğunun olmadığı anlamına gelmemektedir.

Dijital platformlar, hizmet sağlayıcı olarak kullanıcıların içeriklerinden doğan hukuki sorumluluklara ilişkin farklı rejimlere tabidir. Her ne kadar bu alanda da hukuki düzenlemeler çok az olsa da Avrupa Birliği Dijital Hizmetler Yasası, platformların içerik denetimi ve zararlı içeriğin kaldırılması konusundaki sorumluluklarını artırması önemli bir örnektir (European Commission, 2020).

7.1. Dijital Örgütlerin Hukuki Sorumluluklarında Karşılaşılan Zorluklar

Dijital örgütlerin faaliyetleri genellikle birden fazla ülke hukukunu ilgilendirir. Bu durum neticesinde dijital örgüt faaliyetlerinin hangi hukukun uygulanacağı ve yargı yetkisinin kimde ya da hangi ülkede olduğunu tartışmaya açar (Kuner, 2017,209). Bu durum, uyuşmazlıkların çözümünde uluslararası koordinasyonun hızlı bir şekilde sağlanmasını öncelikli kılar. Dijital dünyadaki anonimlik, hukuki sorumluluğun tespitinin önündeki en önemli engel olarak görülürken dijital kanıtların toplanması, korunması ve mahkemelerde kabulü de önemli sorun alanı olarak kabul edilmektedir (Crootof, 2015,123). Sorunlara ek olarak teknolojik gelişmelerin hızı ve ne yazık ki hukuki düzenlemelerin geride kalması da eklenmelidir. Dijital teknolojilerin hızlı gelişimi, mevcut mevzuatın geride kalmasına neden olmaktadır. Bu, dijital örgütlerin hukuki sorumluluklarının belirlenmesinde önemli gecikmelere yol açmaktadır (Bradshaw et al., 2011, 187-223). Dijital örgütlerin karakteri genel itibarı ile "ticari şirketler" olduğu için bir diğer hukuk alanı olan uluslararası ticaret hukuk açısından bu örgütlerin durumunun incelenmesi gerekmektedir.

8. DİJİTALLEŞME VE ULUSLARARASI TİCARET HUKUKU

Dijitalleşme, uluslararası ticaretin klasik yapısını da kökten değiştirmiştir. Geleneksel sınırlar ve fiziksel malların taşınması genel uluslararası ticaret hukukunun ana unsurlarını ifade ederken, dijital hizmetler, elektronik ticaret ve sınır ötesi veri akışları ticaretin ana unsurları haline gelmiştir (Baldwin, 2016, 225-239). Dijitalleşme, ticaretin hızını artırmakta, maliyetleri azaltmakta ve yeni iş modellerinin dahi doğmasını sağlamaktadır.

Mevcut durumda uluslararası ticaret hukuku, bugüne kadar fiziksel ürünlerin ticaretine odaklanmış tarihsel altyapısını dahi dijital ekonominin gereksinimlerine uyarlamak durumunda kalmıştır. Bu süreçte, elektronik belgelerin kabulü, dijital sözleşmelerin geçerliliği, sınır ötesi veri akışları ve e-ticaretin vergilendirilmesi gibi konular hukuki düzenlemelerin ana gündemini oluşturacaktır (UNCTAD, 2020). Bu gerçeği gören uluslararası ticaretin küresel düzeyde düzenlenmesinde tavsiye ve bağlayıcı kararlar alabilen DTÖ, dijital ticaretin gelişimini desteklemek amacıyla çok taraflı müzakereleri teşvik ederek çağa ayak uydurmaya yönelik adımlarını hızlandırmıştır. Özellikle e-ticaret moratoryumu ve sınır aşan veri akışlarının serbestliği gibi konuları, DTÖ üyeleri arasında devam eden müzakerelerde öncelikli hal almıştır (WTO, 2021). Daha önce de ifade edildiği üzere veri akışları ve veri koruma politikaları geliştirmeye çalışan DTÖ

