Anadolu Üniversitesi Sosyal Bilimler Dergisi AÜSBD
Anadolu University Journal of Social Sciences AUJSS

Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları[1]

New Techniques and Enforcement Mechanisms Provided by the European Union General Data Protection Regulation

İpek Çimen Bulut[2]

Başvuru Tarihi: 21.12.2019
Kabul Tarihi: 16.06.2020
Makale Türü: Derleme

Öz

Özellikle 2000'li yıllarda, bilgi ve iletişim teknolojilerinde yaşanan gelişmeler, hayatımızın her alanının dijitalleşmesine yol açmıştır. Hızla dijitalleşen bu dünyada, bireyler için yeni iş fırsatları, çevirim içi işlem yapma ve bilgiye erişim kolaylıkları gibi pek çok fırsat barınsa da, dijitalleşme beraberinde, özellikle de dijital işlemlerin çevirim içi ortamda bıraktığı ayak izleri sebebiyle, kişisel verilerin korunması kapsamında önemli riskler de getirmiştir. Dijitalleşme ile ortaya çıkarak kişisel verilere yönelen bu yeni nesil risk ve tehditler ile bunlardan korunma yolları, Avrupa Birliği'nin zihnini uzun zamandır meşgul etmektedir. 25 Mayıs 2018 tarihinde yürürlüğe giren ve Birlik çapında uyumlulaştırılmış ve doğrudan uygulanabilir yasa hükümleri içeren "Avrupa Birliği Genel Veri Koruma Tüzüğü", güçlendirilmiş Birlik yasaları kapsamında kişisel verilerin korunması ve serbest dolaşımlarının sağlanması bakımından atılmış önemli bir adımdır.

Bu çalışmada, "Avrupa Birliği Genel Veri Koruma Tüzüğü ile", kişisel veri güvenliğinin sağlanması bağlamında getirilen yeni teknik ve yaptırım mekanizmaları, çeşitli Birlik belgelerinin de yardımı ile açıklanmaya çalışılmıştır.

Anahtar Kelimeler: *Kişisel Verilerin Korunması, Avrupa Birliği 2016/679 Sayılı Genel Veri Koruma Tüzüğü, Tasarımla ve Varsayılan Ayarlarla Veri Koruma, Veri Koruma Etki Değerlendirmesi, Takma Ad*

[1] Bu çalışma, yazarın Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, Avrupa Birliği Anabilim Dalı, Avrupa Çalışmaları Doktora Programı bünyesindeki "***Avrupa Dijital Tek Pazarında Kişisel Verilerin Korunması***" isimli yayınlanmamış tez çalışmasından üretilmiştir.

[2] Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, Avrupa Birliği Anabilim Dalı, Avrupa Çalışmaları Doktora Programı, Doktora Adayı, **ipek.cimen@gmail.com,** ORCID: 0000 0002 26714760

Abstract

Especially in the 2000s, the developments in the field of information and communication technologies have digitalized all areas of our lives. In this rapidly digitalized world, although there are many opportunities for individuals, such as new business opportunities, ease of making online transactions and access to information easily, digitalization has also brought significant risks in terms of personal data protection, especially due to the footprints left by digital transactions in the online environment. These new generation risks and threats emerged from the digitalization and targeted to the personal data and the ways of protection from them, have been occupying the mind of the European Union for a long time. The "European Union General Data Protection Regulation", which came into force on 25 May 2018, contains harmonized and directly applicable law provisions across the Union, which is an important step for the protection and free movement of personal data within the reinforced Union law.

In this study, new techniques and enforcement mechanisms introduced by the "European Union General Data Protection Regulation", in the context of ensuring personal data security, have been tried to be explained by the help of various Union documents.

Keywords: Personal Data Protection, European Union 2016/679 Dated General Data Protection Regulation, Privacy by Design and by Default, Data Protection Impact Assessment, Pseudonymization

Giriş

2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (Regulation G. D. P., 2016)[3], 27 Nisan 2016 tarihinde kabul edilerek, Avrupa Birliği'nin 4.5.2016 tarih ve L119/86 sayılı Resmi Gazetesinde yayınlanıp, 25 Mayıs 2018 tarihinde yürürlüğe girerek, 95/46/EC sayılı Kişisel Verilerin Korunması Direktifinin (Parliament, 1995)[4], yerini almıştır

95/46/EC sayılı Direktif, kişisel verilerin korunması ve serbest dolaşımlarının sağlanması hususlarında temel çerçeveyi oluşturup, yasal sınırları çizerek, bu konuda ulusal düzenlemelerin yapılmasını üye devletlerin kendisine bırakmıştı. Bu kısmi serbesti, üye devletler nezdinde kişisel verilerin korunmasına ilişkin olarak birbirinden farklı ulusal yasal düzenleme ve uygulamaların ortaya çıkarak, Birlik genelinde yasal anlamda parçalı bir görünüm oluşmasına sebebiyet vermiştir. Bu durum, kişisel verilerin korunması ve serbest dolaşımlarının sağlanması bağlamında reform ihtiyacının doğmasının en önemli sebeplerinden biridir. Zira, Lizbon Antlaşması ile temel bir hak olarak Kurucu Antlaşmalar düzeyinde tanınarak, korunur hale gelen kişisel verilerin, Birlik hukuku kapsamında doğrudan uygulanabilir olmayan 95/46/EC sayılı Direktif ile korunarak, serbest

[3] Bu çalışmada, "*Kişisel verilerin korunmasına ilişkin 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü*", "*2016/679 sayılı Tüzük*", "*Genel Veri Koruma Tüzüğü*", "*Tüzük*" veya "*GDPR*" olarak da adlandırılabilecektir.

[4] Avrupa Birliği'nin "*95/46/EC sayılı Direktifi*", kimi Türkçe kaynaklarda "*Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiğine İlişkin Direktif*" olarak tercüme edilmektedir. İlgili Direktif, işbu makale çalışması kapsamında, "*95/46/EC sayılı Kişisel Verilerin Korunması Direktifi*", "*Direktif*" ya da "*95/46/EC sayılı Direktif*" şeklinde ifade edilmiştir.

dolaşımlarının sağlanmaya çalışılması yöntemi, bilgi ve iletişim teknolojileri alanında yaşanan devrim niteliğindeki gelişmeler ve artan internet kullanımı sebebiyle ortaya çıkan yeni tehditler de göz önüne alındığında, yeterlilik ve güvenilirliğini yitirmişti. Çerçeve nitelikli hükümler içeren ilgili Direktif'te belirlenen koşul ve sınırlamalar kapsamında, üye devletlerin her birinin ayrı ayrı yaptıkları ulusal düzenlemelerle, kişisel verilerin Birlik içinde birbirinden farklı seviyelerde korunarak, serbest dolaşımlarının sağlanmaya çalışılması, Birlik sınırları içerisinde, kaçınılmaz olarak farklı uygulamaların ortaya çıkmasına da yol açmıştır. Birlik hukukunda temel haklar kapsamında tanınan kişisel verilerin korunması bağlamında, Birlik düzeyinde farklı uygulamaların olması ise, köklerini insan hak ve özgürlüklerinin korunmasına dayandırdığı iddiasında olan Avrupa Birliği için kabul edilebilir bir durum değildir. Tüm bunların yanı sıra, üye devletler nezdinde kişisel verilerin korunmasına ilişkin olarak ortaya çıkan farklı yasal uygulamalar, bunlara uyum sağlayarak, Birlik içinde ticari faaliyette bulunmaya çalışan tüzel kişiler açısından da, katlanılmak zorunda kalınan idari yükün ağırlaşmasına yol açmakta idi. Neticede bu durum, Birlik'in parçalı yapısını perçinleyerek, tüm ticaret engellerinin kaldırılarak, tamamen uyumlulaştırılmış yasal düzenlemeler çerçevesinde tamamlanmaya çalışılan yekpare bir Avrupa dijital tek pazarı oluşturma nihai hedefini de baltalamaktaydı (Diaz Diaz 2016, s. 208; De Hert ve Papakonstantinou 2012, s.131; European Commission (EC) 2010: 609, s.3; Oxman, 2000, s. 192-193, 203).

