Bu proje Avrupa Birliği tarafından finanse edilmektedir.

TÜRKİYE VE AB
MALİ İŞBİRLİĞİ
TEMEL HAKLAR

Temel Haklar Sektör Koordinasyonunun Güçlendirilmesi Projesi

DİJİTAL HAKLARA İLİŞKİN KARŞILAŞTIRMALI ÇALIŞMA
(ALMANYA-AVUSTURYA-İRLANDA)

WEglobal

ANKARA

2023

DİJİTAL HAKLARA İLİŞKİN KARŞILAŞTIRMALI ÇALIŞMA

(ALMANYA-AVUSTURYA-İRLANDA)

Bu doküman Avrupa Birliği'nin mali desteğiyle üretilmiştir. Bu dokümanın içeriğinden sadece WEglobal Danışmanlık A.Ş. liderliğindeki konsorsiyum sorumludur ve hiçbir şekilde Avrupa Birliği veya T.C. Dışişleri Bakanlığı Avrupa Birliği Başkanlığı'nın görüşlerini yansıttığı şeklinde yorumlanamaz.

İÇİNDEKİLER

KISALTMALAR....4

1. Dijital Hakların Önemi....5

2. Seçilen Ülkeler....8

3.Uyum İçin Üye Ülkeler Tarafından Çıkartılan Mevzuata İlişkin Bilgiler....8

3.1. Kişisel Verilerin Korunması Hukuku....9

3.1.1. Almanya....10

3.1.2. Avusturya....10

3.1.3. İrlanda....10

3.2. Veri Yönetişimi Hukuku....11

3.3. E-Ticaret ve Dijital Hizmetler....12

3.3.1. Almanya....13

3.3.2. Avusturya....13

3.3.3. İrlanda....13

3.4. Siber Güvenlik Huku....14

3.5. Yapay Zekâ Hukuku....14

4. Birlik Nezdinde ve Ulusal Düzeyde Kurumsal Yapılanma....16

4.1. Mevcut ve Kurulmasi Öngörülen AB Kurumları....16

4.2.Almanya....16

4.3.Avusturya....17

4.4.İrlanda....17

5. Uygulamadan Örnekler....18

5.1.Almanya....18

5.2.Avusturya....19

5.3.İrlanda....20

6. Karşılaştırma ve Sonuç....20

KAYNAKÇA....23

KISALTMALAR	
AB	Avrupa Birliği
ABA	Avrupa Birliği Antlaşması
DPO	Veri Koruma Görevlisi
DSA	Dijital Hizmetler Düzenlemesi
PET	Mahremiyeti Arttırıcı Teknolojiler

Hazırlayan
Doç. Dr. Mehmet Bedii KAYA

1. Dijital Hakların Önemi

Avrupa Birliği (bundan sonra 'AB' ya da 'Birlik' olarak anılacaktır) nezdinde dijital haklara ilişkin özellikle son dönemlerde önemli gelişmeler yaşanmaktadır. Bu gelişmeleri izah etmek amacıyla öncelikle AB tarafından çizilen genel çerçeve izah edilecek, ardından somut hukuki düzenlemeler ele alınacaktır.

Birlik, özellikle ilk kurulduğu dönemlerde malların ve hizmetlerin serbest dolaşımı ilkelerini hayata geçiren temel hürriyetler açısından doğrudan uygulanabilirlik ilkesini öngörürken, hukuki açıdan yeknesaklaşma faaliyetleri çoğunlukla sadece (kural olarak) üye ülkeleri bağlayan direktifler vesilesiyle yürütülmekte, buna karşılık tüzükler ya da regülasyonlar ise istisnai halleri teşkil etmekteydi. Bir diğer ifade ile Birlik nezdinde eskiden hukuki açıdan yeknesaklaştırmanın yöntemi olarak direktifler tercih edilirken son dönemlerde artık daha çok doğrudan uygulanabilir nitelikte olan tüzük tercih edilmektedir. Dolayısıyla genel bir eğilim olarak Birlik artık hukuki çerçeveyi çizip üye ülkelere belirli bir takdir alanı bırakmak yerine özellikle dijital alanda doğrudan kendi kurallarını koymakta, doğrudan üye ülkelerde uygulanan tüzükleri tercih etmekte, bununla birlikte ilgili tüzüklerde "opening clause" (açılış hükmü) olarak nitelendirilen ve ancak istisnai durumlarda üye ülkelere farklı düzenleme yapma yetkisi tanıyan imkanlar öngörmektedir.

Yukarıda izah edilen genel eğilim neticesinde dijital haklar bağlamında üye ülkelerin kendi iç hukukuna aktarabilecekleri bir direktif çoğu zaman sözkonusu değildir. Bilakis Birlik, tüzükler vesilesiyle kural olarak Üye Ülkelerin ulusal hukuk düzenlerinde doğrudan uygulanabilen düzenlemeyi tercih etmektedir. Hal böyle olunca üye ülkelerin kendine mahsus mevzuat çıkartma imkanları son derece sınırlıdır. Yine Birlik, dijital haklar bağlamında çıkardığı her yeni tüzük kapsamında eşzamanlı olarak da ilgili bir kurumun ihdas edilmesini öngörmektedir. Bu kurum, çoğunlukla henüz üye ülkelerde de mevcut olmayan yeni bir kurum niteliğini haizdir. Dolayısıyla üye ülkeler bazında gerçekleştirilecek incelemeler, öncelikle Birlik mevzuatında bütün üye ülkeler için yeknesak şekilde uygulanacak olan mevzuat ve kurum ve kuruluşları esas alacak, ancak istisnai durumlarda üye ülkelere takdir yetkisi tanındığı hallerde ülke özelinde mevzuat ve kurumlara ilişkin bilgilere yer verilecektir.

Bununla birlikte hukuki açıdan tam yeknesaklık, uygulama açısından da tam yeknesaklık anlamına gelmemektedir. Dolayısıyla ülke bazında gerçekleştirilecek olan incelemeler, özellikle ilgili üye ülke bazındaki farklı uygulamaları esas alacaktır.

Bu genel açıklamalar ışığında Birlik mevzuatına bakıldığında dijital haklar çerçevesini çizen dört ana metinden bahis açmak mümkündür. Bunlar Avrupa Birliği Dijital Tek Pazar Stratejisi, 2030 Dijital Pusula Bilgilendirmesi, Dijital On Yıl Yolu Politika Programı Kararı ve Dijital On Yıl İçin Dijital Hak ve İlkeler Avrupa Bildirisi'nden ibarettir.

Dijital Tek Pazar Stratejisinin amacı, üç ana ilke ışığında Birlik içerisindeki ekonomik büyüme, istihdam, rekabet, yatırım ve inovasyona katkı sağlamaktır. Sözkonusu ilkeler ise tüketiciler ve teşebbüslere Birlik içerisinde dijital ürün ve hizmetlere daha iyi erişim imkanı sunulması, dijital ağlar ve yenilikçi hizmetlerin gelişimi için doğru şartlar ve uygun alanların oluşturulması ve dijital ekonominin büyüme potansiyelini en yüksek seviyelere taşımaktır.

2030 Dijital Pusula Bilgilendirmesi ise dört temel noktadan müteşekkildir. Bunlar, dijital okur-yazarlığı olan bir toplum ve kalifiye dijital çalışanlar, sağlam, işlevsel ve dayanıklı dijital altyapılar, teşebbüslerin dijital dönüşümü ve kamusal hizmetlerin dijitalleşmesidir.

Özellikle dijital haklar açısından incelemeye layık gördüğümüz Dijital On Yıl İçin Dijital Hak ve İlkeler Avrupa Bildirisi de yine farklı ilkelerden yola çıkmaktadır. Bu ilkeler, dijital dönüşümün merkezine insanı yerleştirmek, dayanışma ve kapsayıcılık, bağlanabilirlik, dijital eğitim, öğretim ve beceriler, adil ve hakkaniyetli çalışma koşulları, çevrimiçi dijital kamu hizmetleri, tercih özgürlüğü, algoritmalar ve yapay zekâ sistemleriyle etkileşimler, adil bir dijital ortam, dijital kamusal alana katılım, güvenlik, emniyet ve güçlendirme, korumalı, güvenli ve emniyetli bir dijital ortam, mahremiyet ve veri üzerinde bireysel kontrol, dijital ortamda çocukların ve gençlerin korunması ve güçlendirilmesi ile sürdürülebilirlik olarak özetlenebilecektir. Bu ilkelerden neyin kastedildiğini incelemeden önce sözkonusu ilkelerin kısmen yukarıda zikredilen diğer politika bildirilerinde de mevcut olduğunu, bunlarla örtüştüğünü söylemek mümkün olacaktır. Bununla birlikte özellikle temel hak ve ilkelerden esinlenen Dijital Hak ve İlkeler Avrupa Bildirisinin odağında daha çok Birlik vatandaşlarının dijital çağda haklarının korumasının olduğunu söylemek mümkündür.

Bu çerçevede öncelikle Birlik, dijital dönüşümün merkezine insanı yerleştirmektedir. Dolayısıyla teknoloji, Birlik içerisinde yaşayan tüm insanlara hizmet etmeli, fayda sağlamalı ve tam bir güvenlik ve temel haklarına saygı içerisinde isteklerinin peşinden gidebilmeleri için onları desteklemelidir. Sözkonusu insan merkeziyetçi yaklaşım, ayrıca dayanışma ve kapsayıcılık ilkesiyle desteklenmektedir. Buna göre teknoloji insanları bölmek için değil, birleştirmek için kullanılmalıdır. Dijital dönüşüm, Birlik içerisinde adil ve kapsayıcı bir toplum ve ekonomiye katkıda bulunmalıdır. Eşitlik notasında Birlik içerisinde mukim olan herkesin Birliğin her noktasından uygun fiyat ve yüksek hızla dijital dünyaya erişebilmesi amaçlanmaktadır. Bunun için elbette herkesin eğitim, öğretim ve yaşam boyu öğrenme hakkına sahip olması ve tüm temel ve ileri düzey dijital becerileri edinebilme imkanına sahip olabilmesi gerekmektedir. İş hayatında ise herkes, istihdam statüsü, şekli veya süresi ne olursa olsun, fiziksel iş yerinde olduğu gibi dijital iş ortamında da adil, hakkaniyetli, sağlıklı ve güvenli çalışma koşullarına ve uygun korumaya sahip olma hakkına sahiptir. Dijital kamu hizmetleri çerçevesinde herkesin AB'deki temel kamu hizmetlerine çevrimiçi erişimi olmalıdır. Dijital kamu hizmetlerine erişirken ve bunları kullanırken hiç kimseden gereğinden fazla veri talep edilmemelidir. Dijital dünyanın en önemli unsurlarından olan algoritmalar ve yapay zeka sistemleriyle etkileşimler hususunda ise yapay zekanın nihai olarak insanlığın refahını artırmak için insanlara bir araç olarak hizmet etmesi gerektiği kabul edilmektedir. Dolayısıyla herkes, dijital ortamda kendi bilinçli tercihlerini yapmak da dahil olmak üzere algoritmik ve yapay zeka sistemlerinin avantajlarından yararlanma yetkisine sahip olmalı ve aynı zamanda kişiler bu sistemlerin sağlıklarına, güvenliklerine ve temel haklarına yönelik teşkil ettiği risk ve zararlara karşı korunmalıdır. Benzer şekilde herkesin, objektif, şeffaf, kolay erişilebilir ve güvenilir bilgilere dayanarak hangi çevrimiçi hizmetleri kullanacağını etkin ve özgür bir şekilde seçebilmesi gerekmektedir. Bunun bir diğer görünümü olarak dijital kamusal alana katılım noktasında herkesin, güvenilir, çeşitli ve çok dilli bir dijital ortama erişim sahibi olması amaçlanmaktadır. Nitekim farklı türdeki içeriklere erişim, çoğulcu bir kamusal tartışmaya ve ayrımcı olmayan bir şekilde demokrasiye etkin katılıma katkıda bulunur. Özellikle mahremiyet ve kişisel verilerin korunması ile alakalı olarak herkesin, tasarımı gereği güvenli, emniyetli ve mahremiyet-korumalı dijital teknolojilere, ürünlere ve hizmetlere erişebilmesi ve bu sayede işlenen bilgilerin yüksek düzeyde gizliliği, bütünlüğü, kullanılabilirliği ve doğruluğunun sağlanması ise bir diğer amaç olarak karşımıza çıkmaktadır. Kişisel verilerin korunması hakkının bir diğer uzantısı olarak mahremiyet ve veri üzerinde bireysel kontrol bağlamında herkesin mahremiyet ve kişisel verilerinin korunması hakkına sahip olduğu, sözkonusu hakkın bireylerin kişisel verilerinin nasıl kullanıldığını ve kimlerle paylaşıldığını kontrol etmesini de içerdiği belirtilmektedir. Dijital ortamda çocukların ve gençlerin korunması ve güçlendirilmesi bir diğer önemli başlık olarak karşımıza çıkmaktadır. Bu kapsamda çocuklar ve gençler, güvenli ve bilinçli seçimler yapabilmeleri ve dijital ortamda yaratıcılıklarını ifade edebilmeleri için güçlendirilmelidir. Günümüz dünyasının önemli konularından biri olan sürdürülebilirlik noktasında ise dijital ürünler ve hizmetlerin, çevreye önemli ölçüde zarar vermekten kaçınmak ve döngüsel bir ekonomiyi teşvik etmek için çevre ve toplum üzerindeki olumsuz etkilerini azaltacak ve erken eskimeyi önleyecek şekilde tasarlanması, üretilmesi, kullanılması, onarılması, geri dönüştürülmesi ve imha edilmesi önem arz etmektedir.