müzakerelerinde, veri akışlarının serbest bırakılması ile kişisel veri koruma politikalarının dengelenmesi zorlu bir alan olarak belirlemiştir. Üye ülkeler arasında bu konuda farklılıkların mevcut olması anlaşılır bir durumdur ki bu durum yerel hukuk düzenlemelerinin sonucudur. Ancak farklılıklar ortak müzakere alanları yaratılarak uyumlaştırılabilecektir. (Meltzer, 2019,523-548). Özellikle bölgesel çoklu anlaşmalar ve ikili anlaşmalarla bu uyumun sağlanması adımları atılmaktadır. Bölgesel ticaret anlaşmaları (RTAs), dijital ticaretin hukuki altyapısını şekillendirmede önemli belgelerdir. CPTPP, USMCA ve AB-Canada CETA gibi anlaşmalar, dijital ticaretin düzenlenmesi, elektronik imzalar, veri koruma ve tüketici hakları gibi alanlarda gerçekten ileri hükümler içermektedir (Wilson, Kürzdörfer,2019,8-27).

Ticaret söz konusu olduğunda önemli alanlardan birisi de ticaretin vergilendirilmesidir. Bu kapsamda dijitalleşme, uluslararası vergi hukukunda da yeni sorunları ortaya çıkarmıştır. Dijital şirketlerin kazançlarının nerede ve nasıl vergilendirileceği özellikle OECD ve G20 ülkelerinin ortak çalışmalarında ele alınmaktadır (OECD, 2020). Dijital hizmet vergileri, bazı ülkeler tarafından uygulanmaya başlamış ancak uluslararası uzlaşı bu konuda henüz sağlanamamıştır.

Siber güvenlik ve koruma alt yapılarının oluşturulması da uluslararası ticaretin güvenliği için önem arz etmektedir. Limanlar, lojistik ağları ve ödeme sistemleri önemli ticari altyapılardır. Bu altyapıların korunması ve siber saldırılara karşı güvende olmaları uluslararası ticaretin en önemli ayağını oluşturmaktadır (Lewis, 2018,41).

Dijitalleşme, bir diğer hukuk alanı olan uluslararası ticaret hukukunun düzenlenmesini de diğer konular gibi zorunlu kılar. Çok taraflı ve bölgesel düzeyde düzenlemelerin uyumlaştırılması, ticaret hukuku için de önemli bir durumdur. Uluslararası ticaretin günümüz şartları gereği kolaylaştırılması ve adil vergilendirme sistemlerinin kurulması gerekmektedir. Siber güvenlik alanındaki iş birliği ise dijital ticaretin sürdürülebilirliği için en temel şarttır.

9. DİJİTAL DÖNÜŞÜMDE ETİK VE HUKUKİ MESELELER

9.1. Dijital Dönüşümün Etik Boyutu

Dijital dönüşüm, sadece teknolojik bir değişim değil, aynı zamanda sosyal, ekonomik ve etik boyutları olan çok katmanlı bir süreçtir (Floridi, 2019). Dijitalleşme sürecinde ortaya çıkan etik sorunlar, bireysel hakların korunması, algoritmaların tarafsızlığı, yapay zekâ sistemlerinin adil kullanımı ve veri etiği gibi konuları kapsamaktadır.

Dolayısıyla yapay zekâ uygulamalarının karar süreçlerinde artan rolü, algoritmik önyargı ve ayrımcılık risklerini gündeme getirmektedir. Birçok bilim insanının işaret ettiği üzere etik açıdan, algoritmaların şeffaf, adil ve hesap verebilir olması gerekmektedir (Jobin, Ienca & Vayena, 2019,389-395). Bu bağlamda da hukuki düzenlemeler, yapay zekâ kaynaklı haksızlıkların önlenmesine yönelik standartlar oluşturmalıdır. Bu standartların en başında gelen argüman mahremiyettir. Dijital dönüşümde veri, yeni bir ekonomik değer olarak öne çıkmaktadır. Veri toplama, işleme ve paylaşım süreçlerinde etik ilkelere uyulması, bireylerin mahremiyetinin korunması için gereklidir (Floridi & Taddeo, 2016). Veri etik kuralları, sadece hukuki zorunluluklar değil, aynı zamanda sosyal sorumluluk da gerektirir.