Veri Koruma Reformu kapsamında 95/46/EC sayılı Direktifin, yürürlükten kaldırılarak, yerini 2018 yılı itibarı ile, Avrupa Birliği Genel Veri Koruma Tüzüğü'ne bırakmasıyla, kişisel verilerin korunması ve serbest dolaşımlarının sağlanması hususları, üye devletlerin egemenlik hakları dahilinde yapacağı ulusal yasal düzenlemeler kapsamından çıkarılarak, Birlik düzeyinde uyumlulaştırılmış, doğrudan uygulanabilir hükümlerle regüle edilmeye başlanmıştır. Bu makale çalışmasıyla, Avrupa Birliği'nde kişisel verilerin korunması ve serbest dolaşımlarının sağlanması kapsamında yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğü'nün bel kemiğini oluşturan ve veri güvenliğinin sağlanmasına yönelik olan yeni teknik ve uygulamalar ile kişisel verilerin ihlali halinde uygulanacak yaptırımların ortaya konması hedeflenmiştir.

Kişisel Verilerin İşlenmesinde İhlal Çeşitleri ve Tarafların Yükümlülükleri

Genel Veri Koruma Tüzüğü ile, kişisel veriler bağlamında getirilen yeni koruma teknikleri ve yaptırım mekanizmalarına geçmeden önce, kişisel verilere ilişkin ihlal çeşitlerinin ve bunların önlenebilmesi adına tarafların yükümlülüklerinin neler olduğunu incelemekte fayda vardır. Madde 29 Veri Koruma Çalışma Grubu, 2017 yılında, henüz 2016/679 sayılı Genel Veri Koruma Tüzüğü yürürlüğe girmeden önce, işbu Tüzük çerçevesinde yapılacak veri ihlal bildirimlerine ilişkin bir rehber yayınlayarak, kişisel veri ihlal çeşitlerini üç kategori altında düzenlemiştir. Bu rehbere göre, kişisel verilere ilişkin olarak yetkisiz veya kazara yapılan her türlü ifşa yahut erişim "*gizlilik ihlali (confidentiality breach)*"; kişisel verilerin yetkisiz kişiler tarafından ya da kazara imhası yahut kayıp edilmesi "*ulaşılabilirlik ihlali (availability breach)*"; kişisel verilerin yetkisiz kişilerce veya kazara değiştirilmesi faaliyeti ise "*bütünlük ihlali (integrity breach)*" olarak sınıflandırılmıştır (Article 29 Working Party (A29WP), 2017: 250, s. 6-8).

2016/679 sayılı Tüzük'ün 32.maddesi kapsamında, kişisel verilerin işlenmesi sürecinde, ihlallerin henüz gerçekleşmeden önlenerek, makul ve kabul edilebilir bir seviyede veri güvenliğinin sağlanabilmesine özel önem verilerek, bunun için gerekli ön tedbirlerin alınmasına ilişkin, veri kontrolörü ve işleyicisine düşen sorumluluklar düzenlenmiştir (A29 WP, 2017: 250, s.5). 32.madde hükmü incelendiğinde, uygun teknik ve örgütsel tedbirleri alma yükümlülüğünün eskiye oranla genişletilerek, veri kontrolörünün yanı sıra işleyicinin de bu tedbirlerin alınmasından, kontrolörle birlikte sorumlu olduğunun altının çizildiği görülmektedir.

Tüzük 32. maddeye göre; "*Takma ad kullanılması ve şifreleme yapılması (madde 32/1 a); Veri işlemeye ilişkin sistem ve hizmetlerin ihlal girişimlerine karşı, gizliliğinin, bütünlüğünün, kullanılabilirliğinin ve dayanıklılığının sürekliliğinin sağlanması (madde 32/1 b); Teknik veya fiziki bir müdahalenin gerçekleşmesi durumunda kişisel verilerin yeniden kullanılabilirliğinin ve erişilebilirliğinin sağlanması (madde 32/1 c); İşlem güvenliğinin devamlılığını sağlamak adına alınan tedbirlerin etkinliğinin düzenli aralıklarla kontrol edilerek değerlendirilmesi (madde 32/1 d)*", gibi uygulamalar, veri kontrolörü ve işleyicisinin, somut olayın özelliklerini, uygulama maliyetlerini, işlenecek kişisel verilerin niteliklerini, işleme faaliyetinin kapsam ve amaçlarını, olası riskleri birlikte göz önüne alarak, veri işleme sürecinin güvenliğinin sağlanabilmesi adına alabileceği, teknik ve örgütsel tedbirler kapsamında sayılmaktadırlar.

Tüm bunların yanı sıra, Tüzük madde 32/4'e göre, veri kontrolörü ve işleyicileri, kişisel verilere erişim imkanı bulunan ve kendi yetki ve denetimleri altında çalışan kişilerin, kişisel verilerin işlenmesi hususunda, yalnızca kişisel verilerin korunmasına ilişkin yasa hükümlerine uygun şekilde verecekleri talimatlara göre işleme yapmalarını sağlayabilmek adına gereken tedbirleri de almakla yükümlüdürler. Bu da veri kontrolör ve işleyicilerinin işbu Tüzük kapsamında sorumluluk ve yükümlülüklerinin artırıldığının bir başka somut kanıtı niteliğindedir (Tikkinen-Piri, Rohunen ve Markkula, 2018, s. 143).

2016/679 sayılı Tüzük madde 33 ile, kişisel verilerin işlenmesinde güvenliğin sağlanmasına yönelik olarak, veri kontrolörüne, ihlalin gerçekleştiğinin öğrenilmesini takiben, vakit geçirmeksizin ve herhalikarda ihlalin öğrenilmesinden itibaren 72 saat içerisinde, yetkili denetim makamının, bu durumdan haberdar edilmesi yükümlülüğü de getirilmiştir. Diğer bir ifade ile, veri kontrolörünün her türlü kişisel veri ihlalini, bu ihlalin etkilerini ve gerçekleşen ihlale karşılık alınan düzeltici önlemlerin neler olduğunu detayları ile birlikte kayıt altına alarak, ihlale ilişkin yetkili denetim makamını, bilgilendirme yükümlülüğü bulunmaktadır. En geç 72 saat içerisinde yapılması gereken bu bildirim ile, denetim makamının, hak kayıplarının önüne geçilmesi amacıyla, ihlale ilişkin gerekli ve yeterli tedbirlerin alınarak, yasal düzenlemelere uyulup uyulmadığının tespitine ilişkin, denetim görevini yerine getirebilmesi için uygun koşulların yaratılmasının da hedeflendiğini söylemek yanlış olmayacaktır. Kişisel veri ihlalinin, işleyici tarafından öğrenildiği durumlarda ise, işleyicinin de, veri kontrolörünü bu durumdan, gecikmeksizin haberdar etme yükümlülüğü bulunmaktadır. Yetkili denetim makamına, veri kontrolörü tarafından Tüzük madde 33 kapsamında yapılacak ihlal bildiriminin en azından; "*İhlal edilen, kişisel verilerin kategorileri, ihlale konu veri süjelerinin ve kişisel veri kayıtlarının kategorileri ile gerçekleşen ihlallerin -yaklaşık olarak- sayısı gibi unsurların tarifini (madde 33/3 a); Veri koruma görevlisinin veya daha fazla bilgi*

alınabilecek bir başka iletişim makamının adı ve iletişim bilgilerini (madde 33/3 b); İhlalin olası sonuçlarını (madde 33/3 c); Kontrolör tarafından ihlale ve olası etkilerine yönelik olarak halihazırda alınan ya da alınması önerilen tedbirlerin neler olduğu hususlarını (madde 33/3 d)", içermesi gerekmektedir (Voss, Winter 2016-2017, s. 229).