Çizilen bu genel politika çerçevesi, halihazırda birçok yasal düzenleme ile doldurulmuşken, bu düzenlemelere ayrıca her gün yenileri de eklenmektedir. Dolayısıyla bir sonraki aşamada öncelikle dijital haklara ilişkin mevcut yasal çerçeve izah edilecek, ardından Birlik Dijital Politikaları çerçevesinde öngörülen yeni düzenlemelere değinilecektir.

Halihazırda yürürlükte olan birincil mevzuat olarak elbette Avrupa Birliği Antlaşması'nın ('ABA') hükümleri dikkate alınmalıdır. Antlaşma'nın 2. maddesinde Birliğin temel hak ve özgürlüklerden oluşan bir değerler bütünü üzerine kurulu olduğu açıkça benimsenmektedir; 6. madde de ise Birlik Üye Ülkelerinin anayasal geleneklerinden kaynaklanan temel hak ve özgürlüklerin de Birlik hukukunun genel ilkelerinin bir parçası olduğu kabul edilmiştir. Avrupa Birliği Antlaşması'nın 6. maddesine göre Birliğin Kurucu Antlaşmalarıyla eşdeğer bağlayıcı niteliği haiz olan Avrupa Birliği Temel Haklar Şartı ise madde 7 kapsamında özel ve aile yaşamına saygı ile madde 8 kapsamında kişisel verilerin korunması haklarını bir temel hak ve özgürlük olarak açıkça düzenleme altına almıştır. Yine ilgili Şart madde 21 kapsamında ayrımcılık yasağına ilişkin bir hüküm öngörülmüştür. Her ne kadar birincil hukuk kaynaklarında belirtilen bu düzenlemeler çok soyut nitelikte olsa da bunların Birlik politikalarındaki yansımalarını görmek pekala mümkündür. Nitekim özellikle dijital politikalar bağlamında insan onurunu esas alan, insanı düzenlemenin merkezine oturtan, mahremiyet, kişisel verilerin korunması, hukuk devleti gibi ilkeleri benimseyen bütün politikalarda sözkonusu temel hakların tezahürünü görmek mümkündür.

İkincil mevzuat açısından gerçekleştirilecek incelemede ise sektör bazında bir ayırım yapmanın isabetli olacağı kanaati hasıl olmuştur.

Öncelikle altyapısal düzenlemeler açısından bağlanabilirlik (connectivity) alanında Frekans Bantları Direktifi (ETA) 1987/372, ardından Açık İnternet Erişimi Tüzüğü (EU) 2015/2120, Avrupa Elektronik Haberleşme Direktifi

(AB) 2018/1972, Dolaşım Tüzüğü (AB) 2022/612, Birlik Güvenli Bağlanabilirlik Programı Tüzüğü (AB) 2023/588 ve nihayet ".eu - Üst Seviye Alan Adı" Tüzüğü (AB) 2019/517 ile birlikte bağlanabilirlik için genel çerçeve çizilmiştir.

Veri koruma ve mahremiyet alanında ise elbette AB Genel Veri Koruma Tüzüğü 2016/679 sadece Birlik içerisinde değil, bütün dünya çapında bir standart oluşturmaktadır. Ancak bu alandaki Birlik düzenlemeleri elbette AB Genel Veri Koruma Tüzüğü ile sınırlı değildir. Bilakis sözkonusu Tüzük, bir taraftan Birlik kurum ve kuruluşlarının kişisel veri işleme faaliyetlerini esas alan Birlik Kurumları, Organları ve Ajansları Tarafından İşlenen Kişisel Verilerin Korunmasına İlişkin Tüzük 2018/1725 ile desteklenmektedir. Kolluk Direktifi 2016/680 sayesinde kolluk kuvvetlerinin kişisel veri işleme faaliyetlerine ilişkin özel bir düzenleme getirilmiştir. Sözkonusu düzenleme, AB Genel Veri Koruma Tüzüğü'nün tamamlayıcı bir parçasıdır. Elektronik iletişim çerçevesinde kişisel verilerin korunmasına ilişkin ise e-Mahremiyet Direktifi 2002/58/EC özellikle çerez kullanımı noktasında düzenlemeler içermektedir. Sözkonusu direktif, aslında AB Genel Veri Koruma Tüzüğü ile eş zamanlı olarak çıkartılması amaçlanan e-Mahremiyet Tüzüğü Önerisi ile yürürlükten kalkacaktı. Ancak üye ülkelerin taslak üzerinde halen bir uzlaşıya varamamaları sebebiyle 2002/58/AT, diğer bir deyişle eski Direktif halen yürürlüktedir. Bunun ötesinde kişisel veri niteliğini haiz olmayan verilerin serbest dolaşımına yönelik Kişisel Olmayan Verinin Serbest Akışı Tüzüğü (EU) 2018/1807 ve Açık Veri Direktifi (PSI) (EU) 2019/1024 yürürlüktedir. Sözkonusu düzenlemelerin amacı, kişisel verilerin korunmasının aksine kişisel veri niteliğini haiz olmayan verilere tedavül niteliği kazandırmaktır. Verilere tedavül niteliği kazandırmak ve verilerden dijital ekonomide daha fazla katma değer elde etmek amacıyla öngörülen bir diğer düzenleme, Veri Yönetişimi Yasası olarak anılan (AB) 2022/868 sayılı Veri Yönetişim Tüzüğü'dür. Sözkonusu Tüzük ile özellikle kamu sektörünün elinde bulundurduğu veri setlerinin ilgililere kullandırılmasının kolaylaştırılması amaçlanmaktadır. Bireylerin bağlantılı cihazlar vesilesiyle ürettiği verilere erişim yetkisini düzenleyen 2022/0047 (COD) sayılı Veri Yasası Önerisi ise henüz kabul sürecindedir. Veri Yasası ve Veri Yönetişimi Yasasıyla doğrudan bağlantılı olarak ayrıca Avrupa Sağlık Veri Alanı Tüzüğü de (2022/0140 (COD) kamunun elinde bulundurduğu sağlık verilerine güvenli bir ortamda ve kamunun denetim ve gözetimi altında erişimi mümkün kılmayı amaçlayan bir diğer düzenlemedir. Birlik müesseselerinin dijital alanda birlikte çalışabilirliğini amaçlayan bir diğer düzenleme ise Avrupa Birlikte Çalışabilirlik Tüzüğü'dür (Interoperable Europe Act) 2022/0379 (COD). Sözkonusu Tüzük henüz taslak aşamasında olmakla birlikte, Birlik müesseselerinin dijital alanda teknik, idari ve hukuki açıdan birlikte çalışabilirlik kıstaslarını esas almaktadır.

Fikri Mülkiyete ilişkin düzenlemelerde göze çarpan ilk düzenleme, Veri Tabanları Direktifi'dir (EC) 1996/9. Ardından Birlik Dizayn Direktifi (EC) 2002/6 ile Ticari Sırların Korunması Direktifi (EU) 2016/943 bu alandaki önemli düzenlemeler arasında öne çıkmaktadır. Beklenen düzenlemeler arasında ise Zorunlu Patent Lisansı Tüzük Önerisi 2023/0129 (COD) önem arz etmektedir.

Siber Güvenlik alanında ise Siber Güvenlik Yasası (EU) 2019/881, Avrupa Siber Güvenlik Sanayi, Teknoloji ve Araştırma Yetkinlik Merkezinin Kurulmasına İlişkin Tüzük (EU) 2021/887 ve elbette Şebeke ve Bilgi Güvenliği Direktifi (NIS 2) (EU) 2022/2555 önem arz etmektedir. Bu alanda beklenen düzenlemeler ise Bilgi Güvenliği Tüzük Önerisi 2022/0084 (COD), Siber Güvenlik Tüzük Önerisi 2022/0085 (COD), Siber Dayanıklılık Yasa Önerisi 2022/0272 (COM) ve nihayet Siber Dayanışma Yasa Önerisi 2023/0109 (COD) olarak nitelendirilebilecektir.

Ürün Güvenliği konusunda ise Genel Ürün Güvenliği Tüzüğü (EU) 2023/988 öne çıkmaktadır. Bunun yanında özellikle yapay zeka alanında heyecanla beklenen Yapay Zeka Yasa Önerisi 2021/0106 (COD) ile Yapay Zeka Sorumluluk Direktifi de 2022/0303 (COD) önem arz eden taslak düzenlemeler arasındadır.

E-Ticaret/Tüketicinin Korunması, her zaman Avrupa Birliği kanun koyucusunun önem verdiği konuların başında gelmektedir. Bu minvalde önceki düzenlemeler her ne kadar dijital alana mahsus düzenlemeler içermemekteyse de son dönemde özellikle dijital piyasaları ilgilendiren düzenlemelerin sayısı artmaktadır. Bunlara örnek olarak Geo-Blocking Tüzüğü (EU) 2018/302, Dijital İçerik Direktifi (EU) 2019/770 ve özellikle Dijital Hizmetler Yasası (EU) 2022/2065 önem arz etmektedir.

Rekabet hukuku alanında ise özellikle P2B- Tüzüğü (EU) 2019/1150 ile Dijital Piyasalar Yasası (EU) 2022/1925 dikkat çekmektedir. Her iki düzenleme de bilhassa dijital alana yönelik rekabetin düzenlenmesi amacıyla getirilen önemli düzenlemeler içermektedir.

Finans alanında ise Ödeme Hizmetleri Direktifi 2 (PSD2) (EU) 2015/2366 ile Dijital Varlıklar Tüzüğü (MICA) (EU) 2023/1114 dijital haklar alanında kayda değer iki önemli düzenleme olarak öne çıkmaktadır. Bunun haricinde Dijital Operasyonel Dayanıklılık Tüzüğü (DORA) (EU) 2022/2554'de doğrudan dijital piyasaları esas alan bir düzenlemedir. Yine Dijital Avro 2023/0212 (COD), Finans Verilerine Erişim Tüzüğü 2023/0205 (COD) ve Ödeme Hizmetleri Tüzüğü de 2023/0210 (COD) taslak halinde yasama sürecinde olan düzenlemeler arasındadır.

2. Seçilen Ülkeler

Birlik nezdinde dijital ekonomi alanında yaşanan bütün bu gelişmeler, dijital haklara ilişkin de doğrudan ya da dolaylı olarak birçok düzenleme içermektedir. Bu düzenlemelerin ulusal devletler düzeyinde yansımalarını incelemek amacıyla üç farklı ülke seçilmiştir. Bunlar Almanya, Avusturya ve İrlanda'dır.

Almanya'nın seçilmesindeki sebepler arasında elbette ilgili ülkenin ekonomik gücü, nüfusu ve Birlik hukukunun gelişimi açısından oynadığı önemli rol yer almaktadır. Özellikle veri koruma hukuku gibi alanlarda henüz Birlik nezdinde bir düzenleme mevcut değil iken çok daha önceden bu konuları hem mevzuat hem de içtihatlar bünyesinde düzenlemeye tabi tutmuş olması, Almanya mevzuatı ve uygulamasını incelemeye layık bir örnek kılmaktadır.

Almanya nüfus ve ekonomi açısından Birliğin en büyük ülkelerinden birini teşkil etmekle birlikte Avusturya da orta ya da hatta küçük ölçekli bir ülke örneği olarak önem taşımaktadır. Ancak Avusturya'nın seçilmesindeki ana etken, Avusturya uygulamasıdır. Şöyle ki son dönemde dijital haklar ve bilhassa kişisel verilerin korunması alanında Avrupa Adalet Divanı nezdinde görülen birçok dosya, Avusturya Yüksek Mahkemesi tarafından önsoru şeklinde iletilmektedir. Bunun sebebi de dijital haklar aktivisti Max Schrems ve organisazyonu "NOYB"nin Avusturya menşeli olmasıdır. Dolayısıyla özellikle uygulama açısından önem arz etmesi sebebiyle Avusturya örneği seçilmiştir.

Nihayet İrlanda'nın seçiliş sebebi, ilgili ülkenin 2000'li yılların başlarından bu yana çok uygun bir vergi politikası izlemesi ve bu sebeple küresel ölçekte faaliyet gösteren teknoloji şirketlerinin Avrupa üssü olarak bu ülkeyi tercih etmesidir. "Alphabet", "Meta", "TikTok" gibi pek çok teknoloji devlerine karşı soruşturmalar ve incelemelerin başlangıç noktası çoğu zaman İrlanda olmuştur. Bundan dolayı da İrlanda örneği özellikle incelenmeye layık görülmüştür.

3. Uyum için Üye Ülkeler Tarafından Çıkartılan Mevzuata İlişkin Bilgiler

Yukarıda belirtildiği üzere Avrupa Birliği, dijital alanda gerçekleştirdiği birçok düzenlemeyi eskiden Direktifler vesilesiyle gerçekleştirirken, bundan sonra tercih edilen yöntem artık Tüzüktür. Komisyon bu eğilime dair genellikle yeknesaklaştırma amacına Direktifle yeterince ulaşılamadığını gerekçe göstermektedir. Bunun en çarpıcı örneği, kişisel verilerin korunması alanında 95/46/EC Direktifinin güncellenmesi ve günümüz şartlarına uyarlanması aşamasında tercih edilen yöntemin Tüzük olmasıdır. Yine e-mahremiyet alanında getirilen 2002/58/EC Direktifi'nin güncellenmesi amacıyla da bir Tüzük öngörülmektedir. Veri Yönetişimi Yasası, Veri Yasası Önerisi, Yapay Zeka Yasa Önerisi da hep Tüzük şeklinde öngörülmektedir.