Bir diğer sorunlu alan ise dijital erişim ve dijital uçurum olarak belirlenebilmektedir. Dijital dönüşümün yaygınlaştırılması sürecinde, dijital uçurumun azaltılması önemli bir etik ve sosyal adalet meselesidir. Bu açıdan düşünüldüğünde "fırsat eşitliği ve kapsayıcılık prensipleri", dijital teknolojilere erişimde ayrımcılığın önlenmesini amaçlamalı ve bu amacı hayata geçirebilmelidir (Van Dijk, 2020).

9.2. Hukuki Düzenlemelerde Etik Perspektif

Hukuki düzenlemelerin etik perspektifle uyumlu olması, dijital dönüşümde sürdürülebilirlik için kritik öneme sahiptir. Hukukun öngörülebilir, adil ve hakkaniyetli olması ilkeleri evrensel ilkeler olarak kabul edildiği için bu ilkelerin teknolojinin insan merkezli gelişimini destekler biçimde yapay zekâ uygulamalarında da hayata geçirilmesi beklenir (Binns, 2018,149-159). Ayrıca, düzenleyici kurumların bağımsızlığı ve hesap verebilirliği, etik değerlere bağlılığı da güçlendirilmesi gereken alanlar olarak kabul edildiği için önem arz eder.

Tüm bu düzenlemelerin ve inceliklerin doğal hayat içine kazandırılması dijital dönüşüm sürecinde etik ve hukuki meselelerin birlikte ele alınması, teknolojinin toplum yararına kullanılmasını sağlayacaktır. Algoritmik adalet, veri mahremiyeti, dijital kapsayıcılık ve hukuki düzenlemelerde etik standartların geliştirilmesi, dijital dünyanın adil ve güvenilir bir ortam haline gelmesine katkı sağlamakla kalmayacak insan eliyle yaratılmış olan dijital alanın yine insan hayatını düzene sokan hukuki normlarla kontrol edilmesini sağlayacaktır.

Diğer taraftan özellikle dijital örgütlerde işe alımlarda yapay zekanın kullanımı, performans değerlendirme ve çalışan bağlılığı yönetiminde de adil uygulamaların geliştirilmesi hem iş hukuku hem de çalışma özgürlüğü kapsamında insan haklarının normlarına da yeni bir bakış açısı getirecektir.

Özgeçmiş tarama, yetenek keşfi ve eğitim programlarının kişiselleştirilmesi gibi işlevler yapay zekâ destekli sistemlerle optimize edilirken hakkaniyetli ve normlar çerçevesinde geliştirilmelidir (Chamorro-Premuzic et al., 2017). Aksi halde yapay zeka uygulamalarının dijital örgütlerde kullanımı, algoritmik önyargı, şeffaflık eksikliği ve hesap verebilirlik gibi etik sorunları da beraberinde getirir. Ayrıca, kişisel verilerin korunması ve yapay zekânın sorumluluk alanları, hukuk sistemlerinde henüz tam olarak netleşmediği de bilindiğine göre bu uygulamaların etik ve hukuk kurallara uygun hale getirilmesi diğer sorunlu ve çözülmesi gereken çerçeve olarak belirginleşir (Cath et al., 2018).

10. DİJİTAL DÖNÜŞÜMDE SİBER GÜVENLİK VE RİSK YÖNETİMİ

Dijital dönüşüm, örgütlerin operasyonel verimliliğini arttırdığı gerçeğinin yanı sıra yeni siber tehditlere karşı savunmasızlıkları da beraberinde getirdiği bir gerçektir (Von Solms & Van Niekerk, 2013). Siber saldırılar, veri ihlalleri ve kötü amaçlı yazılımlar, dijital örgütler açısından itibarlarının, finansal durumlarının ve hukuki sorumluluklarının doğrudan etkilendiği bir alanı da ortaya çıkarmaktadır. Bu alanda birçok çeşitli siber saldırılar olabilmektedir.