Kişisel verilere yönelebilecek olası risklerin boyutları, işlenen kişisel verinin niteliği ile işlemenin kapsam ve niteliğine, kullanılan teknolojiye göre değişiklik gösterebilmektedir. Bu doğrultuda 2016/679 sayılı Tüzük ile, kişisel verilerin işlenmesi kapsamında gerçekleşen ihlalin, veri süjesinin temel hak ve özgürlüklerine ilişkin büyük risk oluşturduğu hallerde, salt madde 33 kapsamında veri kontrolörü tarafından denetim makamına ihlal bildiriminde bulunulmasının yeterli olmayacağı kabul edilmiştir. Bu sebeple, ihlalin veri süjesinin temel hak ve özgürlükleri bakımından yüksek risk içermesi durumunda, Tüzük'ün 34.maddesi kapsamında, veri süjesinin de bu ihlalin kapsam ve niteliğine, ihlalin önlenmesi için alınacak tedbirlere ilişkin olarak veri kontrolörü tarafından kolay anlaşılır şekilde, açık ve sade bir dille gecikmeksizin bilgilendirilmesi şartı getirilmiştir (European Union Agency for Fundamental Rights (EUAFR), 2018, s. 179; GDPR Madde 34/1,2).

Tüzük'ün 34/3.maddesi kapsamında sayılan koşullardan herhangi birinin yerine getirilmesi durumunda ise veri kontrolörü, veri süjesini bilgilendirme yükümlülüğünden muaf tutulabilecektir. Muafiyet halleri 2016/679 sayılı Tüzük'ün madde 34/3 kapsamında sayılmıştır. Buna göre, "*Kontrolörün, kişisel verilerin veri süjesi ile bağını şifreleme gibi koruma tedbir ve yöntemleriyle kesmesi sebebiyle, ihlalin veri süjesinin kimliğini ortaya çıkaramadığı durumlar (madde 34/3 a); Veri kontrolörünün ihlalin gerçekleşmesinden sonra aldığı tedbirler neticesinde temel hak ve özgürlükleri tehdit eden koşulların ortadan kalktığı durumlar (madde 34/3 b); Veri süjelerinin halka açık genel bir bilgilendirme vasıtasıyla haberdar edildiği durumlar (madde 34/3 c)*" muafiyet halleri kapsamında sayılmışlardır.

Kişisel verilerin yetkisiz, yasadışı ve kazara kullanımın, imha, ifşa, kayıp ve tahrip edilmesinin, erişilmesinin, yayılmasının, saklanmasının ve değiştirilmesinin engellenmesi amacıyla 2016/679 sayılı Tüzük kapsamında yapılan anılan düzenlemeler, ihlallerin önlenerek veri güvenliğinin sağlanması ve dolayısı ile de temel hak ve özgürlüklerin korunması bağlamında büyük önem taşımaktadırlar. Bunun bilinciyle, Tüzük ile, hesap verebilirlik ilkesi doğrultusunda, risk yönetimi yapılarak, kişisel verilerin işlenmeleri sürecinde, ihlallerin henüz gerçekleşmeden önlenerek, işlem ve veri güvenliğinin sağlanmasına yönelik uygun ve yeterli tedbirlerin alınmasına çalışılmıştır.

Kişisel Verilerin Güvenli İşlenmesinde Yeni Teknik ve Yöntemler

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler neticesinde her alanda ortaya çıkan dijitalleşme rüzgarları, kişisel verilerin çevirim içi ortamda ve sınırlar arası dolaşımları esnasında korunmalarını güçleştirmiştir. Bu durum, Avrupa Birliği'ni kişisel verilerin daha iyi korunabilmelerinin sağlanması amacıyla, özellikle bilgi ve iletişim teknolojileri alanında ortaya çıkan gelişmelere paralel olarak, yeni teknik, ilke ve yöntemler ile daha güçlü yaptırım mekanizmaları ortaya koyma arayışına yöneltmiştir. Devam eden alt başlıklarda bu ilke ve mekanizmalar, bütüncül perspektiften bir arada sunulmuştur.

Tasarımla Veri Koruma İlkesi

Mahremiyetin ve veri güvenliğinin tarihte belki de hiç olmadığı kadar kırılgan hale geldiği içinde bulunduğumuz dijital çağda, kişisel verilerin en üst seviyede korunabilmeleri amacıyla, 2016/679 sayılı Genel Veri Koruma Tüzüğü, bazı yeni ilke, teknik ve yöntemler ortaya koymuştur. Bunlardan en önemlilerinden biri de ilgili Tüzük madde 25 kapsamında açıklanan ve "*Tasarımla Veri Koruma"* olarak dilimize kazandırılmış olan (Başalp, 2015, s. 92) *"Privacy by Design*" ilkesidir.

Tasarımla Veri Koruma İlkesi, kişisel verilerin, etkin ve etkili bir şekilde korunabilmelerinin sağlanması amacıyla, iş yapma süreçleri ve işletim sistemleri içerisindeki veri işleme faaliyetleri kapsamında, bu sistem ve süreçler henüz tasarım aşamasındayken, somut olayın özellikleri ve yapılacak işleme faaliyetinin amaç ve kapsamı çerçevesinde öngörülebilir risklere karşı, veri mahremiyetini güçlendirici uygun ve yeterli teknik ve idari tedbirlerin alınmasını ifade eder. Teknolojik ilerlemelerle birlikte kişisel veri güvenliğine ilişkin tehdit ve ihlallerin artması sebebiyle, siber güvenliği sağlamanın gereğinin her geçen gün daha fazla hissedildiği günümüz dünyasında, tasarımla veri koruma (privacy by design) ilkesi de gün geçtikçe daha önemli hale gelmektedir. Başka bir deyişle, yaşanan teknik ilerlemelere ve internet kullanımının artmasına paralel olarak, popülerliği artan tasarımla veri koruma (privacy by design) ilkesi, kişisel verilerin korunması bağlamında oluşturulacak sistemsel bütünlük içerisinde ve bu sistem henüz tasarım aşamasındayken, reaktif değil, proaktif davranarak, olası risklerin ve güvenlik ihlallerinin gerçekleşmesinden önce, bunların tahmin edilerek somut olayın özelliklerine göre önlemler alınmasını ifade eden önleyici nitelikteki yasal, teknik ve idari tedbirler bütünü olarak da tanımlanabilir (Cavoukian, May 2010, s. 2-4; Cavoukian, August 2010, s. 247-249; European Data Protection Supervisor, 8/2015, s. 9-10).

Varsayılan Ayarlarla Veri Koruma İlkesi

Tüzük'ün 25.maddesi kapsamında düzenlenen özgün adıyla "*Privacy by default", dilimizdeki karşılığı olan* "*Varsayılan Ayarlarla Veri Koruma*" İlkesidir (Başalp, 2015, s. 92). Bu ilke, tasarlanan iş yapma süreçleri kapsamında yapılacak veri işleme faaliyetlerinin, yalnızca ilk başta belirlenerek veri süjesine bildirilen toplanma amacıyla sınırlı olarak yapılmasını sağlayacak nitelikteki mahremiyet dostu teknik mekanizmaların oluşturularak, bu uğurda gereken önlemlerin alınmasını ifade eder. Varsayılan ayarlarla veri koruma ilkesinin, kişisel verilerin korunmasında göz önüne alınması gereken "*Veri Minimizasyonu*" ve "*Amaç ile Sınırlılık*" temel ilkeleri ile doğrudan bağlantılı olduğundan ve bu bağlamda da kişisel veriler üzerinde veri süjesinin kontrolünün artırılmasına katkıda bulunduğundan şüphe yoktur (Sanchez, 2016, s. 124, 129-130; UK Information Commissioner's Office (ICO), 2019).