Bilindiği üzere Tüzük, Direktifin aksine üye ülkeyi muhatap alan, ona genel çerçevesi çizilen mevzuatı iç hukuka aktarma ödevi yükleyen bir norm niteliğini haiz değildir. Bilakis yeknesaklaştırma çerçevesinde en etkili, ancak üye ülkelere de en az takdir alanı tanıyan bu yöntemde Tüzük hükümleri, bütün üye ülkelerde doğruda uygulama alanı bulmaktadır. Hal böyle olunca AB hukukunun uygulandığı hallerde dijital haklar noktasında üye ülkelere tanınan takdir alanı bir hayli dardır. Tüzük doğrudan uygulama alanı bulacağı için üye ülkenin aynı alanda yasama faaliyetinde bulunacağı hususlar çok sınırlı kalmaktadır.

Çalışmada, dijital hakları doğrudan ilgilendiren ve belirli alanlara yönelik Birlik düzenlemelerini incelenmekte ve bu düzenlemelerin üye ülkelerdeki uygulamasına dikkat çekilmektedir. Bu seçili alanlar, kişisel verilerin korunması hukuku, veri yönetişimi hukuku, dijital piyasalar hukuku, elektronik ticaret hukuku ve siber güvenlik hukukudur. Hemen belirtelim ki bu alanların kat'i bir surette birbirinden ayrıştırılması da mümkün değildir. Bilakis sözkonusu alanlar birbirleriyle bağlantılı olduğu için birçok açıdan kesişimler gündeme gelecektir.

3.1. Kişisel Verilerin Korunması Hukuku

Birlik nezdinde kişisel verilerin korunmasını esas alan ilk genel düzenleme, mülga 95/46/EC Direktifidir. Sözkonusu direktif, henüz internetin her evde mevcut bulunmadığı, cep telefonları, tabletler ve hatta kişisel bilgisayarların henüz çok yaygın olmadığı, sosyal medyanın ise henüz ortaya çıkmadığı bir dönemde yürürlüğe girmiştir. Ancak özellikle 90'ların sonları ve 2000'li yılların başlarında kişisel bilgisayarların yaygınlaşması, internetin hemen hemen her eve girmesi ile birlikte yurtdışına aktarıma dair kuralların revize edilmesi gerektiği düşüncesi hasıl olmaya başlamıştır. Ekonomik alanda Avrupa'da faaliyet gösteren şirketlerin Amerikan şirketleriyle sıkı işbirliği, dijital alana taşındıkça, yine sözkonusu düzenlemenin önemi artmaya başlamıştır. Bunun belki en çarpıcı örneklerinden birisi, Alman otomotiv üreticisi Daimler AG'nin Amerikan Chrysler şirketiyle birleşmesi hadisesidir. Nitekim sözkonusu birleşme neticesinde birçok kişisel verinin Amerika Birleşik Devletleri'ne aktarımı zorunluluğu hasıl olmuş, bu sorunun çözülmesi için bugün AB Genel Veri Koruma Tüzüğü çerçevesinde açıkça düzenlenen "Bağlayıcı Şirket Kuralları", veri sorumluları ile üye ülke otoriteleri arasındaki işbirliği neticesinde kabul edilmiştir. Ardından sosyal medyanın gelişmesiyle kişisel verinin sadece yurtdışına aktarımı değil, aynı zamanda bu verilerin çok farklı amaçlarla ve özellikle ticari saiklerle analiz edilmesi sorunları baş göstermiştir. Bulut bilişimin sunduğu fırsatlar birçok ticari şirket için cazibeli olsa da, aynı zamanda veri koruma hukuku açısından birçok sorunu da beraberinde getirmektedir. İşte yaşanan tüm bu gelişmelere ilişkin bütün üye ülkelerin veri koruma otoritelerinin temsilcilerinden oluşan Madde 29 Çalışma Grubu,[1] ilkesel rehberler yayınlamış ve dolayısıyla uygulamaya ışık tutmuştur. Bu gelişmeler neticesinde nihayet ilgili Direktif'in revize edilmesi ihtiyacı hasıl olmuş, uzun tartışmalar neticesinde Mayıs 2016'da AB Genel Veri Koruma Tüzüğü yayımlanarak yürürlüğe girmiş ve üye ülkelere tanınan 2 yıllık geçiş süresinin sonunda 2018 yılında da uygulanmaya başlanmıştır.

Öncelikle Tüzük, genel mantık olarak kişisel verilerin korunmasına şekli bir prosedür olarak yaklaşmamaktadır. Bilakis Tüzük ile birlikte artık risk temelli bir yaklaşım kabul edilmektedir. Bu bağlamda hem kanunun muhatapları, hem de otoriteler açısından farklı ve yeni bir düzenleme yöntemi öngörülmektedir. Şöyle ki düzenleyici otoriteler, özellikle dijital alanda özel teşebbüsler kadar bilgi sahibi değildir. Sözkonusu bilgi asimetrisi ise emredici düzenleme mantığına aykırı düşmektedir. Zira düzenleyici otorite neyi düzenlediğini ve denetlediğini bilemedikten sonra düzenlemenin ve denetlemenin de bir anlamı kalmayacaktır. Öte yandan yine dijital alanda çoğu zaman birçok muhatabın sadece şeklen kanunun gerekliliklerini yerine getirdiğini, bunun ötesinde gerçekten de bir yaşam döngüsü kurmadığını tespit etmek mümkündür. Bu bir taraftan kamu otoriteleri ile özel teşebbüsler arasındaki bilgi asimetrisi, diğer yandan muhatapların şekli bir yaklaşımla yetinmeleri, düzenleme mantığında bir değişime sebebiyet vermiştir. Bu mantığa göre kanunun muhatabı öncelikle kendi faaliyetinden kaynaklanan riski kendisi belirleyecektir. Bu sayede bilgi asimetrisi riski asgari seviyeye indirilecektir. Peki veri sorumlusu veya veri işleyen, bu riski yanlış hesapladı ya da hiçbir şekilde hesaplamadıysa ne olacaktır? İşte bu aşamada Tüzük tarafından getirilen diğer çok önemli yeni bir ilke öne çıkmaktadır: hesap verebilirlik. Buna göre her ne kadar veri sorumlusu veya veri işleyen kendi riskini belirleyecekse de, veri koruma hukukuna aykırılık halinde ilgili otoritenin inceleme yapması halinde hesap verebilir halde olmalıdır. Bir diğer ifade ile hangi önlemi ne sebeple aldığını açıklayabilmeli, bunun hesabını verebilir durumda olmalıdır. Bu sayede klasik emredici düzenleme mantığının aksine her bir veri sorumlusu (ve veri işleyen), artık kendi riskini kendisi tespit edecek, bunu asgari seviyeye indirebilmek için gerekli önlemleri alacak ve gerektiğinde bunları belgeleyebilecek konumda olacaktır. Bu temel yaklaşımın AB Genel Veri Koruma Tüzüğü kapsamında birçok farklı yerde tezahürünü görmek mümkündür.

Öncelikle AB Genel Veri Koruma Tüzüğü'nün genel ilkeler kısmında hesap verilebilirlik açıkça bir genel ilke olarak zikredilmiştir. Dolayısıyla her türlü veri işleme faaliyetinde bu ilkeye riayet edilmesi gerekecektir. Ayrıca hesap verilebilirlik münhasıran otoritelere karşı hesap verilebilirlik olarak da anlaşılmamalıdır. Bilakis hesap verilebilirlik, kişisel verisi işlemeye konu olan ilgili kişiye karşı da önem arz etmektedir. Bu açıdan aydınlatma ve açık rıza metinlerinin anlaşılabilir olması, tasarım yoluyla gizlilik (privacy by design) ve başlangıçtan itibaren gizlilik (privacy by default) ilkelerinin dikkate alınması, mahremiyeti teşvik eden teknolojilerden (Privacy enhancing Technologies (PET)) istifade edilmesi, aynı zamanda ilgili kişi hakları ve dolayısıyla dijital haklar açısından da büyük önem arz etmektedir. Bu noktada AB Genel Veri Koruma Tüzüğü, ilgili kişiye açık rızasını her zaman geri alabilme hakkı yanında meşru menfaate dayalı kişisel veri işleme hallerinde itiraz hakkı tanımakta, ayrıca işlemeye konu olan kişisel verilerinin bir nüshasını talep etme yetkisi de öngörmektedir. Özellikle son husus, güncel ABAD kararları ışığında somutlaştırılmaktadır.

1 AB Genel Veri Koruma Tüzüğü'nün yürürlüğüyle birlikte sözkonusu çalışma grubu EDPB olarak yeniden şekillendirilmiştir.

AB Genel Veri Koruma Tüzüğü'nün risk temelli yaklaşımı benimsemesinin diğer yansımaları, idari ve teknik tedbirler kapsamında da önem arz etmektedir. Şöyle ki veri sorumlularının bazı durumlarda ve kamu otoritelerinin her halükârda Veri Koruma Görevlisi (Data Protection Officer (DPO)) bulundurma zorunlulukları, özellikle risk teşkil eden veri işleme faaliyetleri öncesinde Veri Koruma Etki Analizi (Data Protection Impact Assessment) yapma zorunlulukları, hep bu ilkenin bir tezahürüdür.

Hukuk güvenliğini artırmak ve standartlaşmayı/yeknesaklaşmayı teşvik etmek amacıyla Tüzük ayrıca veri koruma standartlarının ve sektör bazında Davranış Kurallarının (Codes of Conduct) geliştirilmesini de teşvik etmektedir. Bu sayede birçok soyut kavramı içeren Tüzük hükümleri, sözkonusu standartlar sayesinde somutlaştırılmakta, sektör bazında menfaatler dikkate alınmakta ve nihayet hukuk güvenliği tesis edilmektedir.

Ancak belirtildiği üzere kişisel verilerin korunmasına ilişkin düzenlemeler münhasıran AB Genel Veri Koruma Tüzüğü'yle sınırlı değildir. Bilakis diğer birçok alanda da özel düzenlemeler mevcuttur. Bunlardan en önemlisi ise Elektronik Haberleşme Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi ya da kısaca e-Mahremiyet Direktifi olarak adlandırılan 2002/58/EC Direktifidir. Özellikle terminal cihazlara yerleştirilen ve çerez olarak adlandırılan veri paketlerine ilişkin düzenlemeler içermesi sebebiyle sözkonusu Direktif uygulamada birçok tartışmaya da sebebiyet vermiştir. Yine Genel Veri Koruma Tüzüğü ile eş zamanlı olarak revize edilmesi amaçlanan Direktif, e-Mahremiyet Tüzük Önerisi üzerinde Üye Ülkelerin halen bir mutabakat sağlayamamaları sebebiyle güncellenememiştir.

3.1.1. Almanya

Alman hukukunda kişisel verilerin korunması alanında her eyaletin kendine mahsus bir veri koruma kanunu bulunmaktadır. Bunun yanında federal düzeyde Federal Veri Koruma Kanunu da (Bundesdatenschutzgesetz), AB Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesinden sonra uygulama alanı ciddi derecede sınırlanmış şekilde yürürlüktedir. Bu kapsamda özellikle istihdam ilişkilerinde kişisel verilerin korunması (§ 26), bilimsel ya da tarihi araştırmalar ile istatistik amaçlı veri işleme faaliyetleri (§ 27), kamu yararının bulunduğu arşiv faaliyetleri, tüketici kredileri (§ 30) ve kredi puanı hesaplanması faaliyetlerine ilişkin (§ 31) düzenlemeler halen uygulama alanı bulmaktadır.

E-mahremiyet Direktifinin iç hukuka yansıtılması noktasında ise 01.12.2021 tarihinde yürürlüğe giren Telekomünikasyon ve Telemedya Alanında Kişisel Verilerin Korunması Kanunu (Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien, TTDSG) mevcuttur. Bu düzenleme ile Planet49 kararı ışığında çerez işlenmesine dair açık rızanın opt-in yöntemiyle alınması gerektiği görüşü kanunlaşmıştır.

3.1.2. Avusturya

Tıpkı Alman hukukunda olduğu gibi Avusturya hukukunda da Gerçek Kişilerin Kişisel Verilerinin İşlenmesi Bağlamında Korunmasına İlişkin Federal Kanun (Datenschutzgesetz – DSG), AB Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesinin ardından daha çok kamu otoritelerinin veri işleme faaliyetlerini düzenlemekle yetinen ve bazı özel durumlar için (kamu yararının bulunduğu arşivleme faaliyetleri, bilimsel ya da tarihi araştırmalar ve istatistiksel amaçlar için veri işleme faaliyetleri) düzenlemeler öngören bir kanun niteliğiyle yürürlüktedir.

3.1.3. İrlanda

2018 tarihli İrlanda Veri Koruma Yasası da (Data Protection Act 2018) tıpkı Alman ve Avusturya hukukunda olduğu gibi AB Genel Veri Koruma Tüzüğü'nün yanında yürürlüktedir. İlgili düzenleme kamu kurum ve kuruluşlarının veri işleme faaliyetleri ile Veri Koruma Otoritesinin teşkilat yapısına dair hükümler içermektedir. Ayrıca sözkonusu Kanun, çocukların kişisel verilerinin korunmasına dair özel hükümler getirmektedir. Yine soruşturma ve kovuşturma aşamalarında özel nitelikli kişisel verilerin korunmasına ilişkin düzenlemeler de mevcuttur.