10.1. Siber Tehditlerin Çeşitleri ve Dijital Örgütlere Etkileri

Siber tehditler; fidye yazılımları (ransomware), dağıtık hizmet engelleme saldırıları (DDoS), sosyal mühendislik, iç tehditler ve yazılım açıklarından kaynaklanan saldırılar olarak sınıflandırılmaktadırlar (Symantec, 2020). Bu tehditler, dijital örgütlerin faaliyetlerini aksatmak kritik verilerin kaybına veya çalınmasına yol açma gibi sonuçlar doğurmaktadır.

Bu bağlamda siber risk yönetim yaklaşımları önem arz etmektedir. Dijital örgütler, siber riskleri önceden belirleyip yönetmek için kapsamlı risk analizleri yapmak zorunluluğunu göz önünde bulundurmak durumundadır. ISO/IEC 27001 benzeri uluslararası standartlar, bilgi güvenliği yönetim sistemlerinin kurulması için rehberlik sağlamaktadır (ISO, 2013). Bu sistemin diğer etkisinden biri de "sürekli izleme, tehdit istihbaratı ve hızlı müdahale mekanizmaları" ile risklerin minimize edilmesinde de fayda sağlamasıdır. Diğer şekliyle sadece bu sistem üzerinden korumanın yeterli olmayacağı da bir gerçektir. O nedenle siber güvenliğe dair başka güvenlik stratejileri ve politikalarının geliştirilmesi de elzemdir.

Başarılı bir siber güvenlik stratejisi, teknoloji yatırımları kadar insan faktörünü de kapsar ki özellikle hukuki düzenlemelerin yapılması insan faktörünün ayrı düşünülemeyeceği bir alandır. Çalışanların farkındalık

eğitimi, güvenlik kültürünün oluşturulması ve yetki kontrolleri kritik öneme sahiptir ve bu alanda yapılan düzenleme ve eğitimlerin içinde düzenlenmiş hukuki alanın da eğitimi verilmelidir (ENISA, 2019). Ayrıca, yedekleme, şifreleme ve erişim yönetimi gibi teknik önlemler de güvenlik mimarisinin temel taşları olduğu için bu konularda da bilgilendirme gözden kaçırılmamalıdır. Bu bağlamda da uluslararası iş birliği ve hukuki çerçeve genişletilmek durumundadır. Siber tehditler sınır tanımadığı için uluslararası işbirliği kıymetli bir girişim olacaktır. Birleşmiş Milletler, NATO, Avrupa Birliği gibi uluslararası örgütlerin bu bilinçle siber güvenlik alanında ortak standartlar ve işbirliği mekanizmaları geliştirdiği bilinmektedir (UN, 2015). Ayrıca, siber suçların önlenmesi için Budapeşte Sözleşmesi gibi hukuki düzenlemelerin varlığı da inkâr edilemez düzeyde etkindir(Council of Europe, 2001).

Ancak dijital dönüşüm sürecinde siber güvenlik ve risk yönetimi, örgütlerin sürdürülebilirliği için vazgeçilmez unsurlar olduğu düşünülürse, teknolojik altyapının güçlendirilmesi, insan faktörünün eğitilmesi ve uluslararası işbirliği ile siber tehditlere karşı etkin hukuki bir savunma hattı oluşturulması bu bağlamda hızlı adımlar atılan bir başlık halini alması gerekmektedir.

11. DİJİTAL DÖNÜŞÜMÜN HUKUKİ BOYUTLARI: VERİ KORUMA VE SİBER HUKUK

Dijital dönüşüm günümüz dünyasında çok hızlı olduğu bir gerçek bu bağlamda hukukun bu dönüşüme ayak uydurması gerekliliği toplumun düzeninin korunması açısından önemlidir. Dijital dönüşüm, teknolojik gelişmelerin örgüt yapıları ve süreçleri üzerinde etkisini artırırken, beraberinde hukuki düzenlemelerin güncellenmesi gerekliliğini de doğurmuştur. Özellikle kişisel veri koruma ve siber güvenlik alanları, dijital çağ olarak tanımlanan günümüzün hukuki gündeminde öncelikli konular olarak öne çıkmaktadır (Kuner, 2020). Dolayısıyla hukukun koruma alanlarından biri olan "kişisel verilerin korunması" dijitalleşmenin sayesinde risk altına girmiş en önemli hak ihlalleri ile sonuçlanabilecek başlıktır.

11.1. Kişisel Veri Koruma Hukuku

Kişisel verilerin işlenmesi sürecinde hukuki olarak uyulması gereken temel ilkeler vardır. Bunlar; hukuka ve dürüstlük kurallarına uygunluk, belirli, açık ve meşru amaçlar için işlenme, veri minimizasyonu, doğruluk, saklama süresinin sınırlılığı ve güvenlik önlemleri olarak sıralanabilir (Warren & Brandeis, 1890; Avrupa Birliği Genel Veri Koruma Yönetmeliği- GDPR, 2016). Türkiye'de Kişisel Verilerin Korunması Kanunu (KVKK, 2016),

kişisel verilerin işlenmesi ve korunmasına ilişkin temel hukuki çerçeveyi oluşturur. KVKK, veri sorumlularının yükümlülüklerini, veri sahiplerinin haklarını ve yaptırımları detaylı şekilde düzenler (Arıcı, 2019). Uluslararası uyumluluk ise her devletin kendi iç hukukunda bu alanın düzenlenmesi ve uluslararası alandaki normlara uyumlaştırılması açısından önemlidir. Avrupa Birliği'nin GDPR düzenlemesi, dünya genelinde veri koruma standartlarını yükselten bir modeldir. Bu kapsamda Türkiye'nin KVKK'sı ile GDPR arasındaki uyum çalışmaları, dijital ticaret ve veri alışverişinde kritik önem taşır (Kuner, 2020).

Yukarıda bahsettiğimiz düzenlemelerin içeriklerine dair işlenen suçlar "Siber suç" olarak kavramsallaştırılan alanın içine dahildir. Dolayısıyla "dijital dünya suçları" bilişim sistemlerine yönelik izinsiz erişimi, veri hırsızlığını, siber dolandırıcılığı, fidye yazılım saldırıları gibi eylemleri kapsar (Wall, 2007). Bu nedenle bu suçlar, dijitalleşmenin yaygınlaşmasıyla beraber hızla artmakta ve hukuki mücadeleyi zorunlu kılmaktadır.

Türkiye'de Siber Suçlar Kanunu ve ilgili mevzuatların bilişim suçlarına karşı caydırıcı önlemleri içerdiği söylenebilir. Ayrıca, kolluk kuvvetleri ve yargı organlarının siber suçlarla mücadelede etkinliği de gün geçtikçe hem hukuki olarak hem de alanda çalışan görevlilerin nitelikli hale gelmesi açısından verilen eğitimler bağlamında arttırılmaktadır (Doğan, 2018).

Kısaca değinilmesi gereken bir alan da dijital dönüşümle birlikte elektronik ortamda yapılan sözleşmelerdir. Haliyle bu dönüşümün yaratmış olduğu kolaylık dijital sözleşmeleri yaygınlaşmıştır. Elektronik imza ve e-sözleşmelerin hukuki geçerliliği, ilgili mevzuatlarca güvence altına alındığını söylemek gerekir (Reidenberg, 1998). Türkiye'de de 5070 sayılı Elektronik İmza Kanunu, bu geçerliliği düzenlemektedir.

SONUÇ

Dijital dönüşüm, günümüz örgütlerinin yapısını, iş süreçlerini ve stratejilerini köklü biçimde değiştiren çok boyutlu bir süreç olarak tanımlanabilir. Geleneksel örgütlerden dijital örgütlere geçiş, sadece teknolojik yeniliklerin adaptasyonunu değil; aynı zamanda insan kaynakları, kültür, etik, hukuki düzenlemeler ve liderlik anlayışlarında da dönüşümü beraberinde getirir. Dijital dönüşüm, örgütlerin iş yapış şekillerini temelden değiştirirken, beraberinde yeni fırsatlar ve riskler getirmektedir. Başarılı bir dijital dönüşüm için teknolojik altyapının yanı sıra etik ilkeler, hukuki düzenlemeler, insan faktörü ve etkili liderlik kritik öneme sahiptir. Bu bağlamda, dijital örgütlerin sürdürülebilirliği, çok disiplinli yaklaşımların entegrasyonu ve sürekli adaptasyon yeteneğine bağlıdır. Kitapta ele alınan

konular, dijital çağın karmaşık yapısını anlamak ve örgütleri bu yeni ortamda başarılı kılmak için yol gösterici niteliktedir. Dijital dönüşüm sürecinde hukuki düzenlemelerin güncellenmesi, bireylerin ve örgütlerin haklarının korunması için esastır. Veri koruma ve siber hukuk alanlarındaki uyumlu ve etkin düzenlemeler, dijital ekonominin güvenli ve sürdürülebilir gelişimini sağlar.

Geleneksel örgütlerin dijitalleşme sürecinde karşılaştıkları dönüşüm dinamiklerini, yapay zekâ uygulamalarını, etik ve hukuki meseleleri, liderlik ve değişim mühendisliği yaklaşımları analiz ettiğimiz çalışmanın hukuki alana yeni bakışlar getirmesi beklenmektedir. Ayrıca, siber güvenlik, çevresel sürdürülebilirlik ve veri koruma gibi güncel konulara da odaklanılması, hukuki süreçlerin bu ihtiyaçlar göz önünde bulundurularak yapılandırılması gerekliliği de bir gerçektir.

Dijital çağda örgütlerin karşılaştığı fırsat ve zorlukları bütüncül bir perspektiften özellikle uluslararası alandaki hukuki düzenlemelerin arttırılarak sınırı aşan suçlar kapsamında değerlendirilen bu alana ait suçların önlenmesine destek verilmelidir. Sadece uluslararası alanda yapılan düzenlemelerin yeterli olmayacağı gerçeğinden yola çıkılarak bir takım mekanizmaların varlığı arttırılmalı ve ülkelerin düzenlere ayak uydurması ve iç hukuk normlarını yenilemesi gerekmekte ve bu da ulus üstü yapıların çabalarıyla da desteklenmelidir. Günümüz dünyasının "güvenlik" algısı dijitalleşme ile değişime uğramış her alanda devletin, bireyin güvenliğinin sağlanması başat sorun halini almıştır. Dijitalleşme ile ortaya çıkan bu güvenlik değişimi halen hukuki eksikliklerle de beslenmektedir. Ortak hareket edebilme yeteneği ve bireysel güvenliği içeren verilerin korunmasının sağlanması ile örgüt ve devletlerin güvenliğinin arttırılması da sağlanacaktır.

Kaynakça

African Union. (2021). *Digital Transformation Strategy for Africa (2020-2030)*. https://au.int/en/documents/20201221/digital-transformation-strategy-africa-2020-2030

Arıcı, S. (2019). Türkiye'de Kişisel Verilerin Korunması Hukuku. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 68(1), 1-25.

ASEAN. (2020). *ASEAN Cybersecurity Cooperation Strategy*. https://asean.org/storage/2021/01/ASEAN-Cybersecurity-Cooperation-Strategy.pdf

Avolio, B. J., Kahai, S., & Dodge, G. E. (2014). E-Leadership: Re-Examining Transformational Leadership in the Digital Age. *Leadership Quarterly*, 25(1), 105-131.

Baldwin, R. (2016). *The Great Convergence: Information Technology and the New Globalization*. Harvard University Press.

Belkhir, L., & Elmeligi, A. (2018). Assessing ICT Global Emissions Footprint: Trends to 2040 & Recommendations. *Journal of Cleaner Production*, 177, 448-463.

Binns, R. (2018). Fairness in Machine Learning: Lessons from Political Philosophy. *Proceedings of Machine Learning Research*, 81, 149-159.

Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. International Journal of Law and Information Technology, 19(3), 187-223.

Cameron, E., & Green, M. (2015). *Making Sense of Change Management* (4th ed.). Kogan Page.

Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach. *Science and Engineering Ethics*, 24(2), 505-528.

Chander, A., & Lê, U. P. (2015). Data Nationalism. Emory Law Journal, 64(3), 677–739.

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. https://www.coe.int/en/web/cybercrime/the-budapest-convention

CPTPP. (2018). Comprehensive and Progressive Agreement for Trans-Pacific Partnership.https://www.mti.gov.sg/-/media/MTI/Resources/FTA/CPTPP/Annexes-and-Text/Annex-on-Cross-Border-Trade-in-Services.pdf

Crootof, R. (2015). The Killer Robots Are Here: Legal and Policy Implications. *Cardozo Law Review*, 36(1), 183-220.

Davenport, T. H., & Ronanki, R. (2018). Artificial Intelligence for the Real World. *Harvard Business Review*, 96(1), 108-116.

De Hert, P., & Papakonstantinou, V. (2016). The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals? *Computer Law & Security Review*, 32(2), 179-194.).

Doğan, C. (2018). Türkiye'de Siber Suçlar ve Hukuki Düzenlemeler. Bilişim ve Hukuk Dergisi, 12(2), 45-62.

ENISA. (2020). *ENISA Threat Landscape Report 2020*. European Union Agency for Cybersecurity.

ENISA. (2019). ENISA Threat Landscape Report 2019. European Union Agency for Cybersecurity.

European Commission. (2020). A European Green Deal: Striving to be the First Climate-Neutral Continent. https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en

European Commission. (2020). *Shaping Europe's Digital Future*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

European Commission. (2016). *Cybersecurity Strategy of the European Union*. https://ec.europa.eu/digital-strategy/our-policies/cybersecurity_en

European Commission. (2020). *Shaping Europe's Digital Future*. https://digital-strategy.ec.europa.eu/en

European Commission. (2020). *Digital Services Act*. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2014). Embracing Digital Technology: A New Strategic Imperative. MIT Sloan Management Review.

Floridi, L. (2019). The Ethics of Artificial Intelligence. The Oxford Handbook of Ethics of AI.

Floridi, L., & Taddeo, M. (2016). What Is Data Ethics? Philosophical Transactions of the Royal Society A, 374(2083), 20160118.

Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey. *Privacy Laws & Business International Report*, (147), 10-13.

Greenleaf, G. (2018), Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, UNSW Law Research Paper No. 18-56

Hathaway, O. A., et al. (2012). The Law of Cyber-Attack. *California Law Review*, 100(4), 817-885.

Hiatt, J. (2006). *ADKAR: A Model for Change in Business, Government and our Community*. Prosci Research.

https://ccdcoe.org/research/tallinn-manual Erişim Tarihi: 11.07.2025.

https://gdpr-info.eu Erişim Tarihi: 12.08.2025.

ISO. (2013). ISO/IEC 27001: Information Security Management Systems. International Organization for Standardization.

Jobin, A., Ienca, M., & Vayena, E. (2019). The Global Landscape of AI Ethics Guidelines. *Nature Machine Intelligence*, 1, 389-399.

Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2019). Strategy, Not Technology, Drives Digital Transformation. MIT Sloan Management Review.

Khan, L. (2017). Amazon's Antitrust Paradox. Yale Law Journal, 126(3), 710-805.

Kişisel Verileri Koruma Kurumu. (2016). 6698 sayılı Kişisel Verilerin Korunması Kanunu. https://www.kvkk.gov.tr

Kotter, J. P. (1996). *Leading Change*. Harvard Business School Press.

Kuner, C. (2020). GDPR and Its Global Impact: Understanding the EU Data Protection Regulation. International Data Privacy Law, 10(1), 3-10.

Kuner, C. (2017). The Internet and the Global Reach of EU Law. *German Law Journal*, 18(4), 935-962.

Kuner, C. (2020). GDPR and Its Global Impact: Understanding the EU Data Protection Regulation. International Data Privacy Law, 10(1), 3-10.

Lewis, J. A. (2018). *Cybersecurity and Cyberwarfare: What Everyone Needs to Know*. Oxford University Press.

McKinsey & Company. (2018). The Case for Digital Reinvention. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-case-for-digital-reinvention

Meltzer, J. P. (2018). *The Internet, Cross-Border Data Flows and International Trade*. *Issues in Technology Innovation*, 28.

Meltzer, J. P. (2019). Digital Trade and Data Governance: The Need for a New Approach. Brookings Institution.

Murugesan, S. (2008). Harnessing Green IT: Principles and Practices. *IT Professional*, 10(1), 24-33.

NATO. (2016). Cyber Defence. https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. (2018). NATO Cyber Defence. https://www.nato.int/cps/en/natohq/topics_78170.htm

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York University Press.

OECD. (2019). Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies. OECD Publishing.

OECD. (2019). Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies. OECD Publishing.

OECD. (2020). *Tax Challenges Arising from Digitalisation – Report on Pillar One Blueprint*. OECD Publishing.

Reidenberg, J. R. (1998). Electronic Contracting and the Legal System. *Harvard Journal of Law & Technology*, 12(2), 143-174.

Russell, S., & Norvig, P. (2016). *Artificial Intelligence: A Modern Approach* (3rd ed.). Pearson.

Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

Symantec. (2020). Internet Security Threat Report. Symantec Corporation.

UN Special Rapporteur on Freedom of Opinion and Expression. (2011). Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Internet. Doc A/HRC/38/35.

UN Special Rapporteur on Freedom of Opinion and Expression. (2011). Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Internet. UN Doc A/HRC/17/27.

UN. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations.

UNCITRAL. (2017). *Model Law on Electronic Commerce with Guide to Enactment 1996*. United Nations.

UNCTAD. (2019). *Digital Economy Report 2019*. https://unctad.org/system/files/official-document/der2019_en.pdf

UNCTAD. (2020). *E-commerce and Digital Economy Report*. https://unctad.org/system/files/official-document/der2020_en.pdf

United Nations. (1945). *Charter of the United Nations*.

United Nations. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Report to the UN General Assembly.

United Nations. (2020). *UN Cybersecurity Initiatives*. https://www.un.org/en/cybersecurity

United Nations. (2018). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Op pression. UN

United Nations. (2019). The State of Broadband 2019: Broadband as a Foundation for Sustainable Development. https://www.broadbandcommission.org/publication/state-of-broadband-2019/

Van Dijk, J. (2020). *The Digital Divide*. Polity Press.

Van Dijk, J. (2020). *The Digital Divide*. Polity Press.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.

Von Solms, R., & Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, 38, 97-102.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220.

Weiss, T. G. (2013). *Global Governance: Why? What? Whither?* Polity Press.

Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading Digital: Turning Technology into Business Transformation*. *Harvard Business Review* Press.

Willcocks, L., Lacity, M., & Craig, A. (2017). Robotic Process Automation: The Next Transformation Lever for Shared Services. The Outsourcing Unit Working Research Paper Series, 15(1).

Wilson, J. S. (2017). *Digital Trade in the US and Global Economies*. Peterson Institute for International Economics.

Wilson, J. S., Kürzdörfer.N., (2019). Digital Trade and Trade Agreements. Peterson Institute for International Economics. "The dog that does not bark – Weaponised interdependence and digital trade at the World Trade Organization", https://www.tandfonline.com/doi/full/10.1080/09692290.2025.2483371?scroll=top&needAccess=true#abstract

WIPO. (2020). *Intellectual Property and Digital Economy*. https://www.wipo.int/about-ip/en/digital_economy.html

World Bank. (2021). *World Development Report 2021: Data for Better Lives*. https://www.worldbank.org/en/publication/wdr2021

WTO. (2020). *Trade and Digital Economy*. https://www.wto.org/english/tratop_e/digit_e/digit_e.htm

WTO. (2021). *World Trade Report 2021: Economic Resilience and Trade*. https://www.wto.org/english/res_e/reser_e/wtr_e.htm

WTO. (2021). *World Trade Report 2021*. https://www.wto.org/english/res_e/reser_e/wtr_e.htm

Zhou, C., et al. (2017). A Review of Sustainable Development Goals and ICTs. Sustainability, 9(9), 1687.