2016/679 sayılı Tüzük ile getirilen tasarımla ve varsayılan ayarlarla veri koruma ilkelerinin özümsenmesi yoluyla geliştirilecek mahremiyet dostu teknik çözümler, iş yapma süreçleri, işletim sistemleri, iş modelleri ve şirket yapılanmaları vasıtasıyla, ortaya "*veri koruma dostu ürün ve hizmetler*" koyulmasını da kolaylaştırabilecektir (Başalp, 2015, s.92; ENISA, 2014, s. iii, iv, 55-58).
2016/679 sayılı Tüzük'ün 25.maddesi kapsamında, gerek tasarımla veri koruma, gerekse de varsayılan ayarlarla veri koruma ilkeleri ile, veri kontrolörlerine kişisel verilerin korunması bağlamında oluşturacakları mekanizmalar ve kullanacakları yöntemler açısından önemli görev ve

sorumluluklar yüklenmiştir. Bu ilkeler vasıtasıyla, kişisel verilerin, hem tasarım aşamasından itibaren alınacak önleyici tedbirler kapsamında oluşturulacak sistemler aracılığıyla güven içinde işlenmesinin, hem de amaçla sınırlı olma hususunda gereken hassasiyetin gösterilmesinin garanti altına alınmaya çalışıldığı söylenebilir (Wachter, 2018, s. 17-21).

Takma Ad Kullanımı

Kişisel verilerin korunmasında kullanılan bir diğer teknik de, Tüzük'ün getirdiği önemli değişikliklerden biri olan "*takma ad kullanımı*" yahut "*Rumuz*" olarak da Türkçe'ye çevrilebilen "*pseudonymisation*" tekniğidir.

Takma ad kullanımı (Pseudonymisation), Tüzük'ün 4/5.maddesinde tanımlanmıştır. Bu tanıma göre, "*takma ad kullanımı (pseudonymisation)*, kişisel verilerin, ayrı tutulan ve özel teknik ve örgütsel tedbirlerle korunan ek bilgiler olmadan, veri süjesinin kim olduğunun tespit edilemeyeceği şekilde işlenmesi" anlamına gelir. Bu yöntemde, veri süjesinin kimliğinin tespitinde kullanılabilecek nitelikteki veriler, işlenen verilerden ayrı bir yerde tutulup, bunların yerlerine çeşitli kod ve sayılar kullanılır. Böylelikle, işlenen kişisel verilerin gerçekte kime ait olduğunun tespit edilebilmesi engellenerek, mahremiyetin korunması garanti altına alınmaya çalışılmaktadır. Takma ad kullanımı (Pseudonymisation) tekniğiyle işlenen veriler, kişisel veri olma özelliklerini yitirmeseler de, ayrı bir yerde saklanarak özel tekniklerle korunan ek bilgiler olmadan bu verilerin kime ait oldukları tespit edilememektedir (Esayas, 2015, s. 4, 8).

Şifreleme

Özellikle bulut bilişim gibi ileri teknoloji sistemleri dahilinde yapılacak işlemelere ilişkin olarak gerçekleşebilecek güvenlik ihlal ve zaafları karşısında, kişisel verilerin güvenliğinin, en üst seviyede sağlanarak, korunabilmesi için Tüzük kapsamında kullanılabilecek teknik uygulamalardan bir diğeri de "*Şifreleme (Encryption)*" tekniğidir. Veri güvenliğinin sağlanmasında kullanılabilen bir teknik olan şifreleme ile, kişisel verilerin kime ait olduğuna ilişkin belirleyici olabilecek veri ve bilgilerin, gizli bir algoritma, kod veya kripto anahtarı kullanılarak gizlenmesi yoluna gidilerek, erişime yetkili olmayan herhangi bir kimsenin anlayamayacağı hale getirilen verilerin, mahremiyetlerinin korunması hedeflenmektedir. Şifreleme, internet gibi açık ağlar veya cep telefonları, diz üstü bilgisayarları gibi taşınabilir cihazlar üzerinden yapılan işlemler ile bu işlemler dahilinde işlenen kişisel verilerin korunması bağlamında bir uçtan diğer uca, başka bir ifade ile, göndericinin cihazından alıcının cihazına kadar, tüm işlemleri kapsayacak şekilde kesintisiz uygulanması gereken bir yöntemdir (A29WP, Statement, 2018, s. 1; GDPR Recital 83; Mansfield-Devine, 2017, s. 18-19; Spindler ve Schmechel, 2016, s. 169-171). 2016/679 sayılı Tüzük, şifreleme (encryption) yöntemine ilişkin açık bir tanım getirmemekle birlikte, veri güvenliğinin ve işlemenin yasallığının sağlanabilmesi bağlamında, pek çok madde kapsamında bu yöntemin kullanılmasının gereğini işaret etmektedir.

Veri Koruma Etki Değerlendirmesi

2017 yılında, Madde 29 Veri Koruma Çalışma Grubu, 2016/679 sayılı Genel Veri Koruma Tüzüğü'nde düzenlenen veri koruma etki değerlendirmesi tekniğinin tanım ve kapsamına ilişkin bir rehber yayınlamıştır. Yayınlanan bu rehbere göre, "*veri koruma etki değerlendirmesi*, kişisel

verilerin işlenmesinde, işlemenin amacının, gerekliliğinin ve oranının belirlenerek, işleme sürecinin tanımlanmasına ve kişisel verilerin işlenmesinden kaynaklanabilecek olası risk ve ihlallerin öngörülüp, bunların muhtemel olumsuz etki ve sonuçlarının en aza indirilmesini sağlayacak tedbirlerin alınmasına, olanak verecek şekilde risk yönetiminin hedeflendiği, değerlendirme, öngörü ve 2016/679 sayılı Tüzük'ün getirdiği hükümlere uygunluk oluşturma süreci" olarak tanımlanabilir. Bu bağlamda veri koruma etki değerlendirmesi yapılmasının, hem kişisel verileri işlenen veri süjeleri, hem de bu işleme faaliyetini gerçekleştiren tüzel kişiler açısından bazı avantajları olduğu söylenebilir. Zira veri koruma etki değerlendirmesi yöntemi vasıtasıyla olası risklerin henüz gerçekleşmeden elenmesi yolu ile, hem veri süjeleri açısından hak ihlallerinin önlenerek, temel hak ve özgürlüklerin daha iyi korunmasının sağlanmasının, hem de 2016/679 sayılı Tüzük'ün hükümlerine uyulmaması sebebiyle kesilecek idari para cezalarının engellenmeye çalışılmasının hedeflenmekte olduğu söylenebilir (A29WP, 2017: 248, s.4).