3.2. Veri Yönetişimi Hukuku

Veri denildiğinde hukuki düzenlemeler açısından yaklaşım bugüne kadar hep kişisel verilerin korunması olmuştur. Ancak dijital ekonominin en önemli hammaddesi veri olduğu için Avrupa Birliği, verileri sadece kişisel verilerle sınırlandırmak ve bunları da münhasıran korumaya yönelik düzenlemeler yapmanın bir aşama ötesine geçerek, özellikle kişisel veri niteliği haiz olmayan verilerin kullanımını teşvik etmeye yönelik önemli düzenlemeler öngörmüştür.

Bu düzenlemelerden ilki, Veri Yönetişimi Yasası'dır (EU) 2022/868. Henüz taslak aşamasında olan Veri Yasası 2022/0047 (COD) da büyük önem arz etmektedir. Her iki düzenlemenin amacı da özünde mevcut verilere tedavül niteliği kazandırmak, özellikle dijital ekonomi alanında faaliyet gösteren küçük ve orta ölçekli işletmeler ve girişimcilerin veriye erişimini kolaylaştırmak, aynı zamanda verinin doğrudan üreticisi olan bireylere de kendi ürettikleri veriler üzerinde tasarruf imkanı sağlamaktır.

Veri Yönetişimi Yasası, esasında üç temel amacı gütmektedir: (1) Kamunun elinde bulundurduğu verileri bireylerin erişimine sunmak, (2) Müşterek veri kullanımının genel çerçevesini çizmek ve (3) kamu yararına verilerin kullanımını (veri hayırseverliği) müessesesini ihdas etmek.

Hemen belirtelim ki üzerinde kimsenin hak iddia etmediği verilere erişim halihazırda Açık Veri Direktifi çerçevesinde düzenlenmektedir. Bununla birlikte Veri Yönetişimi Yasası, fikri haklar, ticari sırlar ya da kişisel verilerin korunması sebebiyle üçüncü kişilere sunulmasında tereddüt yaşanan verilerin erişime sunulması noktasında genel bir çerçeve çizmeyi amaçlamaktadır. Ancak ilgili Yasa, kamu otoritelerine verilerin erişime sunulmasına dair herhangi bir yükümlülük getirmemektedir. Otoriteler, gerekli her türlü tekniği kullanarak ve hukuki korumayı ihlal etmemek kaydıyla bu sayede ellerinde bulundurdukları verileri ilgili kişilerle paylaşabilmek için gerekli teknik ve idari altyapıyı oluşturabilecektir.

Ayrıca uygulamada halihazırda birden çok teşebbüs tarafından oluşturulan "veri havuzları" mevcuttur. Bunlar, özellikle aynı sektörde faaliyet gösteren aktörlerin aralarında bilgi paylaşımında bulunduğu bir mekanizma olarak karşımıza çıkmaktadır. Yasanın amacı, sözkonusu bilgi havuzlarının oluşumunu teşvik etmek, güvenli ortamlar oluşturmak ve bu sayede veriye erişimi kolaylaştırmaktır. Hatta bunun somut bir örneği olarak Avrupa Sağlık Veri Alanı Tüzük Önerisi (2022/0140 (COD)) yayımlanmıştır. İlgili taslakta kamunun denetimi altında sağlık verilerinin güvenli bir ortamda toplanması ve gerekli denetimler neticesinde ilgili kişilere sunulması amaçlanmaktadır.

Yine verilere tedavül niteliği kazandırmak amacıyla veri hayırseverliği müessesesinin kurulması ve geliştirilmesi, bu kapsamda bir sicil mekanizmasının kurulması, açık rıza metinlerinin oluşturulması da öngörülmektedir.

Son olarak ilgili yasada bütün denetim, gözetim ve özellikle koordinasyonu sağlamak üzere Avrupa Birliği Veri İnovasyon Kurulu'nun ihdas edilmesi öngörülmektedir.

Veri yönetişiminin kurumsal çerçevesini Veri Yönetişimi Yasası çizerken bireylerin kendileri tarafından üretilen verilere erişim imkanını sağlayan düzenleme ise Veri Yasasıdır. Uzun bir müzakere sürecinin sonunda Veri Yasası üzerinde uzlaşı sağlanmıştır. Yasanın 2023 yılı sonunda yasalaşması beklenmektedir.

Veri Yasasının temel amacı, bağlantılı ürün ya da hizmetler vesilesiyle cihazlardan elde edilen verilere, bunları "üreten" bireylerin erişim imkanı sahibi olmasıdır. Bu kapsamda bağlantılı ürün ya da hizmet, ya doğrudan üretilen verilere erişim imkanı sağlayacak, ya da bunun mümkün olmadığı hallerde birey, her zaman kendi kullanımı neticesinde elde edilen verilere her zaman erişim talep edebilecektir. Hatta bu verilerin doğrudan üçüncü kişilere aktarımı da aynı şekilde talep edilebilecektir. Bunun için üretici ile birey arasında elde edilecek ve erişime sunulacak verilere dair bir sözleşme yapılması öngörülmektedir. Dolayısıyla veri üreten herhangi bir bağlantılı ürün ya da cihaz satın alındığında alıcı ile üretici arasında bir "veri lisansı sözleşmesi" akdedilmesi gerekecektir. Sözkonusu verilerin bir üreticiden diğer bir üreticiye aktarımı halinde de yine bir lisans sözleşmesi akdedilmesi sözkonusu olacaktır.

Buradan çıkartılacak önemli bir sonuç şudur ki Avrupa Birliği, hukuk politikası bağlamında kabul edilen birçok amacı gerçekleştirmek için doğrudan özel hukuk kurallarına başvurmakta, özellikle sözleşme serbestisine müdahale edip tarafları sözleşme akdetmeye zorlamakta, aynı zamanda bu sözleşmenin asgari içeriğini de belirlemektedir. Nitekim üretici ile müşterinin talebi üzerine verinin aktarılacağı diğer üretici arasında akdedilmesi öngörülen veri lisansı sözleşmesine ilişkin Veri Yasası, haksız şartlar başlığı altında düzenlemeler içermektedir. Buna karşılık müşteri ile üretici arasında akdedilecek sözleşmeye dair özel bir düzenleme öngörülmemiştir. Bunun gerekçesi olarak genel işlem şartlarının düzenlendiği haksız şartları direktifinin halihazırda yeterli düzenleme içerdiği belirtilmektedir.

Veri ekonomisindeki aktörler arasındaki rekabetin güçlendirilmesi amacıyla ayrıca, müşterilere veri işleme hizmetleri sağlayıcıları arasında serbestçe geçiş yapabilmeleri için düzenlemeler getirilmiştir. Buna göre bir hizmet sağlayıcıdan diğerine geçişi sınırlandıran, zorlaştıran her türlü düzenleme geçersiz olarak kabul edilmektedir.

Nihayet ilgili Tüzük, farklı sistemler arasındaki geçişin kolaylaştırılması açısından birlikte-çalışabilirlik (interoperability) noktasında da önemli yükümlülükler öngörmektedir.

3.3. E-Ticaret ve Dijital Hizmetler

Elektronik ticaretin düzenlenmesinde temel düzenleme, 17 Temmuz 2000 tarihli Bilgi Toplumu Hizmetlerinin Bazı Hukuki Yönleri ve Özellikle İç Pazarda Elektronik Ticaret Konusunda 8 Haziran 2000 tarih ve 2000/31/EC sayılı Avrupa Parlamentosu ve Konsey Direktifidir (Elektronik Ticaret Direktifi) (Directive 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). Direktif'in Dibaceler kapsamında temel hak ve özgürlüklere etkisi bakımından şu ifadelere yer verilmiştir: (Dibace 9): "*Bilgi toplumu hizmetlerinin serbest dolaşımı pek çok durumda, tüm* Üye Ülke*ler tarafından onaylanmış bulunan Avrupa İnsan Hakları Sözleşmesini 10 maddesinin birinci fıkrasında öngörülen ifade özgürlüğü gibi genel prensiplerin, Topluluk hukukuna spesifik yansıması şeklinde ortaya çıkabilecektir. Bu nedenle bilgi toplumu hizmetlerinin sağlanmasına yönelik direktifler, bu madde ışığında sözkonusu eylemlerin özgürce yapılmasını garanti altına alacak nitelikte olmalıdır. Bu konuda tek sınırlama aynı maddenin 2 paragrafı ve Antlaşmanın 46 1 maddesi çerçevesinde öngörülmüştür ve ayrıca sözkonusu direktif, ifade özgürlüğü konusunda ulusal temel kural ve ilkelere halel getirmez*".

Direktifin amacı, Üye Ülkeler arasında bilgi toplumu hizmetlerinin serbest dolaşımını temin ederek, iç pazarın düzgün işleyişine katkı sağlamaktır. Buna göre iç pazara ilişkin bilgi toplumu hizmetlerine, hizmet sunucuların kuruluşuna, ticari iletişime, elektronik sözleşmelere, aracıların sorumluluğuna, davranış kurallarına (codes of conduct), yargı dışı uyuşmazlıkların çözümü yollarına, dava türlerine ve Üye Ülkeler arası işbirliğine ilişkin belirli ulusal hükümlerin yakınlaştırılması hedeflenmiştir.

Menşe ülke ilkesi olarak da kabul gören Direktif'in çok önemli bir ilkesine göre Üye Ülkeler, koordine alanlar kapsamına giren nedenlerle, bir başka Üye Ülkeden bilgi toplumu hizmetlerinin sunulmasını kısıtlayamazlar. Üye Ülkeler, bir bilgi toplumu hizmeti sunucusunun bu faaliyete başlamasının veya icrasını devam ettirmesinin önceden izin şartına veya eş etki doğuran başka bir şarta tabi tutulmamasını temin ederler.

Bu bağlamda getirilen bir diğer önemli yükümlülüğe göre Üye Ülkeler, kendi hukuk sistemlerinin, sözleşmelerin elektronik vasıtalarla akdedilmesine izin vermesini temin ederler. Üye Ülkeler, özellikle sözleşme sürecine uygulanan şartların elektronik sözleşmelerin kullanılmasına engel oluşturacak ya da bu çeşit sözleşmelerin elektronik vasıtalarla yapılmış olması nedeniyle hukuki etkiden ve geçerlilikten mahrum kalmalarına neden olacak şekilde uygulanmamasını temin edeceklerdir.

Benimsenen bir diğer önemli kural ise aracı hizmet sağlayıcıların sorumsuzluğuna ilişkindir.

Birlik nezdinde dijital hizmetleri esas alan ve dolayısıyla dijital hakları da doğrudan ilgilendiren düzenleme ise Dijital Hizmetler Yasası'dır (EU) 2022/2065 (Digital Services Act (DSA)). İlgili Tüzük ile birlikte dijital hizmet sağlayıcılarına yönelik önemli yükümlülükler getirilmiştir. Regülasyon tekniği açısından bu yükümlülükler, her hizmet sağlayıcı açısından eşit değildir. Bilakis büyük çevrimiçi platformlar olarak değerlendirilen ve GAFA (Google, Appale, Facebook ve Amazon) olarak nitelendirilen teşebbüsler açısından çok daha katı kurallar öngörülürken, daha küçük çaptaki teşebbüsler açısından daha basit yükümlülükler öngörülmektedir. Sözkonusu yükümlülükler özetle hukuka aykırı içeriği kaldırma yükümlülüğü, yasal temsilci atama yükümlülüğü, hizmetlere yönelik kısıtlamaların kullanım koşullarında yer alması ve bu kısıtlamaların objektif, ölçülü ve sorumlu bir şekilde uygulanması, içerik denetimi faaliyetlerine ilişkin şeffaflık yükümlülüğü, adli ve kolluk mercilerine ihbar yükümlülüğü, ticari kullanıcılarını tanıma yükümlülüğü (KYBC), reklam şeffaflığı yükümlüğü, risk değerlendirmesi yapma yükümlülüğü, bağımsız denetime tabi olma ve uyum görevlisi atama yükümlülüğü ile öneri sistemlerinin şeffaflığını sağlama yükümlülüğü olarak belirtilebilecektir. Yine bu yükümlülüklere aykırılık halinde önemli cezalar öngörülmektedir. Buna göre DSA'nın veya geçici tedbir/taahhüt kararlarının ihlali durumunda yıllık cironun %6'sına kadar para cezası verebilecektir. Ayrıca yanlış yanıltıcı bilgi verilmesi durumunda dünya çapındaki yıllık cironun %1'ine kadar para cezası verebilecektir. Ayrıca günlük para cezaları (uyum sağlanana kadar) aracı hizmet sağlayıcının günlük ortalama cirosunun %5'ini geçemeyecektir.

3.3.1. Almanya

Alman hukukunda elektronik ticareti düzenleyen yeknesak bir kanun mevcut değildir. Bunun yerine Alman Medeni Kanunu (Bürgerliches Gesetzbuch) içerisinde yer alan § 312 b ff BGB hükümleri bu konuyu düzenlemektedir. Bunun yanında Telemedya Kanunu (Telemediengesetz, TMG) da önemli düzenlemeler içermektedir. Bunun yanında İmza Kanunu (Signaturgesetz, SigG) ile Fiyat Bildirim Yönetmeliği (Preisangabenverordnung, PAngV) ve Tüketici İhtilaflarının Çözümlenmesi Kanunu da (Verbraucherstreitbeilegungsgesetz, VSBG) bu alanda önem arz eden düzenlemeler arasındadır.

3.3.2. Avusturya

Avusturya'da internet üzerinden mal ve hizmet satışı iki temel yasa ile düzenlenmektedir.