Teknolojik gelişmelere paralel olarak kapsamı, nitelik ve niceliği günden güne gelişerek artan otomatik veri işleme teknik ve süreçleri, ekonomik gayelerin gerçekleştirilmesine yönelerek, öncelikli olarak temel hak ve özgürlüklerin korunmasını hedeflemedikleri için, bu otomatik işlemelerden kaynaklanan kişisel veri ihlalleri de doğal olarak artmıştır. Bu gelişmeler, kişisel verilerin işlenmesine başlanmadan önce, amaçlanan işlemenin olası etki ve sonuçlarının incelenerek, risk analizi yapılmasının akabinde, ortaya çıkabilecek muhtemel ihlallere karşı alınacak tedbirlerin belirlenmesi bağlamında, Tüzük'ün 35.maddesi ile ortaya konan veri koruma etki değerlendirmesi tekniğinin önemini bir kere daha ortaya koymaktadır. 2016/679 sayılı Tüzük'ün 35/1.maddesinden anlaşılacağı üzere, ileri teknoloji kullanılarak yapılan ve doğası, kapsamı, içeriği ve amaçları gereği, veri süjesinin hak ve özgürlüklerinin yüksek olasılıkla ihlali neticesini doğurabilecek nitelikteki, işleme faaliyetlerine başlanmasından önce, veri kontrolörü tarafından, veri koruma etki değerlendirmesinin yapılması zorunludur. Bu sayede önceden alınacak tedbirler vasıtasıyla, kişisel verilerin işlenmesi neticesinde ortaya çıkabilecek olumsuz sonuçların öngörülerek, engellenmesi yahut en aza indirilmesi hedeflenmektedir (A29WP, 2017: 248, s. 8; Bieker, Fiedewald, Hansen, Obersteller ve Rost, 2016, s. 21-22, 24-25; EUAFR, 2018, s. 179-181). Ancak her ne kadar madde 35/1'in lafzından, veri koruma etki değerlendirmesinin veri kontrolörü tarafından işleme faaliyetine başlanmasından önce yapılması gerektiği anlaşılsa da, aslında veri koruma etki değerlendirmesinin sadece bir kereye mahsus yapılması gereken bir prosedür değil, riskin ortaya çıkma ihtimalinin olduğu herhangi bir zamanda da tekrarlanabilecek bir süreç olduğu unutulmamalıdır (A29WP, 2017: 248, s. 14).

Tüzük'ün 35/3.maddesi kapsamında ise, veri koruma etki değerlendirmesinin mutlaka yapılması gereken özel durumlar sayılmıştır. Madde 35/3'e göre, "profilleme yapılması da dahil olmak üzere, kişilik özelliklerine dair kapsamlı inceleme yapılmasına ilişkin olan otomatik işleme faaliyetleri ile, otomatik işleme faaliyetlerinin sonuçlarının veri süjesi hakkında yasal etkiler doğurabilecek nitelikteki önemli kararların alınmasında kullanılacak olması durumu, ile (madde 35/3 a); Tüzük'ün 9/1.maddesinde ifade edilen hassas kişisel verilere ilişkin işleme faaliyetleri ile, yine Tüzük'ün 10.maddesinde belirtilen cezai hüküm ve suçlara ilişkin işleme faaliyetleri (madde 35/3 b); ve, halka açık alanların sistematik bir şekilde ve geniş ölçekte izlenmesine ilişkin işleme faaliyetleri (madde 35/3 c)", veri koruma etki değerlendirilmesinin mutlaka yapılmasının gerektiği özel durumlar

kapsamında sayılmıştır. Yine 2016/679 sayılı Tüzük madde 35/4'e göre, yetkili denetim makamı tarafından, hangi veri işleme faaliyetleri öncesinde mutlaka bir veri koruma etki değerlendirmesi yapılmasının gerektiği hususu, özel olarak belirlenip kamuoyuna açıklanarak, bu konuda Avrupa Veri Koruma Kurulu da yine ilgili denetim makamınca bilgilendirilmelidir. Denetim makamının veri koruma etki değerlendirmesi yapılmasına gerek olmayan işleme faaliyetlerinin neler olduğuna ilişkin de bir liste oluşturarak kamuoyunu bilgilendirebileceği Tüzük madde 35/5 kapsamında belirtilmiştir. Yapılan veri koruma etki değerlendirmesi neticesinde, işleme faaliyetinin önlem alınmaması halinde, veri süjesi açısından yüksek risk oluşturacağı sonucuna ulaşılması halinde, işleme faaliyetine başlanmadan önce, veri kontrolörünün, denetim makamını bu hususta bilgilendirerek, izlenecek yola ilişkin olarak denetim makamına danışması gerektiği hususunun altı da Tüzük madde 36 ile çizilmiştir (A29WP, 2017: 248, s. 18; Tikkinen-Piri, Rohunen ve Markkula, 2018, s. 143).

Kişisel Verilerin Korunmasında Yaptırım Mekanizmaları

Kişisel verilerin korunmasında uygulanacak yaptırım mekanizmaları ve para cezalarına ilişkin düzenlemeler, 2016/679 sayılı Tüzük'ün 77 ila 84.maddeleri arasında düzenlenmiştir. Bu düzenlemeler birlikte değerlendirildiğinde, yaptırım mekanizmalarının tasarlanmasında, denetim makamlarından başlayarak üye devlet mahkemelerine kadar uzanan çok katmanlı yönetişim yaklaşımının benimsendiği anlaşılmaktadır (Spataru-Negura ve Lazar, 2018, s. 664).

2016/679 sayılı Tüzük ile getirilen bu yeni düzenlemeler, mülga 95/46/EC sayılı Direktif'teki düzenlemelerle karşılaştırıldığında, Tüzük ile, kişisel verilerin işlenmesinde hukuka aykırı davranılması durumunda, kontrolör ve işleyicilere yüklenen sorumluluğun, birbirleriyle eşit düzeye getirilerek, genişletildiği görülmektedir (A29WP, 2017: 253, Introduction). Ayrıca yine Tüzük kapsamında kişisel verilerin korunması hususunda karşılaşılan sorunlara, daha elverişli çözüm mekanizmaları getirilmeye çalışıldığı da anlaşılmaktadır. Bu bağlamda, Tüzük'ün kabulüyle, kişisel verilerin hukuka aykırı işlenmeleri sonucu uygulanacak çözüm ve yaptırımlar, Birlik düzeyinde birbirleriyle uyumlu hale getirilmeye çalışılarak, idari para cezası miktarları da dahil, yaptırımların kapsam ve içerikleri artırılmıştır. Kişisel verilerinin ihlal edildiğini iddia eden veri süjesinin şikayetini ulaştırdığı yetkili denetim makamı, yapılan şikayete ilişkin olarak Tüzük kapsamında getirilen çözüm yollarını ve yaptırımları uygularken, somut olayın tüm özelliklerini bir arada değerlendirerek karar vermekle yükümlüdür. Bu bağlamda uygulanacak çözüm yolları ile yaptırımların etkili, orantılı ve caydırıcı nitelik taşımaları ve Birlik çapında aynı ya da benzer nitelikteki ihlallere eşdeğer çözüm ve yaptırımlar getirilerek uygulamada tutarlılığın sağlanması da yetkili denetim makamlarının sorumluluğundadır. Yaptırımların uygulanmasında Birlik çapında uyumun yakalanabilmesi için ise, düzenli yapılacak atölye çalışmaları gibi çeşitli işbirliği mekanizmaları aracılığıyla denetim makamları arasında bilgi paylaşımı ve aktif katılımın sağlanması gerekli ve önemlidir (A29WP, 2017: 253, Principles; Alexe, January-June 2018, s. 71-73).

2016/679 sayılı Tüzük ile, siyasi baskı da dahil her türlü baskıdan uzak tutularak bağımsız niteliklerinin korunacağının altı çizilen denetim makamlarının, işbu Tüzük hükümlerinin etkili uygulanmasının sağlanmasına ilişkin önemli yetkilerle donatıldığı görülmektedir (A29WP, 2017: 253, Introduction). Zira Tüzük madde 77 kapsamında, kişisel verilerinin, yasal olmayan şekillerde

işlendiğini düşünen veri süjesinin, ilgili denetim makamlarına doğrudan başvurarak, şikayette bulunma hakkı düzenlenmiştir. Denetim makamı, veri süjesinin yapmış olduğu şikayeti değerlendirirken, bu şikayetin gidişatına ve sonucuna ilişkin süreçten veri süjesini bilgilendirerek haberdar etmekle yükümlüdür. Denetim makamı, yapılan bu şikayet başvurusunu cevapsız bırakır ya da şikayetin gidişatına veya sonucuna ilişkin veri süjesini üç ay içerisinde bilgilendirmez ise, veri süjesinin, Tüzük madde 78/1'e göre, denetim makamları karşı "*etkili hukuk yollarına başvuru hakkı (The Right to an Effective Judicial Remedy)*" da bulunmaktadır (Hofmann, 2013)[5]. Etkili hukuk yollarına başvuru hakkı kapsamında, her gerçek ve tüzel kişinin, denetim makamlarının verdiği bağlayıcı nitelikteki kararlara karşı, ilgili denetim makamının yerleşik bulunduğu üye devlet mahkemelerinde yargı yoluna başvuru haklarının da bulunduğunun altı yine Tüzük'ün 78/1.maddesinde çizilmiştir. Denetim makamlarının bağlayıcı kararlarına karşı, veri süjeleri tarafından yetkili mahkemelere başvurulması halinde, uyuşmazlıkların çözümü hususunda ilgili mahkemeler tam yargı yetkilerini kullanarak her türlü hususu inceleyebileceklerdir (Voigt ve Von Dem Bussche, 2017, s. 214).

Tüzük'ün 79. maddesinde de bu kere, veri süjesinin, kontrolör veya işleyiciye karşı etkili hukuk yollarına başvurma hakkı düzenlenmiştir. Madde 79'a göre, Tüzük'te düzenlenen haklarının ihlal edildiğini iddia eden veri süjesi, 78. madde kapsamında bu hususta denetim makamları başvuru hakkına halel gelmeden, ilgili işleme faaliyetini gerçekleştiren veri kontrolörü veya işleyicisine karşı, bunların kurulu bulundukları üye devlet mahkemelerinde etkili hukuk yollarına başvurabileceklerdir.

Tüzük'ün 82. maddesinde ise, kişisel verilerinin korunmasına ilişkin haklarının ihlali sebebiyle, maddi-manevi zarara uğrayan veri süjesinin, ilgili kontrolör ve işleyiciden tazminat isteme hakkı düzenlenmiştir. Madde 82'ye göre, kontrolör veya işleyicinin tazminat yükümlülüğünün doğabilmesi için, işbu Tüzük ile düzenlenen sorumluluklarını yerine getirmemeleri veya Tüzük'e aykırı talimat vermek sureti ile bu zararın oluşmasına sebep olmaları gerekmektedir. Birden fazla kontrolör veya işleyicinin zarara sebep olan işleme faaliyetine dahil olmaları durumunda ise, bunların her birinin, veri süjesinin katlanmak zorunda kaldığı zararın tamamen ve etkili bir şekilde tazmininden sorumlu olacakları da madde 82/4 kapsamında belirtilmiştir. Kontrolör veya işleyici, 82. maddedeki tazminat yükümlülüğünden, ancak ve ancak somut olaydaki zararın oluşmasında herhangi bir sorumluluklarının bulunmadığını ispatlamaları koşuluyla kurtulabilirler. Ancak kontrolör veya işleyicinin, zararın oluşmasında küçük de olsa bir sorumlulukları olduğu taktirde, madde 83 kapsamında tazminat yükümlülüğü doğmaktadır. Burada dikkat çekici bir diğer konu da,

[5] 2016/679 sayılı Tüzük'ün 78.maddesinde düzenlenen "*Etkili Hukuk Yollarına Başvuru Hakkı*"nın kökenleri, Avrupa İnsan Hakları Sözleşmesinin (European Convention on Human Rights) 13.maddesi kapsamındaki "*Etkili Başvuru Hakkı (Right to an Effective Remedy)*"na dayanmaktadır. Bu hak, özellikle kamu kurum ve kuruluşları karşısından, bireylerin hak ve özgürlüklerinin korunması temel prensibine dayanır. Avrupa Temel Haklar Şartı (Charter of Fundamental Rights of European Union) madde 47'de düzenlenen "*Etkili Hukuki Bir Yola Başvurma ve Adil Yargılanma Hakkı*" da bu temelde düzenlenmiştir. Daha fazla bilgi için bkz. Hofmann, 2013;
Avrupa Birliği Temel Haklar Şartı: madde 47 – "*Etkili Hukuki Bir Yola Başvurma ve Adil Yargılanma Hakkı: Birlik hukuku tarafından teminat altına alınmış olan hakları ve özgürlükleri ihlal edilen herkes, bu maddede belirtilen şartlara Uygun olarak bir mahkemede hukuki yola başvurma hakkına sahiptir.*
Herkes daha önceden yasa ile tesis edilmiş bağımsız ve tarafsız bir mahkemede makul bir sure içinde yapılacak adil ve kamuya açık bir duruşma yapılması hakkına sahiptir. Herkes kendisine bilgi verilmesi, savunulması ve temsil edilmesi fırsatına sahip olmalıdır.
Gerekli imkanlara sahip olmayan herkese, bu yardımın adalete etkin bir şekilde ulaşmasının sağlanması için gerekli olması koşulu ile hukuki yardım sağlanacaktır." İşbu 47.madde tercümesi Avrupa Birliği Türkiye Delegasyonu resmi web sitesinde bulunan Avrupa Birliği Temel Haklar Bildirgesi tercüme metninden aynen alıntılanmıştır. https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708 (Son Erişim Trh.).

mülga 95/46/EC sayılı Direktif ile mücbir sebep hallerinde kontrolörlere tanınan tazminat yükümlülüğünden kurtulabilmeye ilişkin istisnanın, 2016/679 sayılı Tüzük ile tanınmamasıdır (Spataru-Negura ve Lazar, 2018, s. 664; Voigt ve Von Dem Bussche, 2017, s. 205-208; 95/46/EC sayılı Direktif, Recital 55).

Tüzük madde 80'e göre ise, veri süjesi, 77, 78, 79 ve 82. maddelerde düzenlenen haklarını, bizzat kendisi kullanabileceği gibi, yasalar dahilinde kurulmuş olan ve kişisel verilerin korunması hususunda aktif olarak kamu yararına çalışan, kar amacı gütmeyen dernek, kuruluş veya birliği de bu konularda vekaleten yetkilendirebilme hakkına sahiptir.