Uzaktan ve Çevrimdışı Satış Yasası (FAGG), Tüketici Hakları Direktifi'nin uygulanması sonucunda ortaya çıkmıştır ve bir girişimci ile bir tüketici arasında, girişimcinin işyerlerinde değil, uzaktan satış veya hizmet dağıtım sistemi (örneğin web siteleri) aracılığıyla yapılan veya genel olarak uzaktan yapılan her sözleşmeyi kapsamaktadır. FAGG, hem sözleşme öncesi hem de sözleşme sonrası bilgilendirme yükümlülüklerini (örneğin malın/hizmetin temel özelliklerinin tanımı, teslimat ve hizmet şartları) hem de tüketicinin cayma hakkını ortaya koymaktadır.

Elektronik Ticaret Yasası (ECG), Elektronik Ticaret Direktifi'nin uygulanması sonucunda Avusturya'da da oluşturulmuştur. ECG, hem genel bilgilendirme yükümlülüklerini (örneğin ad, adres, en az iki iletişim seçeneği, yetkili düzenleyici makam) hem de reklamda bilgilendirme yükümlülüklerini (örneğin reklamın açıkça tanınması, reklam verenin tanınması) hem de web sitelerinde bilgilendirme yükümlülüklerini (örneğin sipariş işleminin teknik adımlarının bilgisi) içermektedir.

Ek olarak, Şirketler Kanunu (UGB), Meslek Yasası (GewO) ve Medya Kanunu (MedienG) dahil olmak üzere diğer bilgilendirme ve açıklama yükümlülükleri de ortaya çıkmaktadır.

3.3.3. İrlanda

İrlanda'da 2000/31/EC Direktifini doğrudan iç hukuka yansıtan düzenleme, 2003 tarihli (S.I. No. 68/2003) - European Communities (Directive 2000/31/Ec) Regulations düzenlemesidir. Sözkonusu düzenleme, çevrimiçi faaliyet gösteren işletmeler için birtakım yükümlülükler getirmektedir. Bunlar arasında ürünlerini ve hizmetlerini açık ve doğru bir şekilde sunma, tüketicilerin siparişleri kolayca iptal etmelerine izin verme ve tüketicileri dolandırıcılıktan korumak için önlemler alma ihtiyacı yer almaktadır. Ayrıca müşterilerin kişisel verilerinin gizliliğini korumak için işletmelerin almaları gereken önlemler de düzenlenmektedir. Buna göre teşebbüsler, müşterilerin kişisel verilerini toplamadan veya kullanmadan önce onlardan izin almak ve bu verileri güvenli bir şekilde saklamakla yükümlü kılınmaktadır. Bu bağlamda özellikle şu yükümlülükler önem arz etmektedir:

Bilgilendirme yükümlülükleri: İşletmeler, ürünlerini ve hizmetlerini, kimliklerini, iletişim bilgilerini ve bulundukları coğrafi adresi de dahil olmak üzere açık ve doğru bir şekilde sunmalıdır. Ayrıca, sözleşmelerinin şartlarını ve koşullarını ve ödemeleri işleme koymak için kullandıkları yöntemleri de sunmalıdırlar.

İptal hakları: Tüketiciler, mal veya hizmet siparişlerini aldıktan sonra 7 gün içinde herhangi bir neden göstermeksizin iptal etme hakkına sahiptir. İşletmeler, tüketicilere iptal haklarını bildirmeli ve bu haklarını kullanmalarını kolaylaştırmalıdır.

Dolandırıcılığı önleme: İşletmeler, dolandırıcılığı önlemek için önlemler almalıdır, örneğin web sitelerinin güvenli olduğundan ve yetkisiz üçüncü taraflardan ödeme kabul etmediklerinden emin olmak gibi.

Veri koruma: İşletmeler, müşterilerinin kişisel verilerinin gizliliğini korumak için önlemler almalıdır. Bu, müşterilerin kişisel verilerini toplamadan veya kullanmadan önce onlardan izin almak ve bu verileri güvenli bir şekilde saklamak anlamına gelir.

3.4. Siber Güvenlik Hukuku

Dijital hakların korunması açısından önem arz eden siber güvenlik çerçevesinde Birlik düzeyindeki önemli düzenleme Şebeke ve Bilgi Güvenliği Direktifi'dir (NIS 1). Direktif, iç pazarın işleyişini iyileştirmek amacıyla Birlik içerisinde ağ ve bilgi sistemlerinin yüksek düzeyde ortak güvenliğinin sağlanması amacıyla tedbirler ortaya koymaktadır. Sözkonusu Direktif, başta özel hayata ve iletişime saygı hakkı, kişisel verilerin korunması, teşebbüs hürriyeti, mülkiyet hakkı, mahkeme önünde etkili başvuru hakkı ve dinlenilme hakkı olmak üzere Avrupa Birliği Temel Haklar Şartı tarafından tanınan temel hakları dikkate almaktadır. Bu husus Direktif'in uygulanması aşamasında da dikkate alınmalıdır.

Bu genel amaç çerçevesinde temel hizmet operatörleri tanımlanmaktadır. Bunlar enerji, elektrik, petrol, doğalgaz, ulaştırma, kara, demir, hava ve denizyolu taşımacılığı, bankacılık, finansal hizmetler altyapıları, sağlık sektörü, su yönetimi, dijital altyapılar, internet değişim noktaları (IXP), alan adı hizmet sağlayıcıları (DNS) ve üst seviye alan adı kayıtları (TLD) alanlarından ibarettir. Bu alanlarda faaliyet gösterenler temel hizmet operatörü olarak tanımlanmaktadır. Ayrıca dijital hizmet sağlayıcılar tanımlanmaktadır. Bunlar çevrimiçi pazarlar, bulut bilişim hizmetleri ve çevrimiçi arama motorlarıdır.

Sözkonusu aktörler, siber güvenliği sağlama yükümlülüğü altındadırlar. Buna göre riski önlemek veya etkilerini asgari düzeye indirmek için, riske uygun ve operasyonel tedbirler almakla yükümlüdürler. Ayrıca bu aktörler şebeke ve bilgi sistemlerinin güvenliğini sağlamak ve siber güvenlik olaylarını bildirmekle yükümlüdürler.

Şebeke ve Bilgi Güvenliği Direktifi (NIS 2) ise temel hizmet sağlayıcılar ile önemli hizmet sağlayıcıları, ardından yüksek kritik sektörleri tanımlamıştır. Bu sektörler enerji: elektrik, ısıtma ve soğutma, petrol, doğalgaz, hidrojen, ulaştırma: hava, demiryolu, su, karayolu, bankacılık, finansal piyasa altyapıları, sağlık, içme suyu, atık suyu, dijital altyapılar, bilişim hizmetleri yönetimi (b2b), kamu hizmetleri ve uzay sektörü olarak belirlenmiştir. Diğer kritik sektörler ise posta ve diğer taşıma hizmetleri, atık yönetimi, kimyasalların imalat, üretim ve dağıtımı, gıdaların üretimi, işlemesi ve dağıtımı, imalat, dijital sağlayıcılar ve araştırma olarak belirlenmiştir. Ayrıca yeni kapsama alanına dahil edilen sektörler ise elektronik haberleşme hizmet sağlayıcıları, sosyal ağ sağlayıcıları ve veri merkezi hizmetleri gibi dijital hizmetler, atık su ve atık yönetimi, bazı kritik ürünlerin imalatı (İlaç, medikal aletler ve kimyasallar), Posta ve taşıma hizmetleri, Gıda ve kamusal yönetim hizmetleridir.

Direktif kapsamında getirilen temel yükümlülükler ise **s**iber olay yönetimi ve kriz yönetimi, açık yönetimi ve ifşası, risk yönetim tedbirlerinin etkinliğinin değerlendirilmesi, basit bilişim hijyen uygulamaları ve siber güvenlik eğitimi, kriptografinin etkin şekilde uygulanması, insan kaynağı güvenliği, erişim kontrol politikaları ve varlık yönetimi şeklinde özetlenebilecektir.

Yaptırımlar konusunda ise €10 Milyon Euro'ya kadar idari para cezası ya da küresel cironun %2'sine kadar idari para cezası (hangisi yüksekse) uygulanabilecektir.

3.5. Yapay Zekâ Hukuku

Avrupa Komisyonu tarafından Nisan 2021'de yapay zeka sistemleri için yatay bir düzenleme öneren Yapay Zeka Yasa Önerisi (AI Act) 2021/0106 (COD) yayımlanmıştır. Yapay Zeka Yasası Önerisi, çerçevesinde Birlik içindeki yapay zeka sistemlerinin risk seviyelerine göre sınıflandırılması, temel hak ve özgürlüklerin korunması ve toplumun genel çıkarlarının gözetilmesi hedeflenmektedir. Ayrıca yapay zeka sistemlerinin etik, şeffaflık, hesap verilebilirlik ve insan merkezli olması gerektiği vurgulanmaktadır.

Bu amaçların gerçekleştirilebilmesi için ilgili düzenlemede farklı kurallar önerilmektedir. Bunlar özetle yapay zeka uygulamalarının temel hak ve özgürlükler bağlamında sebep olabileceği riskleri ele almak, yüksek riskli YZ uygulamalarının sınıflandırılması, yüksek riskli YZ uygulamaları için net gereksinimlerin belirlenmesi, yüksek riskli YZ uygulamalarının sağlayıcıları için özel yükümlülüklerin tanımlanması, YZ uygulamalarının hizmete girmeden veya piyasaya sürülmeden önce bir uygunluk değerlendirilmesine tâbi tutulması, YZ uygulamalarının piyasaya sürüldükten sonra da devam eden risk değerlendirmelerinin yapılması, Birlik ve ulusal düzeyde bir yönetişim yapısının kurulması şeklindedir.

Bütün dünya çapında ilk kapsamlı ve genel yapay zeka düzenlemesi girişimi olan Yapay Zeka Yasası, gelecekteki YZ düzenleyici yaklaşımları için de kritik bir emsal oluşturacaktır. Nitekim ilgili düzenleme kapsamında öne çıkan bazı unsurlar, diğer kanun koyucular açısından da ışık tutucu niteliktedir. Bunlar risk temelli bir yaklaşımın uygulanması, tasarının yapay zekayı ne kadar geniş tanımlayacağı, bireylere, işletmelere tanıdığı hakların kapsamı, yapay zeka sistemlerinin karmaşıklığı ve karar verme süreçleri göz önüne alındığında sorumluluğun belirlenmesi, bir düzenlemenin ne derece "geleceğe dönük" olması gerektiği, risk kategorilerinin genişliği ve yasaklanan yapay zeka kullanım durumları ile büyük teknolojinin çıkarları ile kamu yararının nasıl dengeleneceği hususlarıdır.

Bu genel açıklamalar ışığında Taslak, YZ uygulamaları için 4 risk seviyesi tanımlamaktadır:

a. Kabul edilemez risk

Hükümetler tarafından yapılan sosyal puanlamadan, tehlikeli davranışları teşvik eden sesli yardım kullanan oyuncaklara kadar, insanların güvenliği, geçim kaynakları ve hakları için açık bir tehdit olarak görülen tüm yapay zeka sistemleri yasaklanacaktır.

b. Yüksek risk

Yüksek riskli YZ sistemleri, kritik altyapılar, eğitim, ürün güvenliği, istihdam, kamu hizmetleri, kolluk kuvvetleri, göç, adalet ve demokratik süreçler dahil olmak üzere çeşitli alanları kapsamaktadır. Bu sistemler pazara girmeden önce katı yükümlülükleri yerine getirmelidir.

c. Sınırlı risk

Sınırlı risk, belirli şeffaflık yükümlülükleri olan YZ uygulamalarını ifade eder. Sohbet robotları gibi YZ sistemlerini kullanırken, kullanıcılar bir makine ile etkileşime girdiklerinin farkında olmalıdır, böylece devam etmek veya geri adım atmak için bilinçli bir karar alabilirler.

d. Minimal veya Sıfır Risk

Çerçeve, minimum riskli yapay zekanın serbestçe kullanılmasına izin vermektedir. Bu, yapay zeka destekli video oyunları veya spam filtreleri gibi uygulamaları içerir. Şu anda AB'de kullanılan YZ uygulamalarının büyük çoğunluğu bu kategoriye girmektedir.

Yukarıda zikredilen dört farklı risk kategorisinden Tüzük açısından en önemlisi elbette yüksek riskli yapay zeka sistemlerine ilişkindir. Nitekim bu çerçevede ağır yükümlülükler öngörülmektedir. Bu yükümlülüklerin üç ana kategoriye ayrılması mümkündür. Bu kategoriler, uygunluk değerlendirmeleri, teknik altyapı ve denetim ile pazarlama sonrası izleme gereklilikleri olarak belirtilebilecektir.

Öngörülen yükümlülüklerin önemli bir kısmının muhatabı ise YZ sistemini piyasaya süren veya piyasaya sürülmüş ürünün üzerinde önemli değişiklikler yapay ve sağlayıcı olarak tanımlanan gerçek ya da tüzel kişidir. Ancak Taslak, YZ sistemlerinin bütün yaşam döngüsünü esas aldığı için kullanıcılar, ithalatçılar, distribütörler ve onaylanmış kuruluşların da sorumlulukları öngörülmektedir.

Sözkonusu yükümlülüklere uyumun denetimi noktasında ise Üye Ülkeler, denetim organlarının uygulamaları ve yaptırımlarından sorumlu olacaktır. Ayrıca bu bağlamda ulusal denetim organlarına tavsiyelerde bulunmak üzere Üye Ülkeler ve Komisyon temsilcilerinden oluşan bir "Avrupa Yapay Zeka Kurulu" ihdas edilecektir. Bu Kurul, "bu tüzüğün uygulanmasıyla ilgili konularda" görüş bildirecek ve tavsiyelerde bulunacaktır. Ayrıca Kurul, toplantılarına katılmaları ve ilgili üçüncü taraflarla görüş alışverişinde bulunmaları için dışarıdan uzman ve gözlemcileri davet edebilecektir.

Yaptırımlar noktasında ise risk kategorisine göre bir mekanizma öngörülmektedir. Buna göre en ağır para cezaları, 35 milyon Euro'ya veya %7 ciroya kadar olup yasaklı YZ sistemlerinin kullanılmasında uygulanacaktır. Yüksek riskli YZ sistemleri için yükümlülüklerin ihlalinde ise üst sınır 15 milyon Avro veya cironun yüzde 3'üdür. Ulusal kurumlara doğru ve eksiksiz bilgi verilmemesi 7.5 milyon Avro'ya veya cironun yüzde 1,5'sine kadar para cezasına neden olabilir. Önemle vurgulamak gerekir ki, henüz düzenleme tasarı aşamasındadır ve bu yaptırımlar değişikle uğrayabilir. Tasarı üzerinde hem AB Konseyi hem de Parlamento arasında uzlaşı sağlanmış olup 2024 yılı içerisinde önerinin yasalaşaması beklenmektedir.

4. Birlik Nezdinde ve Ulusal Düzeyde Kurumsal Yapılanmalar

Belirtildiği üzere dijital ekonomi alanında getirilen birçok düzenleme, artık Tüzük şeklindedir. Bu düzenlemeler kapsamında da yeni Avrupa Birliği yapılarının ihdas edilmesi öngörülmektedir. Bu sebeple öncelikle yukarıda etraflıca değinilen alanlarla ilgili ihdas edilmesi öngörülen kurumlara değinilecektir. Ancak bu kurumlar, doğrudan yaptırım uygulamak yerine daha çok düzenleyici faaliyetlerde bulunmakta, Üye Ülkelerin farklı otoriteleri arasındaki koordinasyonu sağlama görevi üstlenmektedir. Dolayısıyla AB hukukunun Üye Ülkelerde uygulanması noktasında devletlerdeki kurumsal yapılar halen büyük önem taşımaktadır. Bu sebeple aşağıda, seçilen ülkeler bazında veri hukuku, elektronik ticaret ve dijital hizmetler ile siber güvenlik alanlarındaki kurumsal yapılar incelenecektir.

4.1. Mevcut ve Kurulması Öngörülen AB Kurumları

Yukarıda etraflıca izah edilen AB düzenlemelerinde birçok alanda yeni kurumların ihdas edilmesi öngörülmektedir. Bu kurumlar, ilgili regülasyonlar çerçevesinde şu şekildedir:

Yapay Zeka Yasa Önerisi çerçevesinde bir Avrupa Yapay Zeka Kurulu'nun (European Artificial Intelligence Board) kurulması öngörülmektedir. Veri yönetişimi noktasında ise Veri Yönetişimi Yasasında kurulması öngörülen kurum, Avrupa Veri İnovasyonu Kurulu'dur (European Data Innovation Board). AB Genel Veri Koruma Tüzüğü kapsamında ise halihazırda Avrupa Veri Koruma Kurulu (European Data Protection Board-EDPB) ile Avrupa Veri Koruma Denetçisi (European Data Protection Supervisor-EDPS) mevcuttur. Siber güvenlik alanında ise Avrupa Siber Güvenlik Sanayi, Teknoloji ve Araştırma Yetkinlik Merkezi ile Avrupa Siber Güvenlik Ajansı (ENISA) yetkili kuruluşlar olarak önem arz etmektedir.

4.2. Almanya

Almanya'nın federe devlet yapısı sebebiyle veri koruma hukukunda her bir federe devletin kendi veri koruma otoritesi bulunmaktadır. Bu eyalet otoriteleri, kendi eyaletleri içerisinde veri koruma faaliyetlerinin denetimi ve gözetiminden sorumludurlar. Ayrıca federal düzeyde de Federal Veri Koruma Otoritesi mevcuttur. Ancak Almanya uygulamasında düzenleyici işlemler, denetimler ve özellikle yaptırımlar noktasında eyalet otoriteleri ön plana çıkmaktadır.

Sözkonusu eyalet otoriteleri, AB Genel Veri Koruma Tüzüğü'nün uygulanması noktasında doğrudan yetkilidirler. Bununla birlikte AB Genel Veri Koruma Tüzüğü'nün "opening clause" çerçevesinde üye ülkelere düzenleme yapma yetkisi sunduğu istisnai haller açından da yetkili otoriteler, yine ilgili eyalet veri koruma otoriteleridir.

Otoriteler arasındaki işbirliğini sağlamak amacıyla ayrıca Datenschutzkonferenz (DSK) adlı bir organizasyon mevcuttur. Bu organizasyon, tıpkı EDBP gibi tavsiyelerde bulunmakta, kararlar almakta, farklı otoriteler arasındaki koordinasyonu sağlamakta ve uygulamaya ışık tutacak rehberler yayımlamaktadır.

Veri yönetişimi noktasında ise henüz Almanya düzeyinde bir otorite belirlenmemiştir. Bu kapsamda öncelikle kamunun elinde bulundurduğu veriler açısından yönetişimi düzenleyecek merkezi bir kurumun belirlenmesi gerekecektir. Ayrıca veri aracılık hizmetlerinin denetimi ve gözetimi için de ayrı bir kurumun belirlenmesi gerekecektir. Ancak bu kurumun veri koruma, rekabet ve siber güvenliğe ilişkin otoritelerden farklı bir otorite olması gerekecektir (Art. 13 f. 3 DGA). Nihayet veri hayırseverliği noktasında da bir sicilin kurulması ve yetkili bir otoritenin belirlenmesi gerekecektir.

Elektronik ticaret ve dijital hizmetler alanında ise birçok farklı kurumun yetkisi sözkonusudur. Bunlardan ilki, telekomünikasyon ve telemedya kanunları çerçevesinde yetkili kılınan Federal Ağ Ajansı'dır (Bundesnetzagentur). Bunun yanında ödeme hizmetleri açısından Finansal Hizmetler Denetim Kurumu (Finanzdienstleistungsaufsicht, BaFin), haksız rekabete ilişkin Federal Rekabet Kurumu (Bundeskartellamt), tüketici hakları açısından Tüketicinin Korunması ve Gıda Güvenliği Bakanlığı (Bundesamt für Verbraucherschutz und Lebensmittelsicherheit) ve

nihayet siber güvenlik açısından Federal Bilgi Teknolojileri Güvenliği Ajansı (Bundesamt für Sicherheit in der Informationstechnik, BSI) yetkili kuruluşlardır.

Siber güvenlik noktasında yetkili kuruluş, belirtildiği üzere Federal Bilgi Teknolojileri Güvenliği Ajansı'dır (Bundesamt für Sicherheit in der Informationstechnik, BSI). Bilgi Teknolojileri Güvenliği Ajansı, Almanya'nın içişleri bakanlığına bağlı bir federal üst kurumdur. BSI, Almanya'da bilgi teknolojisi sistemlerinin ve ağlarının güvenliğinden sorumludur. Özel teşebbüslere, kamu otoritelerine ve bireylere danışmanlık, destek ve eğitim sunmaktadır. Ayrıca güvenlik standartları ve yönergeleri geliştirmekten de sorumludur. Bu kapsamda BSI, şirketlere, idarelere ve bireylere bilgi güvenliği konusunda danışmanlık ve destek sağlamak, güvenlik standartları ve yönergeleri geliştirmek, bilgi güvenliği denetimleri yapmak, bilgi güvenliği risklerine karşı uyarıda bulunmak ve bilgi güvenliği konusunda halkı bilinçlendirmekle görevlidir.

4.3. Avusturya

Veri koruma hukuku alanında Avusturya'da yetkili merci önceden Veri Koruma Komisyonu idi (Datenschutzkommission). Ancak sözkonusu otoritenin organizasyonel açıdan Adalet Bakanlığı'na bağlı olması sebebiyle Adalet Divanı, 16.10.2012 tarihli kararıyla sözkonusu otoritenin bağımsız olmadığına ve dolayısıyla 95/46/EC Direktifine uyumlu olmadığına hükmetmiş, bunun üzerine Avusturya'da tamamen bağımsız bir otorite olan Veri Koruma Kurumu (Datenschutzbehörde) ihdas edilmiştir. Veri Koruma Kurumu, Avusturya'da veri koruma düzenlemelerine ve ceza soruşturmaları için veri koruma mevzuatına uygun olarak kurulan veri koruma otoritesidir. Veri Koruma Kurumu, görevlerini yerine getirirken ve yetkilerini kullanırken tamamen bağımsızdır. Veri Koruma Kurumu'nun çeşitli görevleri arasında, özellikle veri koruma şikayetleri, resmi incelemeler ve idari yaptırım soruşturmaları yürütmek ve AB veya Avrupa Ekonomik Alanı (AEA) içinde sınır ötesi durumlarda diğer veri koruma otoriteleriyle işbirliği yapmak yer almaktadır. Veri Koruma Kurumu'nun kararlarına karşı temyiz ve şikayet makamı olarak Federal İdare Mahkemesi sorumludur. Federal İdare Mahkemesi, Veri Koruma Kurumu'nun kararlarının yanı sıra şikayetçilerin şikayetlerini ve Veri Koruma Kurumu'nun karar verme yükümlülüğünü yerine getirmemesi durumunda temyizleri değerlendirir.

Veri yönetişimi hukuku için Almanya çerçevesinde yapılan açıklamalar Avusturya açısından da geçerlidir.

E-ticaret alanında ise E-ticaret yasası (Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz – ECG), § 30 kapsamında elektronik ticari iletiler bağlamında Trafik, İnovasyon ve Teknoloji Bakanlığı'nı, şeffaflık ve diğer kurumlarla işbirliği noktasında Adalet Bakanlığı'nı ve diğer bütün yükümlülükler açısından Adalet Bakanlığı ile Ekonomi ve İstihdam Bakanlığı'nı yetkili kılmaktadır.

Nihayet siber güvenlik noktasında toplam dört farklı kurumun yetkisi mevcuttur. Bunlar Başbakanlık, İç işler Bakanlığı, Savunma Bakanlığı ve Avrupa ve Dış İlişkiler Bakanlığı'dır.

4.4. İrlanda

İrlanda'da veri koruma alanında yetkili olan kurum, Veri Koruma Komisyonu'dur (Data Protection Commission). Komisyonun yetki alanına dahil olan düzenlemeler, AB Genel Veri Koruma Tüzüğü ve Kolluk Direktifi yanında İrlanda'nın e-mahremiyet alanındaki düzenlemesi olan 2011 tarihli İrlanda eMahremiyet Tüzüğüdür (ePrivacy Regulation). Otoritenin görev ve yetkileri ile kuruluşuna ilişkin hususlar, 2018 tarihli Veri Koruma Kanunu 9 ila 27.maddeler kapsamında belirlenmiştir.

Elektronik ticaretin düzenlenmesi alanında yetkili kılınan otorite ise Teşebbüs, Ticaret ve İstihdam Bakanlığı'dır (Ministry for Enterprise, Trade and Employment).

Siber güvenlik noktasında ise İrlanda Ulusal Siber Güvenlik Merkezi (National Cyber Security Center) önem arz etmektedir. Ulusal Siber Güvenlik Merkezi (NCSC), 2011 yılında kurulmuş olup, ağ ve bilgi güvenliği ile ilgili hükümet birimidir. NCSC'nin rolü, büyük siber güvenlik olaylarının yönetiminde liderlik etmek, vatandaşlara ve işletmelere rehberlik ve tavsiye vermek ve kilit hizmetlere yönelik siber güvenlik risklerini yönetmektir. Diğer AB üye ülkelerindeki benzer kuruluşlar gibi, NCSC de bir dizi alanda daha proaktif bir yaklaşım benimsemeye başlamıştır. NCSC'nin bir parçası olan Bilgisayar Güvenlik Olay Müdahale Ekibi (CSIRT), devlette risk ve olay

yönetimini üstlenmektedir. Sorumlulukları arasında devlet kurumları içinde meydana gelen olayları izlemek, ilgili paydaşlara risk ve olaylar hakkında erken uyarılar, alarmlar, duyurular ve bilgi yaymak, bildirildikleri olaylara yanıt vermek ve dinamik risk ve olay analizi ve durumsal farkındalık sağlama faaliyetleri bulunmaktadır.

5. Uygulamadan Örnekler

Her ne kadar Avrupa Birliği, hukuki açıdan getirilen düzenlemelerin yeknesaklaştırılması amacıyla Tüzük yöntemini tercih etmekteyse de, bu düzenlemelerin uygulanmasında elbette Üye Ülke otoriteleri ve bunların uygulamaları büyük önem arz etmektedir. Bu sebeple bu bölümde üye ülkeler nezdinde dijital haklar bağlamında meydana gelen ve bilhassa Birlik nezdinde tartışmalara konu olan olaylar incelenecektir.

5.1. Almanya

Dijital haklar bağlamında Almanya'da yaşanan ve Avrupa Adalet Divanı'na kadar uzanan çeşitli kararlar önem arz etmektedir.

Bunlardan ilk ikisi, Facebook-Fanpage (C-210/16 - Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH) ile Fahsion-ID (C-40/17 - Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV) kararlarıdır. Facebook-Fanpage kararında bir eğitim teşebbüsü Facebook üzerinden çeşitli eğitim faaliyetleri sunmakta, Fashion-ID kararında ise bir ticari teşebbüs, kendi web sitesinde Facebook-Like Button kullanmak suretiyle ziyaretçi verilerinden bazılarını doğrudan Facebook'a aktarmaktadır. Buna karşılık Facebook ise bu kişilerle siteyi ziyaret eden kişiler hakkında istatistiksel veriler paylaşmakta, ancak ziyaretçilerin kimliği ya da onları belirlenebilecek kılan herhangi bir veri paylaşmamaktadır. Her iki durumda da ilgili veri koruma otoriteleri, ilgili site işleticilerinin Facebook ile birlikte sorumlu olduklarından hareketle işlem yapmıştır. Bunun üzerine itiraz yoluna giden muhatapların başlattığı yargılama süreci Avrupa Adalet Divanı'na kadar uzanmıştır. Divan, her ne kadar web sitesi işleticilerinin doğrudan ziyaretçi bilgilerine sahip olmasalar da Facebook ile birlikte ticari bir amaç gütmeleri sebebiyle ortak veri sorumlusu olduklarına kanaat getirmiştir.

Özellikle çevrimiçi ortamları ilgilendiren bir diğer gelişme ise Planet-49 (C673/17 - Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH) kararıdır. Sözkonusu kararda 2002/58/EC Direktifini iç hukuka aktarmasına rağmen Alman hukukunda çerezlere ilişkin açık rızanın opt-in yöntemiyle mi, opt-out yöntemiyle mi alınması gerektiği hususu tartışmalıydı. İlgili kararda Divan, açık bir şekilde AB Genel Veri Koruma Tüzüğü ve e-Mahremiyet Direktifi bağlamında alınması gereken rızanın zımnen olamayacağına, bilakis ilgili kişinin aktif bir davranışının gerekli olduğuna hükmetmiştir. Bu karar neticesinde Birlik nezdinde birçok web sitesinde zorunlu, istatistiksel ve pazarlama amaçlı çerezler arasında bir ayırıma gidilmiş, son iki çerez kategorisi açısından açık rıza verme ya da bu çerezleri reddetme imkanı kullanıcılara sunulmaya başlanmıştır.

Önem arz eden bir diğer gelişme ise yine Genel Veri Koruma Tüzüğü bağlamında uygulanan yaptırımlara ilişkindir. Şöyle ki Berlin Veri Koruma Otoritesi, Deutsche Wohnen SE ünvanlı şirket aleyhine 15 Milyon € para cezası uygulamıştır. Karara itiraz sonrası başvurulan Berlin Eyalet Mahkemesi ise Alman Kabahatler Kanunu çerçevesinde bir tüzel kişi aleyhine yaptırım uygulayabilmek için öncelikle gerçek kişi sıfatıyla ilgili tüzel kişinin organı ya da temsile yetkili bir gerçek kişinin kusurunun tespit edilmesi gerektiğine hükmetmiş, bu gerekçeyle para cezasını bütünüyle kaldırmıştır. Hükmün istinaf aşamasında Berlin Eyalet Yüksek Mahkemesi önsoru çerçevesinde olayı Avrupa Adalet Divanı'na taşımıştır (C-807/21). Divan henüz nihai bir karar vermemiştir. Ancak ilgili dosyadaki savcı mütalaasında tüzel kişilerin de doğrudan Genel Veri Koruma Tüzüğünde öngörülen yaptırımlara muhatap olabileceği, ayrıca yönetim organının bir üyesi olmayan ya da temsil yetkisini haiz olmayan kişilerin de fiillerinden dolayı tüzel kişilerin sorumlu kılınabileceğini belirtmiştir. Bunun için objektif bir ihlalin yeterli olduğu da savunulmuştur. AB Genel Veri Koruma Tüzüğü ve diğer düzenlemelerde öngörülen yaptırımların hukuki niteliğine dair bu önemli tartışma, sadece veri koruma hukuku açısından değil, ağır yaptırımlar öngören dijital alandaki bütün düzenlemeler açısından büyük önem arz etmektedir.

Almanya açısından önem arz eden bir diğer husus, Meta ile Alman Rekabet Kurumu (Bundeskartellamt) arasındaki ihtilafa ilişkindir. Meta'nın Facebook, Whatsapp ve Instagramm'dan elde ettiği verileri birleştireceğini duyurmasının

akabinde Alman Rekabet Kurumu bu faaliyeti yasaklamış, ardından Meta yargı yoluna başvurmuştur. Yaşanan ihtilaf neticesinde Avrupa Adalet Divanı, çok güncel bir kararında (C-252/21 - Meta Platforms and Others) rekabet otoritelerinin de veri koruma hukukundan kaynaklanan ihlaller çerçevesinde yetkili olabileceğine hükmetmiştir. Dolayısıyla veri koruma hukuku, münhasıran veri koruma otoritelerinin yetki alanıyla sınırlandırılmamış, rekabeti bozucu ve haksız rekabet teşkil eden davranışlar halinde rekabet kurumunun yetkili olabileceği hususu açıklığa kavuşturulmuştur.

5.2. Avusturya

Avusturya uygulamasında veri koruma hukuku ile e-ticaret alanında önemli gelişmeler yaşanmıştır. Bu gelişmelerden ilki, Avrupa Birliği Adalet Divanı'nın C-300/21 – Österreichische Post/UI kararına ilişkindir. İlgili kararda incelenen hukuki sorun, Genel Veri Koruma Tüzüğüne aykırılığın başlı başına tazminata hükmedilebilmesi için yeterli olup olmadığına ilişkindir. Divan ilgili kararında salt Genel Veri Koruma Tüzüğüne aykırılığın maddi ya da manevi tazminat talepleri açısından yeterli olmayacağına, hukuka aykırı fiilin bir zarara sebebiyet vermesi gerektiği ve haksız fiil ile zarar arasında illiyet bağının bulunması gerektiğine hükmetmiştir. Bu bağlamda her türlü olumsuz duygu/düşünce/hissiyatın zarar teşkil etmeyeceğini belirten Divan, ayrıca üye ülkelerin yetkili mahkemelerinin tazminat hesaplamaması yaparken denklik ve işlevsellik ilkelerini dikkate alması gerektiğini de vurgulamıştır. Dijital haklar bağlamında bu karar özellikle önem arz etmektedir. Nitekim veri koruma hukukunda bireylerin hak ve hürriyetlerinin etkin bir şekilde korunabilmesi için bir taraftan idari otoritelere yaptırım uygulama yetkisi tanınırken, diğer yandan bireylere de ihlallere karşı tazminat talep etme yetkisi tanınmaktadır. İşte bireylerin bu talepleri kapsamında işlevsel bir tazminat mekanizmasının mevcut olmadığı hallerde birey hak ve hürriyetlerinin etkin bir şekilde korunması sözkonusu olmayacaktır. Bu duruma işaret eden Divan kararı, bu açıdan büyük önem taşımaktadır.

Yine Avusturya Yüksek Mahkemesi tarafından Avrupa Adalet Divanı'na taşınan bir diğer uyuşmazlık kapsamında (C-487/21 – Österreichische Datenschutzbehörde/CRIF GmbH) ilgili kişiye tanınan haklar incelemeye konu olmuştur. İlgili kararda AB Genel Veri Koruma Tüzüğü madde 15 f. 3 c. 1'e göre ilgili kişinin kişisel verilerinin bir nüshasını talep etme hakkının kapsamı değerlendirilmiştir. Tüzüğün yürürlüğe girdiği dönemden bu yana tartışma konusu olan bu hak, Divan tarafından geniş bir şekilde yorumlanmıştır. Divan'a göre ilgili kişinin haklarını kullanabilmesi için gerekli olduğu takdirde, işlemeye konu olan kişisel verilerin bir nüshasını talep etme hakkı, sözkonusu kişisel verileri içeren belge ya da veri tabanının ilgili kısımlarının ya da belgenin tümünün sunulması yükümlülüğünü de kapsayabilir. Zira ancak bu takdirde ilgili kişi Tüzükten kaynaklanan haklarını etkin bir şekilde kullanabilecektir. Her ne kadar ilgili karar veri sorumluları bağlamında operasyonel, mali ve personel olarak ek yükümlülükler getirse de bireylerin Tüzükten kaynaklanan haklarını işlevsel bir şekilde kullanabilmeleri açısından büyük önem taşımaktadır.

Avusturya hukukuyla bağlantılı bir diğer önemli gelişme, çevrimiçi platformların sunduğu dijital hizmetlere ilişkindir. Sözkonusu ihtilaf kapsamında Avusturya'da 2020 yılında yürürlüğe giren iletişim platformları yasası, büyük sosyal medya platformlarına raporlama, temsilci atama gibi yükümlülükler getirmekte, aykırı davranış halinde ise milyon avrolara varan cezalar öngörmektedir. Bu düzenleme, 5651 sayılı Kanun kapsamında sosyal ağ sağlayıcılarına getirilen yükümlülüklere benzerlik teşkil etmektedir. Büyük platform niteliğini haiz olan Google Ireland Limited, Meta Platforms Ireland Limited ve Tik Tok Technology Limited ise, sözkonusu düzenlemelerin, 2000/31/EC no.lu Elektronik Ticaret Direktifi md. 3 f. 2 kapsamında kabul edilen menşe ülke ilkesine aykırılık teşkil ettiğini savunmaktadır. Nitekim İrlanda'da yerleşik olan bu şirketlerin İrlanda kanunlarına uyum göstermelerinin yeterli olduğunu, her bir üyede temsilci atama ve rapor yayınlama gibi yükümlülüklerin ise menşe ülke ilkesine aykırılık teşkil edeceği savunulmaktadır. Yargılama sürecinde henüz bir karar çıkmamış olmakla birlikte, 8 Haziran 2023 tarihinde savcı Szpunar, C-376/22 no.lu dosya kapsamında mütalaasını sunmuştur. Sözkonusu mütalaasında Szpunar, üye ülkelerce yürürlüğe sokulan genel-soyut kanuni düzenlemelerin, bilgi toplumu hizmetlerinin serbest dolaşımını etkilediği müddetçe 2000/31 no.lu Direktifin md. 3 f. 2 ve 4 hükümlerine aykırılık teşkil edeceğini savunmuş, bu sayede platformlar lehine bir eğilim göstermiştir..

5.3. İrlanda

Belirtildiği üzere İrlanda, vergi politikaları sebebiyle birçok teknoloji şirketinin Avrupa merkezidir. Dolayısıyla dünya çapında faaliyet gösteren teknoloji devlerinin Avrupa merkezleri bu ülkededir. Bilhassa veri koruma hukukunda da bu teşebbüslerin doğrudan tabi olduğu otorite, İrlanda Veri Koruma Otoritesidir. Bununla birlikte İrlanda Veri Koruma Otoritesi, sözkonusu teşebbüslere karşı "müsamahalı" davranışlarından dolayı eleştirilere maruz kalmıştır. Her ne kadar AB Genel Veri Koruma Tüzüğü kapsamında uygulanan en yüksek yaptırım, Meta'ya karşı İrlanda Veri Koruma Otoritesi tarafından uygulanan 1.2 Milyar Avro para cezası olsa da, ilgili otorite, bu kararı ancak, Avrupa Veri Koruma Kurumunun verdiği bağlayıcı karar neticesinde almak zorunda kalmıştır.

Sözkonusu kararda Meta İrlanda'nın Meta US'e gerçekleştirdiği kişisel veri aktarımının Genel Veri Koruma Tüzüğünde üçüncü ülkelere kişisel veri aktarımı için öngörülen şartlara uymadığı belirtilmiş, bu sebeple idari para cezası öngörülmüş ve aynı zamanda veri aktarımının hukuka uygun hale getirilmesi için ilgili veri sorumlusuna altı aylık bir süre tanınmıştır. Hukuka aykırılığı teşkil eden durum ise, Amerika Birleşik Devletleri'nde uygulanan PRİSM ve UPSTREAM programlarının dayanağı olan Sec. 702 FISA ve EO. 12333.70 ile PPD-28'in, Avrupa Birliği'nde elde edilen kişisel verilerin işlenmesi bağlamında yeterli koruma sağlamadığıdır. Her ne kadar META, ABD'ye aktarılan kişisel verilerin dayanağı olarak Komisyon tarafından yayımlanan Standart Sözleşme Hükümlerine (SCC) başvurmuş olsa da, ABD otoritelerinin sözkonusu kişisel verilere erişim yetkileri dikkate alındığında kişisel verisi işlenen gerçek kişilerin ABD makamları nezdinde Birlik standartlarına benzer şekilde hak arama imkanlarının bulunmadığı tespit edilmiştir.

İlgili karar, sadece verilen para cezasının miktarı açısından değil, Birlik standartlarının üçüncü ülkelerde de muhafaza edilmesi gerekliliği açısından da büyük bir önem taşımaktadır. Bir diğer ifade ile Avrupa Birliği, kendi sınırları içerisinde geliştirdiği koruma seviyesini, Birlik'te bulunan gerçek kişilerin kişisel verilerinin Birlik dışarısında işlenmesi halinde de muhafaza edilmesini amaçlamaktadır.

6. Karşılaştırma ve Sonuç

Avrupa Birliği, dijital çağda bir taraftan dijital ekonominin genel çerçevesini çizmek, diğer yandan da bireylerin temel hak ve özgürlüklerini korumak amacıyla yoğun bir düzenleme faaliyeti içerisine girmiştir. Sözkonusu düzenleme, kişisel verilerin korunması ve mahremiyet, elektronik ticaret ve dijital hizmetler, internet hukuku, siber güvenlik hukuku, rekabet hukuku, yapay zeka hukuku, ürün güvenliği gibi birçok farklı alanı kapsamaktadır. Her bir düzenleme ise beraberinde AB Üye Ülkeleri için uyum (compliance) yükümlülüğünü getirmektedir.

Genel bir eğilim olarak Birlik, evvelden hukukun yeknesaklaştırılması noktasında ve bilhassa dijital hakların düzenlenmesi bağlamında Direktif yöntemini tercih ederken son dönem gerçekleştirilen düzenlemelerde Tüzük yöntemi tercih edilmektedir. Bu sebeple üye ülkelerin takdir yetkileri kısıtlanmakta, öte yandan yeknesaklaştırma büyük bir oranda gerçekleştirilmektedir.

Öte yandan sözkonusu düzenlemeler sadece piyasa aktörlerine birtakım yükümlülükler getirmekle sınırlı kalmamaktadır. Aynı zamanda bu kapsamda bireylere de birçok imkânın sunulması sözkonusudur. Nitekim Birlik, özellikle büyük teknoloji şirketlerine karşı münhasıran idari yaptırımların yeterli olmadığı neticesine ulaşmıştır. Dolayısıyla bireylerin de kendi haklarını aramaları için işlevsel mekanizmaların oluşturulması ve muhafaza edilmesi önem arz etmektedir. Ayrıca dijital alanda meydana gelen ihtilaflarda alternatif uyuşmazlık çözümü mekanizmalarının ihdas edilmesi ve teşvik edilmesi, bir taraftan ihtilafların hızlı bir şekilde çözümlenmesine katkıda bulunacak, diğer yandan da mahkemelerin iş yükünü azaltacaktır.

Yukarıda etraflıca izah edilen düzenlemeler ayrıca idare açısından da büyük önem taşımaktadır. Öncelikle yeknesaklaşma, her ne kadar mevzuat açısından sözkonusu olsa da sözkonusu mevzuatın uygulanması noktasında üye ülkeler arasındaki koordinasyonun sağlanması da kaçınılmaz olacaktır. Bu amaçla Birlik nezdinde birçok yeni kurumun ihdas edilmesi öngörülmektedir. Bu otoritelerin görevi, doğrudan düzenlemeleri uygulamaktan çok, Üye Ülkelerin otoriteleri arasındaki koordinasyonu sağlamak, uygulamada birliği temin etmek, rehberler, tavsiyeler ve kararlar vesilesiyle de yeknesak uygulamaya katkı sağlamaktır.

Birlik düzeyinde dijital alanlarda getirilen düzenlemelerin olumlu yönleri açısından öncelikle hukuk politikasına

değinmekte fayda olacaktır. Şöyle ki yukarıda etraflıca izah edildiği üzere birçok alanda eş zamanlı olarak çok farklı düzenlemeler öngörülmektedir. Bütün bu düzenlemelerin birbiriyle çelişmemesi büyük önem arz etmektedir. Bu sebeple öncelikle genel ve soyut politikaları içeren Avrupa Birliği Dijital Tek Pazar Stratejisi, 2030 Dijital Pusula Bilgilendirmesi, Dijital On Yıl Yolu Politika Programı Kararı ve Dijital On Yıl İçin Dijital Hak ve İlkeler Avrupa Bildirisi gibi belgeler yayımlanmakta, ardından münferit düzenleme taslakları kaleme alınmaktadır. Dijital alanlarda kanun yapma tekniği açısından ise önem arz eden husus, kamu otoriteleri ile piyasa aktörleri arasındaki bilgi asimetrisinin dikkate alınması ve buradan hareketle emredici regülasyon tekniği yerine birlikte regülasyon yöntemlerinin tercih edilmesidir. Şöyle ki dijital alanda öngörülen birçok düzenlemede artık risk temelli bir yaklaşım, hesap verilebilirlik ilkesi ile birlikte kaleme alınmakta, hukuka aykırı, uyumsuz faaliyette bulunma riski, bilgi asimetrisi kapsamında daha avantajlı konumda olan aktörlere yükletilmektedir. Bu yaklaşım özellikle AB Genel Veri Koruma Tüzüğü kapsamında alınması gereken idari ve teknik tedbirler ile Yapay Zeka Yasa Önerisi çerçevesinde oluşturulması öngörülen kalite yönetim sistemlerinde görmek mümkündür. Ayrıca standartlar, sertifikalar, davranış kuralları gibi yöntemlerle hukuk güvenliğinin sağlanması da uyum masraflarının asgari seviyeye indirilmesi de bu yaklaşımın bir diğer görünümüdür. Bu yaklaşımın örneğini Genel Veri Koruma Tüzüğü kapsamında öngörülen standartlar, sertifikalar ve davranış kurallarında görmek mümkündür.

Düzenleme mantığı açısından önem arz eden bir diğer husus, düzenlemelerin esnek niteliğine ilişkindir. Şöyle ki dijital alanda yaşanan gelişmeler çok hızlı olduğu için her seferinde yeni düzenlemeler yapmak ya da düzenlemelerin bu değişikliklere adapte edilmesi ihtiyacı hasıl olacaktır. Dolayısıyla Birlik düzenlemelerinde daha esnek düzenleme yöntemleri tercih edilmektedir. Buna örnek olarak AB Genel Veri Koruma Tüzüğü kapsamında veri koruma etki analizi yapılması gereken ve gerekmeyen durumlar, beyaz ve kara listeler şeklinde AB Komisyonu tarafından yayımlanmakta, Dijital Piyasalar Yasası kapsamında çok büyük çevrimiçi platform olarak nitelendirilen "gatekeeper" olarak anılan geçit bekçileri listeleri yine Komisyon tarafından yayınlanmakta, Yapay Zeka Yasa Önerisine göre yüksek risk arz eden yapay zeka sistemleri de yine Komisyon tarafından yayımlanmaktadır. Bu listeleri esnek kılan husus ise, bunların Komisyon tarafından sürekli güncellemeye tabi tutulmasıdır. Dolayısıyla statik bir regülasyon yerine teknolojinin gelişimi ve beraberinde getirdiği ihtiyaçlar ışığında esnek bir regülasyon öngörülmektedir.

Dijital haklar özelinde ise Avrupa Birliği'nin insan odaklı yaklaşımı önem arz etmektedir. Şöyle ki bütün teknolojik gelişmeler, ekonomik açıdan ciddi bir potansiyel barındırmaktadır. Bununla birlikte sözkonusu potansiyel, olumsuz sonuçları da beraberinde getirebilir. Bu kapsamda kanun koyucular yeni teknolojiyi bütünüyle yasaklamakla riski tamamen bertaraf edebilmekte, ancak bu teknolojinin barındırdığı bütün menfaatlerden de mahrum kalmaktadır. Diğer yandan teknolojiye hiçbir şekilde müdahale edilmemesi de özellikle bireyler açısından telafisi imkansız zararlara sebebiyet verebilecektir. İşte bu iki menfaat arasında bir denge sağlamayı amaçlayan Birlik mevzuatı, insan odaklı bir yaklaşımla birey temel hak ve hürriyetlerinin en üst seviyede temin edilmesini amaçlamaktadır.

Keza dijital haklar bağlamında bireylere tanınan imkanlar açısından önem arz eden bir diğer husus, özel olarak uygulama ("private enforcement") yaklaşımıdır. Şöyle ki kanunlara uyumu denetleyen kamu kurumları mevcuttur. Piyasa aktörlerinin hukuka aykırı faaliyetlerini tespit eden bu kurumlar idari para cezası öngörmekte, bu sayede bu aktörleri hukuka uyumlu davranmaya zorlamaktadır. Ancak piyasa aktörlerinin hukuka uyumlu davranmaya teşvik edilmesi noktasında tek yöntem, idarenin elinde bulundurduğu yaptırımlardan ibaret değildir. Kaldı ki öngörülen idari para cezaları, ilgili teşebbüslerin hukuka aykırı davranışlarından elde ettikleri gelirlerin küçük bir kısmına tekabül etmekte, dolayısıyla gerçekten caydırıcı bir etkiye sahip olamamaktadır. Dolayısıyla bu bağlamda bireyler de önemli bir konuma sahiptir. Şöyle ki bireyler de gerek Birliğin bağlayıcı hukuki tasarruflarından kaynaklanan haklarının kullanılması kapsamında, gerekse bilhassa tazminat talepleri çerçevesinde teşebbüsleri hukuka uyumlu davranmaya zorlayabilecektir. Bunun için ise her bir üye ülke uygulamasında işlevsel bir mekanizmanın varlığı şarttır. Bunun ötesinde özellikle dijital alanda yaşanan ihlaller, çoğu zaman bireylerde maddi zararlara yol açmayacak ya da çok cüzi zararlar sözkonusu olacaktır. Dolayısıyla daha çok manevi tazminat talepleri gündeme gelecektir. Ancak manevi tazminatın miktarı noktasındaki belirsizlik de birçok bireyin, teknoloji devlerine karşı yargı yoluna başvurmaktan imtina etmesine sebebiyet vermektedir. Hal böyle olunca bir taraftan hızlı ve kolay alternatif uyuşmazlık çözümü yollarının geliştirilmesi önem arz etmekte, diğer taraftan da toplu dava imkanlarının teşvik edilmesi öngörülmektedir. Bunun somut bir örneği olarak AB Genel Veri Koruma Tüzüğü kapsamında veri koruma dernek ve kuruluşlarının toplu dava açma imkanları öngörülmektedir.

Ancak Birlik nezdinde yaşanan bu gelişmeler, elbette sadece olumlu yönlere sahip değildir. Bilakis özellikle her geçen gün yeni bir düzenlemenin duyurulması, dijital alanda faaliyet gösteren piyasa aktörleri açısından çok ciddi uyum (compliance) yükümlülükleri ve masraflarını da beraberinde getirmektedir. Dijital alanda faaliyet göstermek isteyen teşebbüslerin aynı anda birden fazla ulusal mevzuatın yanında Birlik mevzuatını dikkate alması

kaçınılmaz olacaktır. “Aşırı düzenleme (overregulation)” olarak adlandırılan bu durum, Birlik içerisinde AB Temel Haklar Şartının 16. maddesinde de kendisine yer bulan teşebbüs hürriyetinin orantısız şekilde sınırlandırıldığı eleştirilerine sebebiyet vermektedir.

Bu düzenlemelerin üye ülkelere yansımaları bakımından ise ülkelerin ekonomik, sosyo-kültürel yaklaşımları dikkat çekmektedir.

Örnek olarak Almanya’da veri koruma hukuku köklü bir geçmişe sahip olduğu için veri koruma otoriteleri de bu tecrübeye dayalı olarak aktif bir şekilde faaliyet göstermektedir. Ancak önemle belirtelim ki bu ülkede faaliyet gösteren veri koruma otoriteleri, çoğu zaman veri sorumluları ile işbirliği içerisinde hareket etmekte, bir diğer ifade ile “emredici düzenleme” yaklaşımını ancak istisnai durumlarda uygulamaktadır. Öte yandan federe devlet yapısı sebebiyle her bir eyalet bazında dikkate alınması gereken hususların olduğunu da gözden kaçırmamak gerekecektir.

Avusturya örneğinde ise özellikle Max Schrems tarafından kurulan veri koruma aktivisti kuruluş sayesinde birçok husus, yüksek yargıya taşınmaktadır. Dolayısıyla her ne kadar nüfus ve ekonomik hacim açısından Birlik üye ülkeleri arasında daha az önem taşıyan bir ülke olsa da, Avusturya uygulaması sayesinde Genel Veri Koruma Tüzüğü bağlamında birçok hususun yüksek yargıya taşındığını ve bu sorunlara açıklık getirildiğini söylemek mümkündür.

Buna karşılık İrlanda örneğinde başlangıçtan itibaren düşük kurumlar vergisi sayesinde teknoloji devlerini kendi ülkesine çekmeye çalışan bir Üye Ülke sözkonusudur. Özellikle veri koruma hukuku alanında ilgili ülke otoritesi, çoğu zaman gerekli aksiyonları almaması sebebiyle eleştirilere maruz kalmıştır.

Dolayısıyla her ne kadar mevzuat açısından bir yeknesaklık sözkonusu olsa da her üye ülkenin kendi menfaatleri kapsamında bir uygulama geliştirmesi de engellenemeyecektir. Bu aşamada ise Birlik kurumları devreye girmekte, farklı uygulamaların önüne geçmek adına koordinasyon vazifesi ifa etmektedir.

KAYNAKÇA

Çekin MS, Berktaş AE, Akıncı MF, Veri Hukuku (On İki Levha Yayıncılık, 2023)

Develioğlu HM, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku (On İki Levha Yayıncılık, 2017)

Kama Işık S, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış (On İki Levha Yayıncılık, 2019)

Kuner C, Bygrave L A, Docksey C, The EU General Data Protection Regulation (GDPR) A commentary (Oxford University Press 2020)

Kühling J, Buchner B, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG (Beck, 2024)

Lambert PB, Understanding the New European Data Protection Rules (CRC Press - Taylor & Francis 2018)

Schulze R, Staudenmayer D, EU Digital Law - Article-by-Article Commentary (Nomos Verlagsgesellschaft 2020)

Taeger J, Gabel D, DSGVO BDSG TTDS (Deutscher Fachverlag, 2022)

Voigt P, Bussche A, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017)

Bu proje Avrupa Birliği tarafından finanse edilmektedir.

TÜRKİYE VE AB
MALİ İŞBİRLİĞİ
TEMEL HAKLAR

Temel Haklar Sektör Koordinasyonunun Güçlendirilmesi Projesi

WEglobal