Kişisel verilerin korunmasına ilişkin Tüzük hükümlerine aykırı davranılması sonucu denetim makamlarınca kesilebilen ve somut olayın özelliklerine göre etkili, orantılı ve caydırıcı olacak nitelikteki idari para cezaları, Tüzük'ün 83. maddesi kapsamında düzenlenmiştir. Yetkili denetim makamlarınca somut olay kapsamında, idari para cezası kesilip kesilmeyeceği veya cezanın miktarı belirlenirken, 83/2.maddede yer alan aşağıdaki hususlar göz önüne alınmalıdır: "İşleme faaliyetinin doğası, kapsam ve amacı dikkate alındığında, somut olayda ortaya çıkan ihlalin kapsam ve niteliği ile süresi, ihlalden etkilenen veri süjelerinin sayısı ve etkilenme dereceleri (*madde 83/2 a*); İhlalin bir kasıt yahut ihmalden kaynaklı olup olmadığı (*madde 83/2 b*); Veri süjelerinin uğradıkları zararı hafifletmek adına kontrolör veya işleyici tarafından herhangi bir işlem yapılıp yapılmadığı (*madde 83/2 c*); Tüzük'ün 25.maddesinde düzenlenen tasarımla ve varsayılan ayarlarla veri koruma ilkeleri (privacy by design ve privacy by default) ile 32.maddesi kapsamındaki kişisel verilerin güvenli bir şekilde işlenebilmesi için gerekli, uygun ve yeterli teknik ve idari tedbirlerin alınıp alınmadığı konularında kontrolör ve işleyicinin sorumluluk düzeyinin ne olduğu (*madde 83/2 d*); Kontrolör ve işleyicinin daha önceden benzer bir ihlal gerçekleştirip gerçekleştirmediği (*madde 83/2 e*); İhlalin giderilmesi ve olası olumsuz etkilerinin giderilmesi için denetim makamı ile işbirliği yapılıp yapılmadığı (*madde 83/2 f*); İhlalden etkilenen kişisel veri türlerinin neler olduğu (*madde 83/2 g*); İhlalin veri kontrolör veya işleyicisi tarafından yetkili denetim makamına bildirilip bildirilmediği, bildirildi ise ne kapsamda bildirim yapıldığı (*madde 83/2 h*); Veri kontrolör veya işleyicisinin, daha önceden, Tüzük'ün 58/2.maddesinde sayılan, denetim makamının düzeltici yetkileri kapsamındaki uyarı, kınama gibi yaptırımlara maruz kalıp kalmadığı (*madde 83/2 i*); Tüzük'ün 40.maddesi kapsamındaki onaylı davranış kurallarına veya 42.maddedeki onaylı belgelendirme mekanizmalarına uyulup uyulmadığı (*madde 83/2 j*); Somut olayda ihlal nedeniyle doğrudan ya da dolaylı olarak elde edilen maddi menfaatler yahut önüne geçilen kayıplar gibi ağırlaştırıcı veya hafifletici faktörlerin bulunup bulunmadığı (*madde 83/2 k*)", hususları somut olayda, idari para cezalarının uygulanıp uygulanmayacağı veya uygulanacak ise bu cezaların miktarlarının ne olacağının belirlenmesinde etkilidirler.

Kişisel verilerin ihlali halinde uygulanacak idari para cezalarının üst limitleri, söz konusu ihlalin kapsam ve niteliğine göre, Tüzük'ün 83/4 ve 83/5.maddelerinde iki kategori halinde düzenlenmişlerdir. 2016/679 sayılı Tüzük ile getirilen idari para cezalarının niteliklerine bakıldığında bu cezaların, Tüzük kapsamında doğrudan uygulanan en güçlü yaptırım mekanizmaları olduğu söylenebilir. 2016/679 sayılı Tüzük'ün 83/5.maddesi kapsamında düzenlenen ve ağır ihlaller olarak nitelendirilebilen durumlarda, sorumlulara, 20 milyon Avro'ya

veya bir önceki mali yılın küresel cirosunun %4'üne kadar –hangisi daha fazla ise o uygulanacak şekilde- idari para cezası kesilebilmektedir. Tüzük madde 83/4'te ise, daha hafif ihlaller için, 10 milyon Avro'ya veya bir önceki mali yılın küresel cirosunun %2'sine kadar –hangisi daha fazla ise o uygulanacak şekilde- idari para cezası uygulanabileceği hüküm altına alınmıştır (Albrecht, 2016, s. 287; Golla, 2017, s. 74).

İlgili Tüzük'ün 84. maddesi kapsamında, üye devletlerin, Tüzük'ün 83.maddesi ile idari para cezası kesebilmeleri için belirlenen genel hükümlerin kapsamına dahil olmayan diğer ihlallere ilişkin cezaların miktar ve uygulama koşullarını, yapacakları etkili, orantılı ve caydırıcı nitelikteki yasal düzenlemelerle hüküm altına alabilecekleri düzenlenmiştir. Diğer bir ifade ile, Tüzük madde 84 ile, üye devletlere, Tüzük'ün 83. maddesi kapsamına girmeyen ihlallerin gerçekleşmesi halinde verilecek cezalara ilişkin olarak bir takdir yetkisi tanındığı görülmektedir.

Tüzük ile idari para cezalarının bu derece yüksek seviyelere yükseltilmesi ilk etapta büyük tartışmalara yol açmıştır. Ancak bu tartışmalar yapılırken, kişisel verilerin, demokratik toplum yaşamının olmazsa olmazlarından biri olan temel hak ve özgürlükler bağlamında hazırlanarak, Lizbon Antlaşması'na atıf yoluyla dahil edilip, Avrupa Birliği hukukunda kurucu antlaşmalar düzeyine yükselen Avrupa Temel Haklar Şartı kapsamında tanınarak koruma altına alındığı unutulmamalıdır. Bu sebeple kişisel verilerin, uyumlu yasalar ve güçlü yaptırımlar kapsamında, Birlik düzeyinde eşit ve yüksek korumadan yararlanmaları, Birlik'in etik değerlerinin dayandığı temel hakların korunmasının güçlendirilmesi bağlamında, sosyal ve toplumsal gelişim bakımından önemli olduğu gibi, bu yolla gerçek ve tüzel kişiler bakımından oluşturulacak güven ortamının Avrupa dijital tek pazarında işlem hacminin artırılmasına yardımcı olarak, ekonomik büyümeye katkıda bulunması, bakımından da önemlidir.

Sonuç ve Değerlendirme

Avrupa Birliği'nde Veri Koruma Reformu yapılması ihtiyacının ortaya çıkmasının pek çok sebebi bulunmaktaydı. Bu sebeplerden en önemlilerinden biri, bilgi ve iletişim teknolojileri alanında ortaya çıkan önlenemez gelişmeler ve artan internet kullanımı sonucunda, hayatın sosyal, siyasal, ekonomik manada her alanına değen dijitalleşme neticesinde Birlik hukukunda bir temel hak olarak tanınan kişisel verilere yönelen tehditlerin artmasıdır. Nitekim gelişen dijital teknolojiler sayesinde hem kişisel verilerin toplanma ve çeşitli şekillerde işlenme kapsam ve niteliklerinde devrim boyutunda değişiklikler meydana gelmiş, hem internet kullanımının artması sonucu sınırlar arası veri trafiği sıklaşmış, hem de özellikle Bulut teknolojiler, veri madenciliği, Büyük Veri (Big Data), yapay zeka gibi teknik ve uygulamaların yaygın kullanımı sebebiyle, bireylerin kişisel verileri üzerindeki kontrolleri giderek zayıflayarak, bu verilerin yetkisiz üçüncü kişilerce işlenme oranları artmıştır. Bu artış, Avrupa Birliği hukukunda temel hak ve özgürlükler kapsamında tanınan kişisel verilerin, Birlik düzeyinde uyumlulaştırılmış güçlü yasalarla ve gelişen teknolojiler bağlamında ortaya çıkan yeni risklerle başa çıkabilecek yeni tekniklerle korunmasının önemini net şekilde ortaya çıkarmıştır.

Avrupa Birliği, ayrıca, kişisel verilerin uyumlu ve güçlü yasalarla Birlik çapında korunarak, tüketici güveninin yükseltilmesinin, genel küresel ekonomi içindeki payını her geçen gün daha fazla artıran dijital ekonomiden alacağı payın yükseltilmesi için de önemli ve gerekli olduğunu, henüz 2000'li yılların başında idrak ederek, kişisel verilerin korunmasına ilişkin çalışmalarını hızlandırmıştır.

Yaşanan tüm bu gelişmelerle birlikte, kişisel verilerin korunması ve serbest dolaşımlarının sağlanması bağlamında çerçeve hükümler getirerek diğer hususların düzenlenmesini üye devletlere bırakan 95/46/EC sayılı Direktif'in, Birlik genelinde farklı uygulamaların ortaya çıkmasına yol açarak, Birlik'in parçalı yapısını perçinlediği ve dijital teknolojiler kapsamında beliren yeni risk ve tehditlerle başa çıkmakta yetersiz kaldığı da anlaşılmış ve bu da Birlik'in, Veri Koruma Reformu yapılması ihtiyacını pekiştirmiştir. Böyle bir ortamda ortaya konarak, Avrupa Birliği'ne üye tüm devletlerde aynı anda, doğrudan uygulanabilir olarak yürürlüğe giren, 2016/679 sayılı Genel Veri Koruma Tüzüğü, yasal düzenlemelerin Birlik düzeyinde uyumlulaştırılması sebebiyle, kişisel verilerin korunması ve serbest dolaşımlarının sağlanması anlamında atılmış dev bir adım niteliğindedir.

Kişisel veri güvenliğinin sağlanmasına ilişkin olarak Tüzük kapsamında ortaya konan "tasarımla ve varsayılan ayarlarla veri koruma (*Privacy by design ve Privacy by default) ilkeleri, takma ad (pseudonymisation), şifreleme (encryption), veri koruma etki değerlendirmesi*" gibi yeni teknik ve uygulamalar ile birlikte getirilen güçlü yaptırım mekanizmaları ve artırılmış idari para cezaları; sayesinde temel haklar kapsamında tanınarak koruma altına alınan kişisel verilerin, gelişen dijital teknolojiler ve artan internet kullanımı karşısında daha güçlü şekilde korunmasını temin etme yolunda, önemli bir mesafe kat edildiği söylenebilir. Ancak bilgi ve iletişim teknolojileri kapsamındaki gelişmelerin devam ettiği de göz önüne alındığında, Avrupa Birliği'nin kişisel verilerin korunması ve serbest dolaşımlarının sağlanması hususlarında gelecekte de ortaya çıkamaya devam edecek yeni risk ve tehditlere karşı uyanık olarak izlemede kalması ve gerektiğinde bu yeni risklere ilişkin yeni teknik ve yaptırımlar ortaya koyması kişisel verilerin etkili bir şekilde korunmaya devam edilebilmesi bakımından önemli ve gereklidir.

Kaynakça

Albrecht, J.P. (2016). How the GDPR will change the world. *European Data Protection Law Review*, *2*(3), 287-289.

Alexe, I. (2018, Ocak-Haziran). Personal data protection, the sanctioning regime provided by regulation (EU) 20167679 on the protection of personal data, *Law Review*, *VIII*(1), 60-73.

Başalp, N. (2015). Avrupa Birliği veri koruması genel regülasyonu'nun temel yenilikleri, *Marmara Üniversitesi Hukuk Fakültesi Dergisi, 21*(1), 77-105.

Bieker, F., Fiedewald, M., Hansen, M., Obersteller, H. ve Rost, M. (2016). A process for data protection impact assessment under the European general data protection regulation. S.Schiffner ve diğerleri (Ed.), *Privacy Technologies and policy* (s.21-37) içinde. İsviçre, Springer, doi: 10.1007/978-3-319-44760-5.

Cavoukian, A. (2010, Mayıs). Privacy by Design, The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, *PbD*. Erişim adresi: http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf

Cavoukian, A. (2010, Ağustos). Privacy by Design: the Definitive Workshop. A Foreword by Ann Cavoukian. *Identity in the Information Society (IDIS), 3*(2), 247-251.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J., Le Métayer, D., Tirtea, R., Schiffner, S., (2014). *Privacy and Data Protection by Design from Policy to Engineering*. ENISA, Erişim adresi: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

De Hert, P. ve Papakonstantinou, V. (2012). The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals. *Computer Law & Security Review*, *28*(2), 130-142.

Diaz Diaz, E. (2016). The new European Union general regulation on data protection and the legal consequences for institutions. *Church, Communication and Culture*, *1*(1), 206-239.

Esayas, S.Y. (2015). The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules: Beyond the "All or Nothing" Approach. *European Journal of Law and Technology*, *6*(2), 1-23.

Golla S.J. (2017). Is data protection law growing teeth? The current lack of sanctions in data protection law and administrative fines under the GDPR. *Journal of Intellectıal Property, Information Technology and E-Commerce Law*, *70*(8/1), 70-78.

Hofmann, H. C. (2013). The right to an 'effective judicial remedy' and the changing conditions of implementing eu law. Lüksemburg Üniversitesi, Hukuk Fakültesi, Çalışma Kağıdı Serisi, No.2, Lüksemburg. Erişim adresi: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2292542

Mansfield-Devine, S. (2017). Meeting the needs of GDPR with Encryption. *Computer Fraud and Security, 9,* 16-20.

Oxman, S.A. (2000). Exemptions to the European Union personal data privacy directive: Will they Swallow the directive?. *Boston College International and Comparative Law Review*, *24*(1), 191-203.

Parliament, E. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities, number L(281)*, 31-50.

Regulation, G. D. P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. *Official Journal of the European Union (OJ)*, *59*(1-88), 294.

Sanchez, A. N. (2016). "Privacy by default" and active "informed consent" by layers: Essential measures to protect ICT users' privacy. *Journal of Information, Communication and Ethics in Society*, *14*(2), 124-138.

Spataru-Negura, L.C. ve Lazar, C. (2018). *Lifting the Veil of the GPPR to Data Subjects.* Challenges of the Knowledge Society, Nicolae Titulescu Universitesi, Romanya. Erişim adresi: http://cks.univnt.ro/articles/12.html

Spindler, G. ve Schmechel, P. (2016). Personal data and Encryption in the European general data protection regulation. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, *7*(2), 163-177.

Tikkinen-Piri, C., Rohunen, A. ve Markkula, J. (2018). EU general data protection regulation: changes and implications for personal data collecting companies. *Computer Law and Security Review: The International Journal of Technology Law and Practice*, *34*(1), 134-153.

Voigt, P. ve Von Dem Bussche, A. (2017). *The EU general data protection regulation (GDPR), A practical guide*. İsviçre: Springer.

Wachter, S. (2018). Normative challenges of identification in the internet of things: Privacy, profiling, discrimination and the GDPR. *Computer Law and Security Review, 34*(3), 436-449.

Voss, W.G., (Winter 2016-2017). European Union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting. *The Business Lawyer, 72*(1), 221-234.

Article 29 Data Protection Working Party, (2017). *Guidelines on Personal Data Breach Notification under Regulation 2016/679.* Brüksel: WP250. Erişim adres: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Article 29 Data Protection Working Party, (2017). Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679. Brüksel: WP 253. Erişim adresi: https://knowww.eu/search-tree?t=5ad7131ed39f5aa2bcbf0f34#

Article 29 Data Protection Working Party, (2017). Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is 'Likely to result in a High Risk' for the Purposes of Regulation 2016/679. Brüksel: WP 248. Erişim adresi: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Article 29 Data Protection Working Party, (2018). Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU. Brüksel. Erişim adresi: https://www.aepd.es/sites/default/files/2019-09/art29-statement.pdf

European Commission, (2010). *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A Comprehensive Approach on Personal Data Protection in the European Union, COM (2010) 609 final.* Erişim adresi: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF

European Data Protection Supervisor, (2015). *Opinion 8/2015, Dissemination and Use of Intrusive Surveillance Technologies.* Erişim adresi: https://edps.europa.eu/sites/edp/files/publication/15-12-15_intrusive_surveillance_en.pdf

European Union Agency for Fundamental Rights, (2018). *Handbook on European Data Protection Law*, Luxembourg. Erişim adresi: https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

UK Information Commissioner's Office (ICO), (2019). *Guide to the General Data Protection Regulation (GDPR), Data Protection by Design and Default.* Erişim adresi: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf