GSM SEKTÖRÜNE YÖNELİK DÜZENLEMELER VE ETKİLERİ (KİŞİSEL VERİ KORUMASI BAZINDA)

Akif ONUR
111692004

İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

Yrd.Doç. Dr. Leyla KESER BERBER

2013

GSM SEKTÖRÜNE YÖNELİK DÜZENLEMELER VE ETKİLERİ
(KİŞİSEL VERİ KORUMASI BAZINDA)

IMPACT OF TELECOMMUNICATIONS REGULATION ON DATA PROTECTION

Akif ONUR
111692004

Yrd.Doç. Dr. Leyla KESER BERBER :

Yrd. Doç. Dr. Nilgün BAŞALP :

Yrd. Doç. Dr. Bülent ÖZEL :

Tezin Onaylandığı Tarih : 15.08.2013

Toplam Sayfa Sayısı : 80

Anahtar Kelimeler (Türkçe)	Anahtar Kelimeler (İngilizce)
1) BİLİŞİM HUKUKU	1) ICT LAW
2) VERİ GİZLİLİĞİ	2) DATA PRIVACY
3) VERİ İŞLEME	3) DATA PROCESSING
4) YAKINSAMA	4) CONVERGENCY
5) REGÜLASYON	5) REGULATION

İçindekiler

Özet

İletişim ve teknoloji araçlarının kullanım oranlarında son yıllarda hayli artış görülmüştür. Keşfedilen farklı kullanım metodlarıyla birlikte kişisel verilerin kolay işlenebilmesi ve bu verilerin üçüncü şahıslara kolaylıkla aktarılabilmesi önlemler almayı gerektirmiştir. Özel hayatın gizliliğini esas alan kişisel verilerin korunması temel haklar arasında sayılmaktadır. Bu çalışma kişisel verilerin hukuka uygun bir amaç ve şekilde verilerin işlenmesini, saklanmasını ve silinmesini ışık tutmayı amaçlayan AB direktif ve regülasyon otoriterileri düzenlemelerini baz almaktadır. Bu düzenleme ve direktifler ülkemizde ve başta AB ülkeleri olmak üzere kişisel verilerin gizliliği için gerekli teknik ve hukuki tedbirlerin alınmasını gerekli kılmaktadır. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik kapsamında kişisel veri ihlallerinin regulatör otoritelere ve bilgileri işlenmek suretiyle etkilenen kişilere bildirilmesi ve rıza alınması gerekmektedir. Gerekli uyarı ve yaptırımlar ile elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin gizliliğin korunmasına önem vermeleri sağlanmaya çalışılmaktadır. Kişisel verilerin işlenmesini, saklanmasını ve korunmasını ilgili AB ve BTK uygulamaları nezdinde mevcut Türkiye durum analizi ve ilgili ülke düzenlemelerine kapsayıcı türden yer verilmektedir.

Abstract

In recent years, there has been a significant increase in the means of communication and technology. The ease of the process and transfer to third parties of personal data necessitated preventive actions. Protection of personal data that aims the safety of the privacy of private life is considered one of the fundamental rights. This work is based on EU regulations regarding the process, storage, and erasure of personal data. These regulations and instructions require that the technical and legal measures must be taken in order fort he protection of such data, not only in the EU countries, but also in our country. Regulations Regarding the Process of Personal Data and The Protection of Privacy fort he Electronical Communication Sector dictates that the facts of violation of personal data must be informed to regulating authorities and shared with affected parties. With necessary warnings and sanctions, it is aimed that people in the communications sector pay attention to the protection of personal data. Situation analysis about Turkey with regards to the EU and 'Bilgi Teknolojileri İletişim Kurumu' (Information Communication Technologies Institution) regulations about the process, storage, and protection of personal data will be covered in this work in detail.

Kullanılan Kısaltmalar

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ABGS	Avrupa Birliği Genel Sekreterliği
ABİDA	Avrupa Birliğinin İşleyişine Dair Antlaşma
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AK	Avrupa Komisyonu (European Commission (EC))
BM	Birleşmiş Milletler (United Nations)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CDR	Çağrı Detay Kayıtları (Call Detail Records)
EHK	Elektronik Haberleşme Kanunu
ENISA	Avrupa Şebeke ve Bilgi Güvenliği Ajansı
FCC	Amerika Birleşik Devletleri Haberleşme Komisyonu
IP	Internet Protokolü (Internet Protocol)
IPTV	Internet Protokollü TV
ISDN	Tümleşik Hizmetler Sayısal Şebekesi
LBS	Konum Tabanlı Servisler (Location Based Services)
KVKKT	Kişisel Verilerin Korunması Kanun Tasarısı
MMS	Çoklu Ortam Mesajlaşma Hizmeti
MSISDN	Abone Telefon Numarası
OFCOM	İngiltere İletişim Düzenleme Kurumu
ONP	Açık Şebeke Sunumu
PET	Gizliliği Artırıcı Teknolojiler (Privacy Enhancing Technologies)
RFID	Radyo frekanslı tanımlama (Radio Frequency Identification)
SMS	Kısa Mesaj Servisi (Short Message Service)
URL	Tekbiçimli Kaynak Konumlayıcı (Uniform Resource Locator)
VKÇG	Veri Koruma Çalışma Grubu
VOIP	Voice Over Internet Protocol

Kaynakça

- *Council of Europe*, Avrupa İnsan Hakları Sözleşmesi, M.8,
- *Council of Europe*, AB Temel Haklar Şartı, M.7, 8,
- *BM*, Evrensel İnsan Hakları Beyannamesi, M.12,
- *BM*, Bireysel ve Siyasal Haklar Sözleşmesi, M.17,
- *BM*, Kişisel Verilerin İşlenmesine İlişkin Tavsiye Kararı,
- *OECD*, Kişisel Verilerin Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeler,
- *Council of Europe*, 108 Numaralı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme,
- *Council of Europe*, 95/46/AT sayılı Avrupa Parlamentosu ve Konseyinin Kişisel Veriler Kararı,
- *Maastricht, EU*, 2007, Treaty of Maastricht on European Union,
- *ONP* çerçeve direktifi, Abl. EG Nr. L. 295/23 v. 29.10.1997,
- *Caprioli, E, Saadoun, Y, Cantero I,* "The Right To Digital Privacy",
- *European Survey*, Rutgers Journal of Law & Urban Policy,
- *Burgsdorff,W*:www.europa.eu.int/comm/intepnel_market/en/dataprot/news /decision.pdf,
- *Civelek, D,* DPT Kişisel Verilerin Korunması ve Yapılanması
- *Dinc, E*, "Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye'nin Durumu",
- *Özdemir, H,* Kişisel verilerin özel hukuk hükümlerine göre korunması,
- *Halen, F, Wächter, M,* Wiechert/Schmidt/Königshofen,
- *Berberoğlu, T,* Gizliliği Koruyan Bulanık Veri Madenciliği Yöntemi,
- (Definition Meta Model For ITIL) http://link.springer.com/chapter/10.1007%2F978-0-387-78578-3_39,
- *Kaboğlu, İ,* Özgürlükler Hukuku, Afa Yayınları, İstanbul 1999,
- *David, B, Simon, D,* Global Trends in Privacy Protection: an International Survey,

- *Şahin, O,* EHS Kişisel Verilerin İşlenmesi
- *Okur, N,* anayasa hukuku açısından özel hayatın gizliliği ve korunması
- *Hornung G*, The Federal Constitutional Court and the Online Searching Judgement 2009, http://www.cpdpconferences.org/Resources/HornungGerrit.pdf,
- Borking vd., 2003
- Veri Koruma Direktifi
- DUTCHDPA, 2009
- EDPS, 2010
- VKCG, 2010
- ABGS, 2010
- Drucker, 1993
- Coase, 1939
- Peters, T, Search For Excellenge
- Telekommunikationsrecht der Bundesrepubli, Heidelberg 1999
    - *Article 29 Data Protection:* Working Party,Future Work on Codes of Conduct, http://ec.europa.eu/iustice/policies/privacy/docs/wpdocs/1998/wen.pdf,
    - *Article 29 Data Protection:* Working Party, 1999, Recommendation on theInclusion of the Fundamental Right to Data Protection in theEuropean Catalogue of Fundamental Rights, http://ec.europa.eu/iustice/policies/privacy/docs/wpdocs/1999/wp26e n.pdf
    - *Article 29 Data Protection:* Working Party, 2004, Opinion 5/2004 on Unsolicited Communications for Marketing Purposes under Article 13 of Directive 2002/58/EC, http://ec.europa.eu/iustice/policies/privacy/docs/wpdocs/2004/wp90 en.pdf
    - *Article 29 Data Protection:* Working Party, 2005, Opinion on

the Use of Location Data With a View to Providing Value-Added Services, http://ec.europa.eu/iustice/policies/privacv/docs/wpdocs/2005/wp115 en.pdf

- *Article 29 Data Protection:* Working Party, 2007, Opinion 4/2007 on the Concept of Personal Data, http://ec.europa.eu/iustice/policies/privacy/docs/wpdocs/2007/w p136 en.pdf
- *Article 29 Data Protection:* Working Party, 2009, The Future of Privacy, http://ec.europa.eu/iustice/policies/privacy/docs/wpdocs/2009/wp168en.pd
- *Article 29 Data Protection:* Working Party, 2010, Report on ComplianceNational Level of Telecom Providers and ISPs with the Obligations

- *Oxford University Press*, Required from National Traffic Data Retention Legislation on the International Data Privacy Law, 2011
- Privacy and Information Law Report, Westlaw International 2000 to present, Resource Type: Journal, Publisher: Glasser Legalworks
- The Google Privacy Channel, LexisNexis Academic 2009 to present, Resource Type: Journal, Publisher: Newstex LLC

1. GİRİŞ

Vücudumuzu oluşturan en küçük yapı taşına hücre denir. Hücrelerin bir araya gelmesiyle dokuların, uygun dokuların bir araya gelmesiyle organların, organların sistematik çalışmaları sonucu meydana gelen birden fazla sistemin bir araya gelmesiyle de yeryüzündeki en karmaşık canlı metabolizması, insan oluşmuştur. Hücreler bir canlının var olabilmesi için ne anlam ifade ediyorsa "veri" de var olan veya var olmuş canlıların yaşamlarına delalet eden gelecek değeri taşıyan nesnel ve öznel değerler topluluğudur.

Veriler araştırılabilir, deneye tabi tutulabilir, sınıflandırılabilir, işlenebilir veya referans kabul edilerek farklı veriler elde edilmesi yoluna gidilebilmektedir. Verilerin niteliği ve niceliği hakkında bilgi sahibi olunması verilerin kapsamına ve uygulanan veri işleme metodolojisine göre şekillenmektedir. Veriler tek başlarına ve işlenmedikleri sürece bir değer taşımamaktadırlar. Biyoloji için hücre, Bilgi ve İletişim Teknolojileri (BT) ve Mühendislik Bilimlerinde "bit[1]" olan veri işlenip değer kazanarak metalaştığında, kişisellik, gizlilik ve özel hayat kavramlarını ihlal etme girişimlerinde hukukun düzenleyiciliğine ihtiyaç duyulmaktadır.

Konu kapsam gereği Özel Hukuk alanını esasen ilgilendiriyor olsa da çalışmamızı Veri Koruma Hukuku kapsamında, Kişisel Verilerin, Özel Hayatın ve Haberleşme Gizliliğinin Koruması alanları BTK regülasyonları nezdinde GSM teknolojileri kapsamını teşkil edecektir.

[1] Bit, binary türde ikili halde bulunan en küçük veri parçası.

2. KİŞİSEL VERİ KAVRAMI ÖZEL HAYATIN GİZLİLİĞİ

Hayatımıza yeni giren duymaya pek de alışkın olmadığımız, e-ticaret, mobil imza, mobil bankacılık ve e-devlet gibi platformların hayatımızı kolaylaştırıcı etkilerinin yanında, bu işlemler esnasında sanal ortamda sergilemiş olduğumuz davranışlarımızın gözlemlenerek kişi bazlı kampanya ve yönlendirmelere maruz kalarak birilerinin sanki bizi takip ettiği hissini oluşturmaktadır. Teknik olarak bu takibin gerçekleştirilmesinde bir zorluk olmayıp ticari kurguyu destekler olması ve asli niyetler hukuk dışı bir işlem yapmak olmasa da, OECD Genel Sekreteri Angel Gurria'nın ifadesiyle hukuka aykırı çok sayıda fiilin ve failin yer aldığı yeni bir yeraltı ekonomisi oluşturan kişisel verileri İnternet ekonomisinin para birimi olarak tanımlamak mümkündür.[2] Bu sektöre farkında olmadan, günlük yaşantımızda ya da geliştirmiş olduğumuz projelerde destek oluyor olabiliriz, bunun önüne geçebilmek için kanuni esasların ve direktiflerin ve insanlığın en temel onuru olan kişilik kavramının bilinmesi gerekmektedir.

2.1 Özel Hayat ve Gizliliği Kavramı

Kişi-Kişilik Hakları ve Kişisel Veri Kavramı Teknoloji ve Elektronik haberleşme (e-haberleşme) alanında meydana gelen gelişmeler hayatımızı kolaylaştırırken temel hak ve özgürlükleri kısıtlar duruma gelerek, kişinin ve kişiliğin korunmasında önem taşıyan "kişisel verilerin" korunması ilkelerinin belirlenmesini gerekli kılmaktadır.

Meydana gelen gelişmeler kişi temel hak ve özgürlüklerinin koruma önlemlerinin geliştirilmesi ve özel hayata saygı ilkelerinin belirlenmesini gerekli kılmıştır. Herkes özel ve aile hayatına, meskenine ve haberleşmesine saygı gösterilmesini

---

[2] Civelek,D. OECD Genel Sekreteri Angel Gurria, 17 Haziran 2008 tarihinde Kore'de gerçekleştirilen "İnternet Ekonomisinin Geleceği Hakkında Bakanlar Toplantısı"nda, bireyin İnternet Ekonomisinin odağında olduğunu vurgulamış; kişisel verilerin ise bu ekonominin "para birimi" olduğu benzetmesini yapmıştır. Bu konuşmanın ayrıntıları için bkz. http://www.oecd.org/document/8/0,3343,en_2649_34487_40863240_1_1_1_1,00.html

isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.[3] Özel hayat; kişilerin kamuya açık alanlarının hukuk kurallarıyla devlet tarafından korunmasıdır. Bu sosyal devlet olgusunu ortaya çıkaran en büyük etmenlerden bir tanesidir ve Anayasanın 5. Maddesi ile Devletin temel amaç ve görevleri, Türk Milletinin bağımsızlığını ve bütünlüğünü, ülkenin bölünmezliğini, Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddî ve manevî varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır.

2.2 Hukuk ve Teknoloji

Sınırlar ve tanımlar farklı olsa da insan hakları evrenseldir. Sosyal devlet olma anlayışı bu hakları korumayı gerektirir. Hak, bir diğer hakkın varlık sebebini oluşturabilir, haberleşme hakkının tıpkı haberleşme gizliliğini oluşturduğu gibi. Aslında temelde tüm hakların insan onurundan doğmasına karşın her bir hak kendi içinde bir bölünmezlik ve bağımlılık içerse de, özel hayatın gizliliği ve kişilik hakları esas kabul edilmektedir.

II. Dünya Savaşı'ndan sonra devletlerin, bireylere tanınan hak ve özgürlüklerin güvence altına alma çabası, 10 Aralık 1948 İnsan Hakları Evrensel bildirgesinin kabulü ortamının oluşmasına destek sağlamıştır.

Bu bildirgeyle koruma altına alınmaya çalışılan devletin kamu yararı ve bu yarar üzerine kurmuş olduğu stratejiler ile bireyin yararı arasında kurması gereken dengede öz ağırlığın kamudan yana kullanılması halinde bireylerin özgürlüğünü kısıtlamanın önüne geçilmesidir.[4]

Bu kontrol geçmişten bu yana devletin asli görevleri arasında beklenmektedir.

---

[3] 4 Kasım 1950 AB Sözleşmesi Madde 8, TC Anayasa Madde 20

[4] Ergun Özbudun, "Anayasa Hukuku Bakımından Özel haberleşmenin Gizliliği", AÜHFM. 50. Yıl Armağanı, Ankara 1977, s.266.

Ancak neoklasizm dönemiyle birlikte gelişen bilgi teknolojileri bu kontrolün devlet tarafından yapılmasını zorlaştırmaktadır ve IT Projelerinde bu unsuru kapsayacak türde çalışmalar yapılması gerekmektedir.

IT projeleri PMO tarafından atanan bir PM tarafından yürütülür ve PMO Officer tarafından, Proje'nin IT yönetim metodolojilerine uygunluk durumu denetlenmektedir.[5]

Maalesef ülkemizde verilen mühendislik bilimleri eğitimleri içeriğinde etik ve bilişim hukuku gibi kavramlardan yeterince bahsedilmediği için mühendislerimizin bu perspektiflerde bakış acıları tamam kılınamayarak, projelerin hukuki ihtiyaçları karşılanamamaktadır. Bu kontrolün yapılması hukuk ve regülasyon grupları tarafından beklenmekte ve hukuk-teknoloji bacağı entegre olamayarak zayıf bir ölçümlemeye tabi durumda kalınmaktadır. Sözlük anlamı "başkalarından saklanan, duyurulmayan, saklı, mahrem"[6] olan gizlilik kelimesinin herkes tarafından bilindiği ve bu durumun ihlalinin kendi hayatlarımızdan yola çıkılarak eksik bırakılmasının rahatsızlık oluşturacağı bilinmektedir. Ancak kişisel verilerin işlenmesine yönelik bir hukuki süreç ile karşılaşıldığında proje geliştiricilerin proje planlarının kendilerine yöneticileri tarafından paylaşıldığı söylemiyle birlikte hukuk-bilişim koordinasyonunun sağlanmaması noktasında proje paydaş ve yöneticilerinin haklı çıkma çabalarının göz ardı edilmesi gerekmektedir.

Sağduyu bunu gerektirirken, hukuk ise Türkiye'nin uluslararası alanda imzalamış olduğu Avrupa Birliği direktiflerine uymayı gerektirmektedir. Türkiye, üyesi olmadığı birliğin kişisel verilerin elektronik ortamda korunmasına ilişkin çıkarılan direktifleri imzalamıştır. Ancak direktifler, imzalanmış olmasına rağmen çerçeve bir kanunla desteklenmediği için beklenilen ağırlık kazandırılamamıştır.

---

[5] PMO:Project Management Office, PM: Project Manager, IT yönetim metadolojileri: ITIL, PMI, SDLC (Definition Meta Model For ITIL)

[6] Türk Dil Kurumu Sözlük

Bilgi Teknolojileri ve İletişim Kurumu (BTK), kişisel verilerin korunmasına ilişkin olarak hazırlamış olduğu, son direktifi de içeren yönetmelikte kişisel verilerin korunmasına ilişkin uygun düzenlemeleri elektronik haberleşme sektörü için hazırlamış bulunmaktadır.

Yönetmeliklerin kanunları desteklemesi beklenmekle birlikte; henüz kanuni bir dayanak bulamayan yönetmelik, hukuki bir zemin bulmakta güçlük çekmektedir. Beklenti imzalanan uluslararası anlaşmaların ve direktiflerin hukuki dayanağının oluşturulmasıyla karışıklığın ortadan kaldırılması şeklindedir.

Kişisel verilerin korunması, aslında kişiliğin ve kişilerin hukuk tarafından korunan hayat alanlarıyla yakından ilgilidir ve ülkemizde son dönemlerde BTK elektronik haberleşme sektörünün düzenleyicisi olarak bu çalışmalarda öncü ve örnek olmuştur.

2.3 Özel Hayatın Kapsamı Dışından Kalan Alan

Herkesin kolaylıkla ulaşabileceği ve kamu sınırları içinde yaşanan olaylar ortak alan kapsamında değerlendirilerek korunma kapsamında bulundurulmamaktadır. Bu, sabah işe gitmek, alışveriş yapmak, benzin almak veya toplu taşıma araçlarını kullanmak şeklindedir, fakat bu günlük işler için takip edilen lokasyon bilgilerine ulaşmak anlamı taşımamaktadır. Bu verilerin istatistiksel olarak değerlendirilmesi, davranışları ve profilleri belirlemeye yönelik tutumlar, sınırın ihlal edildiği anlamına gelmektedir. İstatistik kurumuna da sahip olan bir ülke olarak istatistikler ve genellemeler ile hareket etmeyi faydalı görürüz ki bu veriler satış politikalarını, yeni bir mağaza/şube lokasyon yerini belirlemek noktasında dahi kullanılabilmektedirler.

Altın değerindeki bu deneyimlerin takibini sürekli kılmak içinse şirketlerimizde veri madenciliği adı altında birimler bulunmaktadır.

Veri Madenciliği kapsamından olabildiğince uzak kalabilmek için "Özel Hayat" kavramını hayatımızda olabildiğince yer bulmasını sağlamak gerekmektedir. Çünkü özel hayat, kimlik hakkını da içermesi sebebiyle; "nedensiz ve açık rıza

olmaksızın gerçek adını, adresini, yaşını, ailevi durumunu, boş zamanlarından yararlanma biçimini, mal varlığını ve günlük alışkanlıklarını açıklamamak üzere kurgulanmış bir hayattır ve koruma altında bulunmaktadır. Aynı şekilde konut ve aile mahremiyeti duygusal yaşama ilişkin gizlilik hakkını da güvence altına almaktadır. Kısaca gizlilik ilkesi, üçüncü kişilerin merak alanı dışında tutulan varlık ortamı olup, her bireyin kişisel, ilişkisel ve ailesel yaşam alanına dışarıdan müdahaleye karşı bulunan mahremiyettir."[7]

Mahremiyet olan bu tip verilerin doğrudan ticari veya dolaylı olarak pazar amaçlı Veri Madenciliği yöntemlerine tabi tutularak işlenmesi ve Veri Ambarlarında saklanarak birtakım faaliyetler gösterilmesi rızasız haberleşme şekline girmektedir ve sektörde bu tür davranışlardan düzenleme ihtiyaçlarını barındırmaktadır.

Bu rıza, Kolluk Kuvvetleri'nin asayişi sağlamak ve izne tabi bazı özel durumları dışında uygun bulunmamakta olup bu verilere başvurulması özel hayatın gizliliği ilkesine ters düşmektedir.

Özel hayatın gizliliğinin korunması dört farklı alanı kapsamına almaktadır:

- Bilgi Mahremiyeti (Information Privacy): Kredi kartı bilgisi ya da tıbbi kayıtlar gibi kişisel bilgilerin elde edilmesi ve toplanmasına ilişkin kuralları düzenleyen bir alandır.
- Fiziki Mahremiyeti (Body Privacy): Medikal araştırmalarda olduğu gibi kişinin fiziksel bütünlüğünün müdahaleci usul ve araştırmalara karşı korunması ile ilgilidir.
- Haberleşme Mahremiyeti (Privacy of Communications): Telefon, e-posta gibi iletişim alanlarının mahremiyetini ve güvenliğini kapsar.
- Yaşama Alanı ve Coğrafi Mahremiyet (Territorial Privacy): Konut, çalışma ofisleri gibi kişisel alanlara yapılan müdahalenin sınırlarının belirlenmesini kapsar.[8]

---

[7] Kaboğlu, İ, Özgürlükler Hukuku, Afa Yayınları, İstanbul 1999, s.189.
[8] David, B, Simon, D, Global Trends in Privacy Protection: an International Survey Privacy, Data

2.4 Elektronik Haberleşme

Elektronik haberleşme, özel hayatın olmazsa olmazlarındandır ve başımıza gelen bazı beklenmedik ve istenmeyen olayların özel hayatımıza sirayet etmesinin başlıca sebeplerindendir. Elektronik Haberleşme, Elektronik Haberleşme Kanunu M. 3/h de: "Elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınmasını" şeklinde tanımlanmıştır. Teknik bir ifade ile modülasyon ya da kipleme olarak tanımlanan bu olay, bir taşıyıcı sinyal ile bilgi sinyalini birleştirmekten ibaret olan ve iletişim teknolojisinde kullanılan bir yöntemdir. Yani sesin dalga üzerine bindirilmesi ve taşınması şeklinde ifade edilmektedir. Yöntem başlarda sadece anten yoluyla yapılan yayınlar için öngörülmüş olsa da, günümüzde kablolu, kablosuz her tür iletişimde kullanılmaktadır. Çok düşük frekanslı sinyallerin örneğin; ses çok uzak mesafelere gönderilmesi maliyetlidir, bu nedenle alçak frekanslı sinyalin, yüksek frekanslı taşıyıcı bir sinyal üzerine bindirilerek uzak mesafelere taşınması sağlanabilmektedir. Bu olaya "kipleme" denir.[9] Elektronik haberleşme kavramına bu alanda ilk düzenleme niteliğine sahip olan Telgraf ve Telefon Kanunu'nun temel esaslar ve tanımlar kısmı 1. maddesinde, 'telekomünikasyon' olarak yer verilmiştir. Ancak daha sonra tüm elektronik haberleşme sektöründe düzenlemeyi amaçlayan BTK Elektronik Haberleşme Yönetmeliğinde, "Telekomünikasyon" 6.2.2004 tarihli, Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması hakkındaki yönetmeliğin yürürlükten kaldırılmasıyla, "Elektronik Haberleşme" olarak değiştirilmiştir. Elektronik haberleşme, üretilmiş veya iletilmek üzere saklanmış dijital ortama aktarılabilen konvertible verilerin işaret, ses, görüntü vb. kanallar ile iletilmesi ve kabul edilmesi suretiyle bireyler, makineler arasında kurulup iletişimi sağlayan; kişiler, kurumlar, bilgisayarlar ve sistemler arasında iletişimin hızlı,[10]

---

[9] Wikipedia: Modulasyon

[10] Protection and Surveillance Laws and Developments, Jhon Marshall Jounal of Computer Information Law, 18, 1-111, 1999.

etkin, kesintisiz ve kaliteli bir şekilde sağlanması olarak özetlenebilmektedir. Haberleşmenin gerçekleşmesi için verinin nitelikli ve sistematik olması beklenmektedir. Televizyon(TV) ve radyo yayınları kitlesel haberleşme araçları kapsamında olup düzenleme kapsamına dahil edilmeyerek sektör RTÜK tarafından regüle edilmektedir.

Hukukun teknolojiye bakışını incelemeye devam ediyoruz bu bağlamda GSM sektöründe sıklıkla kullanılan teknik terimleri yapılmış regülasyonları ve sektörü anlamak adına bilmek gerekmektedir.

2.4.1 BTK Düzenleyici Kurul ve Yapısı

10 Kasım 2008 tarihinde yürürlüğe giren Elektronik Haberleşme Kanunu (EHK) veri gizliliğine ilişkin hükümleri kapsayan, BTK'nın görev ve yetkileri bu kanunda belirlenmiştir. Bu kapsamda "Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak ve sektörel ihtiyaçları teknolojide meydana gelen değişikliklerle düzenleme ve eklenen yönetmelik ile kişisel veri gizliliği koruması durumunda yetkili kılmıştır.

Türkiye'de mali özerkliği haiz bağımsız düzenleyici kurum bütçeleri genel ve özel bütçeden farklı olarak, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununun belirli maddeleri ile bağlıdırlar. 5018 sayılı Kanunun 17'nci maddesine göre bu bütçeler, üç yıllık bütçeleme anlayışı ile stratejik plan ve performans hedefleri ile kurumsal, işlevsel ve ekonomik sınıflandırma sistemine göre hazırlandıktan sonra doğrudan TBMM'ye sunulmaktadır. Bu sürece genel ve özel, mahalli idareler ve sosyal güvenlik kurumları bütçelerinden farklı olarak Bakanlar Kurulu dahil olmamaktadır. Bağımsız düzenleyici kurum bütçeleri, "Merkezi Yönetim Bütçe Kanunu"nda yer almakta olup, bunların uygulama sonuçları "Kesin Hesap Kanunu" ile yine TBMM tarafından onaylanmaktadır. Bununla birlikte, bu kurumlarda iç denetim birimleri bulunmamakta olup, dış denetimleri ise Sayıştay tarafından yerine getirilmekte ve her üç ayda bir belirlenen gelir fazlaları ise genel bütçeye aktarılmaktadır.

Kurumun gelirlerinin şu kalemlerden oluşması önerilmektedir: Kurum tarafından uygulanacak idari para cezaları, yayın gelirleri, kuruma ait taşınır ve taşınmaz mallardan elde edilen gelirler, müşavirlik hizmetlerinden elde edilecek gelirler, kurs, toplantı, seminer ve eğitim faaliyetlerinden sağlanacak gelirler, genel bütçeden gerektiğinde yapılacak yardımlar, her türlü bağış, yardım ve diğer gelirler ile bu gelirlerin nemalandırılması suretiyle elde edilecek gelirler. Kurum gelirleri 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununun üçüncü maddesinin birinci fıkrasının (c) bendinde belirtilen cetvel için öngörülen usul ve esaslara göre hazırlanmalı ve kabul edilmelidir.

2.4.2 Haberleşme Sektörü ve Genel Teknik Terimleri

a) Abone: Bir işletmeci ile elektronik haberleşme hizmetinin sunumuna yönelik olarak yapılan bir sözleşmeye taraf olan gerçek ya da tüzel kişiyi,

b) Acil yardım çağrıları: Ulusal ve uluslararası düzenlemelerde kabul görmüş yangın, sağlık, doğal afetler ve güvenlik gibi acil durumlarla ilgili olarak itfaiye, polis, jandarma, sağlık ve benzeri kuruluşlara yardım talebiyle yapılan çağrıları,

c) Anonim hale getirme: Kişisel verilerin, belirli veya kimliği belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek veya kaynağı belirlenemeyecek hale getirilmek suretiyle işlenmesini,

ç) Gerçekleşmeyen arama: Başarılı bir şekilde bağlantı kurulmasına rağmen, aranan tarafın cevap vermemesi ya da şebeke yönetiminden kaynaklanan bir nedenle görüşmenin gerçekleşmemesini,

d) Hücre kimliği: Mobil telefon çağrısının başladığı ya da sona erdiği hücrenin kimliğini,

e) IMEI: Uluslararası mobil cihaz kimliğini,

f) IMSI: Uluslararası mobil abone kimliğini,

g) İşlem kaydı: Kişisel verilere erişebilen kişiler tarafından yapılan işlemin ileriki

bir tarihte tanımlanabilmesi temin edilen söz konusu işleme ilişkin olarak tutulan ve en az işlemi yapan kişi, işlemin yapıldığı tarih ve zamanı, yapılan işlemin detayı, gerekçesi ve niteliği ile işlemi yapan kişinin bağlandığı nokta bilgilerini içeren elektronik kayıtları,

ğ) İşletmeci: Yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketi,

h) Kişisel veri: Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgileri,

ı) Kişisel veri ihlali: İstem dışı, yetki dışı ya da yasa dışı olarak; kişisel verilerin tahrip edilmesine, kaybolmasına, iletilmesine, değiştirilmesine, depolanmasına veya başka bir ortama kaydedilmesine, işlenmesine, ifşa edilmesine ve söz konusu verilere erişilmesine neden olan güvenlik ihlalini,

i) Kişisel verilerin işlenmesi: Kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi, tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen işlem ya da işlemler bütününü,

j) Konum verisi: Kamuya açık elektronik haberleşme hizmeti kullanıcısına ait bir cihazın coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde veya elektronik haberleşme hizmeti aracılığıyla işlenen belirli veriyi,

k) Kullanıcı: Aboneliği olup olmamasına bakılmaksızın elektronik haberleşme hizmetlerinden yararlanan gerçek veya tüzel kişiyi,

l) Kullanıcı kimliği: İnternet erişim hizmetlerine ya da internet haberleşme hizmetlerine abonelik ya da kayıt esnasında tahsis edilen tek ve kişiye özel tanımlamayı,

m) Kurul: Bilgi Teknolojileri ve İletişim Kurulunu,

n) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,

o) Maskeleme: İşletmecinin kişisel verileri, üçüncü tarafların bu verileri ilgili kişi ile ilişkilendiremeyecek hale getirmesini,

ö) Rıza: İlgili kişinin kendisine ait kişisel verisinin işlenmesine yönelik, verinin işlenme amaç ve kapsamı dâhilinde, verinin işlenmesi öncesinde özgür iradesiyle verdiği ispatlanabilir kabul beyanını,

p) Trafik verisi: Bir elektronik haberleşme şebekesinde haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi,

r) Veri: Abone ya da kullanıcıyı teşhis etmek için yararlanılan trafik verisi, konum verisi ya da ilgili diğer bilgileri, ifade eder. (BTK, E-Haberleşme Direktifi)

2.4.3 Abone Kavramı

Abone, Elektronik Haberleşme Kanununa göre, "bir işletmeci ile elektronik haberleşme hizmetinin sunumuna yönelik yapılan sözleşmeye taraf olan gerçek ve tüzel kişilerdir".[11] Taraflar arasında yapılan sözleşme gereği, abonelerin kişisel verileri işlenmektedir.

Aboneler, sözleşme hükümlerince korunan gerçek ve tüzel kişiler olarak ifade edilmektedir. Veri koruması alanında Avrupa Parlamentosu ve Konseyi tarafından kabul edilen 95/66/EC direktifinde gerçek kişilerin ve haberleşme özgürlüğünün korunması amaçlanmıştır. 95/66/EC direktifi 97/66/EC ile eksik tarafları desteklenmek üzere Telekomünikasyon Alanında Kişisel Verilerin Korunması ve tüzel kişilik kavramı da içeren Elektronik Veri Koruma Direktifinde (2002/58/EC) yayımlanmıştır. Ülkemizde yürürlüğe alınan Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönetmeliği'nin

[11] (EHK. M. 3/a).

hazırlanmasına da bu direktifler zemin oluşturmuştur.

2.4.4 İşletmeci Kavramı

İşletmeci, EHK m. 3/z'de, "Yetkilendirme çerçevesinde, elektronik haberleşme hizmetini sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirket" olarak tanımlanmıştır.

"Bir görev sözleşmesi, imtiyaz sözleşmesi ruhsatı ya da BTK genel izin kapsamında yapılan bir kayıtlanma uyarınca telekomünikasyon hizmetleri yürüten, işleten sermayeli şirkettir"[12].

2.4.5 Kullanıcı Kavramı

Kullanıcı: "Aboneliği olup olmamasına bakılmadan telekomünikasyon hizmetlerinden yararlanan gerçek veya tüzel kişiyi" ifade eder.[13]

2.4.6 Ara Bağlantı Kavramı

Ara bağlantı, "İki ayrı telekomünikasyon şebekesi arasındaki telekomünikasyon trafiğinin gerçekleştirilmesini teminin iki şebekenin birbirine irtibatlandırılması" olarak tanımlanmaktadır. "Bir telekomünikasyon hizmetini sunabilmek için lisans alabilen ve böylece bu türden hizmetleri yürütme hakkına sahip olan işletmeciler, kendi şebekeleriyle sabit veya mobil telefon hizmeti veren diğer işletmecilerin şebekeleri arasında bağlantı kurabilmek için bu işletmecilerle anlaşmak ve böylece kendi aboneleriyle diğer işletmecilerin abonelerinin haberleşebilmelerinin sağlanmasını."[14] ifade etmektedir.

---

[12] (TSKVKY. m. 3)
[13] Elektronik Haberleşme Kanunu 3/k
[14] European Commission, Notice on Application of Competition Rules to Acces Agreements in the Telecommunications Sektor-Framework, Relevant Markets and Principles O.J. C. 265/2 (1998),prg. 49. (naklen, Ünver, 101).
http://eur-lex.europa.eu/LexUriServ/site/en/oj/1998/c_26519980822en00020028.pdf

2.4.7 Roaming Kavramı

Roaming; GSMA lisansı bulunan operatörlerin "hücresel alıcılar için kendi şebekelerinin coğrafi kapsama alanı dışında seyahat ederken girilen ve ziyaret edilen şebekeler ve bu şebekeler bünyesinde sesli konuşma yapma, karşılıklı bilgi aktarımı ve başka hizmetlere ulaşım imkânı" olarak tanımlanmaktadır. Ulusal ve uluslar arası roaming yapılabilmesi için ülkemiz işletmecileri tarafından imzalanmış international roaming anlaşmaları bulunmakla birlikte ülkemiz işletmecileri arasında roaming uygulanmamaktadır.

3. AB DİREKTİFLERİ VE ÜLKEMİZ KAPSAMINDA KİŞİSEL VERİLERİN İŞLENMESİ, SAKLANMASI VE GİZLİLİĞİNİN KORUNMASI

AB direktiflerinde yer alan kişisel veri, trafik ve konum verisi gibi veri türlerinin açıklandığı bu bölümde, kişisel verilerin doğrudan pazarlama amaçlı kullanım alanları reklam tanıtım amaçlı istek dışı haberleşmeye değinilmek suretiyle, verilerin tanımları sonrası işlenmesine yönelik kısıtlar ve işlenme türleri, bu veriler için işlenebilme koşulları ve taraflarca işlenebilirliği, kişisel verilerin saklanması ve saklanması hususunda işletmecilerin sorumlulukları ve Veri Madenciliğinin etkileri aktarılarak, ülkemiz uygulamalarıyla devam edilecektir.

25 Mart 1957'de imzalanan ve 1 Ocak 1958'de yürürlüğe giren Avrupa Ekonomik Topluluğu olarak bilinen grup, ABİDA (Avrupa Birliği İşleyişine Dair Antlaşma), Maastricht ve Amsterdam Antlaşmalarıyla değişikliğe uğramış Lizbon Antlaşmasıyla son halini alarak Avrupa Birliği tanımını almıştır. (2009 Lizbon Antlaşması yürürlüğe girişi)

7 Şubat 1992'de imzalanarak 1 Kasım 1993'te yürürlüğe giren Maastricht yani Avrupa Birliği Antlaşması Avrupa Birliği üye ülkelerinin birliği dört düşünce etrafında şekillenmiştir. Bunlar: "Malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımıdır."[15] Akabinde Amsterdam (1997) ve Nice Antlaşmaları'yla (2001) AB'de değişiklikler yapılmıştır (EU, 2007).

Lizbon, Avrupa Birliği ticari faaliyetleri canlı tutabilmek için teknolojik ihtiyaçların karşılanmakta olduğu telekomünikasyon sektörü alanında yaşanan gelişmeler karşısında aktif bir rol alabilmek ve hukukî anlamda birliği sağlayabilmek amacıyla direktifler yayınlanmış ve kabul edilmiştir.

Söz konusu direktifler, telekomünikasyon alanında özelleştirmeler gerçekleştirmiş

[15] Maastricht (9, 30, 42, 48, 59, 736)

diğer ülkelerin tecrübelerinden yararlanarak oluşturulmuştur.[16]

Hizmetlerin yerine getirilebilmesi için kişisel verilerin toplanması ve işlenmesi bir zorunluluk taşımaktadır. Yeni teknoloji ve özel hayatlara müdahale etkileri göz önüne alınarak verilerin temel haklara uygunluğunu sağlanmasının önemi düşünülerek AB'nin kişisel verilerin korunmasında temel referans belgesi niteliği taşıyacak olan (95/46/AT) direktifleri yürürlüğe konulmuştur.

Bu ve benzeri birliktelik sağlayıcı faaliyetler için Avrupa Birliği karar, tüzük, direktif olarak çalışmalarını sürdürmüştür.

Tüzükler, uygulanması için ülkelerde bir hukuki ihtiyaç gerektirmeyip direk iç kanuna aktarılabilen bağlayıcı olan ve doğrudan uygulanan, birlik vatandaşları için ulusal kanunlar gibi hak ve yükümlülükler getiren hukuki tasarruflardır. Tüzük çıktığı andan itibaren uygulamaya konulur ve tüzüğün gerçekleşmesine yönelik tüm hükümlerin uygulanması zorunludur.

Direktifler, uygulanması için ülkelerde hukuki iç aktarım ihtiyaçları gerektiren, çerçeveleri çizilmiş ve bu çerçeve uyulması istenen fakat bulunduğu ülkenin hukuk sistemini de tezahür eden yöneylem planları şeklinde ifade edilebilmektedir.

3.1 95/46/EC Sayılı Veri Koruma Direktifi

Tavsiye kararların hukuki açıdan bağlayıcılığının olmadığının anlaşılmasıyla direktif haline getirilen 95/46/EC sayılı direktifin kökeni, üye ülkelerde kişisel verilerin korunmasına ilişkin düzenlemelerin uyumlaştırılmasına dayanmakta olup direktifin 1. maddesi, üye ülkelere "özel hayatın gizliliği" esasını koruma bilinci yüklemektedir. 24 Ekim 1995 yılında nihai halini almıştır[17]. Bu direktifte ayrıca teknolojik maliyetleri düşürücü ve ortak ticaret projeler geliştirmenin önünü açacak olan açık ağların kurulmasını da amaçlayan ONP (Open Network

[16] Özdemir,H 32
[17] Buellesbach, 2010

Provision) çerçeve direktif özelliği de bulunmaktadır. Hatların kiraya verilmesi ve sesli telefon hizmetlerini sağlamak üzere toplu bağlanma direktifleri kabul edilmiştir.[18]

Kural olarak kişisel verilerin ilgili kişinin açık rızası ve maddede sayılan istisnalar dışında işlenmesi yasaktır. 95/46 EC sayılı Avrupa Birliği Direktifinin 2. m/h bendinde rızanın tanımı yapılmıştır. Buna göre rıza beyanı, ilgili kişinin kendisiyle ilgili veri işlenmesi fiiline, özgürce ve konuyla ilgili yeterli bilgi sahibi olarak verdiği ve sadece o işlemle sınırlı onay beyanıdır. Buna göre ilgili kişi, kendisine ait verilerin işlenmesini kabul etmektedir. Yine direktifin; 7. maddesine göre rıza, ilgili kişi tarafından "tereddüde yer bırakmayacak şekilde" verilmiş olmalıdır. Maddenin 1. fıkrasındaki hükmün doğal sonucu olarak; kanunlarda öngörülen yükümlülüklerin yerine getirilmesi dışında, ilgili kişinin bir itirazda bulunması halinde veri işlenemeyecektir.

Avrupa Birliği komisyonu tarafından üye ülkelerin kişisel bilgilerin korunmasına ilişkin millî mevzuatlarının uyumlu hale getirilmesine yönelik verilerin korunması ile ilgili dünyada ilk yasal düzenleme 1970 yılında Federal Almanya'nın Hessen eyaletinde yapılmıştır. Bu düzenleme ile ilk veri koruma otoritesi olan Veri Güvenlik Ofisi (Datenschutzbeauftragter) kurulmuştur.[19]

Kişisel verilerin transferinin gerçekleşebilmesi için uygunluğun bir diğer şartı, transferin gerçekleşeceği o ülkede koruma kanunlarının bulunması ve yürütmesinin aktif bir şekilde yapılıyor olmasıdır.

Veri sahibinin verileri direktifler kapsamı dışında bir işleme tabi tutulduğunda, ülkesindeki hakları o ülkede de, sahip olabilmesi gelmektedir. Bu şartın uygulamada yerine getirilmesi oldukça güçtür. Mevzuatın uyumlu hale getirilmesiyle kişisel verilerin Avrupa Birliği ülkelerinde serbest dolaşımını izin verilmesiyle birlikte AB ve ABD arasında ticareti sürdürmek ve birliktelik

[18] ONP, Çerçeve direktifi
[19] Caprioli at al, 2006:214

sağlamak amacıyla "Safe-Harbor-Lösung" (Güvenli Liman Çözümü) adı verilen anlaşma AB veri korumasını içerecek şekilde imzalanarak kişi hak ve özgürlüklerinin korumasının devam edilmesi amaçlanmaktadır.[20]

Türkiye'den üçüncü ülkelere kişisel veri iletilirken, VKD ile uyumlu olarak, iletilen ülkede de kişisel verileri koruyucu düzenlemelerin varlığı şartının aranması kanuna devredilmelidir. Uluslararası antlaşmalardan kaynaklanan yükümlülükler ile kanuni zorunluluk halleri ve ayrıca kanunda sayılacak olan hukuka uygunluk sebepleri gibi istisnalar dışında bu şart kanunda öncelikle yer almalıdır.

Birliğe üye ülkeler arasında kişisel verilerin aynı derecede korunamıyor olmasının da etkisiyle direktifin 1. maddesine göre, "Birliğe üye ülkeler; bu direktifte belirtilen kişilerin hak ve özgürlüklerine ve kişisel verilerin işlenmesinde gerçek kişilerin özel hayatlarını garanti altına almalıdırlar" (VKD. m.1/1) hükmü uyarınca, "Birliğe üye ülkeler, m.1'de sayılan hak ve özgürlüklere ilişkin sebeplerden dolayı Avrupa Birliğine üye ülkeler arasında dahi kişisel verilerin serbest dolaşımını yasaklayabilirler veya sınırlayabilirler" (VKD. m.1/2).[21]

3.2 97/66/EC Sayılı Kişisel Verilerin İşlenmesi, Özel Hayatın Korunması Direktifi

Direktif, daha evvel yürürlüğe giren 95/46/EC direktifinden farklı olarak gerçek kişilerin yanı sıra, tüzel kişileri de ilgili kapsamına alarak etkisini sektörel bazda artırmıştır. Avrupa Parlamentosu tarafından kabul edilen elektronik haberleşme alanını da kapsayan 31 Temmuz 2002 tarihli "Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Direktifi" ile birlikte 97/66/AT yürürlükten kaldırılmıştır.

---

[20] Burgsdorff, 83
[21] Tinnefeld/Ehmann/Gerling, 123; Ellger, 61

3.3 2002/58/EC Sayılı Avrupa Birliği e-Gizlilik Direktifi

Abonelerin, kişisel verilerinin gizliliğinin korunması konusunda özel ihtiyaçlarının ortaya çıkmasına sebep olan yeni ileri teknolojiler, son dönemlerde kamu haberleşme şebekelerinde de kullanılmaya başlanmasıyla ilk yayınlandığında sadece yerleşik ses hizmetlerini kapsayacak şekilde oluşturulan direktif ile elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve özel hayatın gizliliğinin korunması eksik kalmıştır. Bu hizmetleri kablolu haberleşmeden kablosuz haberleşmeye, ses hizmetinden veri hizmetlerine geçişin uyumunu sağlamak amacıyla direktifinin yenilenmesi öngörülmüştür. Bu kapsamda, AK tarafından 1999'da hazırlanan Taslak, 12 Temmuz 2002'de kabul edilerek 2002/58/EC sayılı E-Gizlilik direktifi yürürlüğe girmiş, ISDN direktifi ise yürürlükten kaldırılmıştır.

Dolayısıyla direktif 97/66/EC, 95/46/EC sayılı direktiflerde yer alan ilkelerle, elektronik 97/66/EC sayılı direktifi de kapsayacak şekilde geniş bir geçerlik alanına sahiptir.[22] Bu sayede direktif kapsayıcılık bakımından elektronik haberleşme ve elektronik haberleşme sistemlerindeki kişisel verilerin ve özel hayatın gizliliğinin korunmasına ilişkin esaslara yer vermektedir.

Direktiflerin anlaşılabilirliğinin artırılması adına kurulan 29. Başlık Veri Koruma Grubu'nun paylaşmış olduğu prensipler önem arz etmekte olup direktiflerin bu şekilde yorumlanması beklenmektedir:

a) Adil ve yasalara uygun şekilde işlenmesi

b) Verilerin belirlenmiş yasal amaçlara göre toplanmış olması ve farklı amaçlar için herhangi bir işleme tabi tutulamaması

c) Veriler, toplama ve işleme amaçları için yeterli olması, aşırı olmaması

---

[22] (EK-VKD. m. 4, 5)
Article 29 Data Protection Working Party olan bu grup hakkında ayrıntılı bilgi için bkz. http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

d) Verilerin doğru ve güncel olarak tutulması, veri kalitesi sağlanması yanlış veya eksik olan verinin silinmesi veya düzeltilmesi için gerekli adımlar atılması

e) Verilerin gerektirdiğinden daha uzun süre saklanmaması

Düzenlemenin Adı	Düzenlemenin İçeriği
Kişisel Verilerin İşlenmesi ve Bu Verilerin Serbest Dolaşımı Hakkında Bireylerin Korunması Hakkında Avrupa Parlamentosu ve Konseyin 95/46/AT Sayılı Direktifi (Veri Koruma Direktifi)	Kişisel verilerin korunması ile ilgili temel çerçeve düzenlemedir.
2001/497/AT sayılı Komisyon Kararı	15 Haziran 2001tarihli bu Karar, 95/46 sayılı Veri Koruma Direktifi altında üçüncü ülkelere kişisel veri transferi ile ilgili sözleşme hükümleri hakkındadır.
45/2001 Sayılı Kişisel Verilerin Topluluk Kurum ve Kuruluşları Tarafından İşlenmesi Bağlamında Bireylerin Korunması ve Bu Verilerin Serbest Dolaşımı Hakkında Tüzük	Birliğin kurum ve organlarının kişisel verileri korumak konusunda uyacakları esasları belirlemektedir. Birlik kurum ve kuruluşlarının tüm veri işleme operasyonlarının ve bu Tüzükle kurulan bağımsız "Avrupa Veri Koruma Denetçisi" vasıtasıyla izleneceği hüküm altına alınmıştır.
2004/915/AT sayılı ve 2001/497/AT sayılı kararları değiştiren Komisyon Kararı	Kişisel verilerin üçüncü ülkelere transferine ilişkin sözleşmelerde alternatif standart ifadelere ilişkin karardır.
97/66/AT Sayılı Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Hakkında Avrupa Parlamentosu ve Konsey Direktifi	Elektronik Haberleşme alanında kişisel veri korumasını düzenlemektedir.
Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Avrupa Parlamentosu ve Konseyin 2002/58/AT sayılı Direktifi (Elektronik Haberleşme ve Gizlilik Direktifi)	
2006/24/AT Sayılı Kamu Elektronik Haberleşme Hizmetlerinin Sağlanması veya Kamu Haberleşme Ağları Çerçevesinde Üretilen veya İşlenen Verilerin Saklanmasına İlişkin 2002/58 Sayılı Direktifi Değiştiren Direktif	2002/58/AT sayılı Direktifte bazı değişiklikler yapmakta ve veri saklanmasına ilişkin hükümler ihdas etmektedir.
92/242/AET sayılı Konsey Kararı	Bilgi güvenliği ile ilgilidir.
2005/222/JHA sayılı Konseyin Çerçeve Kararı	Bilgi Sistemlerine yönelik saldırılar hakkında çerçeve hükümler içermektedir.
Avrupa Parlamentosu ve Konseyin 460/2004 sayılı Tüzüğü	Avrupa Ağ ve Bilgi Güvenliği Ajansını kuran Tüzüktür.

Tablo-1[23]

[23]European Commission, "Justice and Home Affairs, Data Protection"

4. VERİ TÜRLERİ, VERİ TÜRLERİ ARASINDAKİ İLİŞKİ VE İSTEK DIŞI HABERLEŞME

AB direktifleri temel alınarak ülkemizde düzenlenmiş olan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması yönetmeliği 24 Temmuz 2012 tarihinde resmi gazetede yayınlanmış ancak operatörlerin ortak uzatma talepleriyle birlikte Temmuz 2013 tarihine ötelenmiştir.

Yönetmelik 1.Maddesinde; bu yönetmeliğin amacı, elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması için elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenlemek olarak belirtilmiştir.

İşlenmesi, saklanması ve gizliliği olmak üzere 3 ana kapsamda değerlendirilen veriler, 5.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 4, 6, 12 ve 51. maddelerine dayanılarak hazırlanmıştır.

Haberleşmenin içeriğine ilişkin verilerin saklanmasının bu yönetmeliğin kapsamına dâhil edilmediği ancak kişilerin özel hayat gizliliği ihtiva eden lokasyon verilerinin de kişisel veri kapsamında değerlendirilmesi belirtilmektedir.

4.1 Kişisel Veriler

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması yönetmeliğinde, belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler kişisel veri olarak kabul edilmiştir.

4.1.1 Kimlik Bilgileri

İsim, soy isim, TC vatandaşlık numarası, doğum yeri-tarihi, anne-baba adı, anne kızlık soyadı, nüfusa kayıt yeri ve dini gibi kişinin tanınabilirliğini ortaya koyan her türlü kanun tarafından kimlik özelliği taşıyan kartlar ve bu kartlar üzerindeki fotoğraf, resim kimlik bilgisi olarak değerlendirilmektedir.

4.1.2 Adres Bilgileri

Kendisi veya ailesinin ikamet ettiği, işyerine ya da yazlık adresi gibi geçici yerlere ait adresler, adres bilgileri olarak değerlendirilmektedir.

4.1.3 Kredi/Debit Kart Bilgileri

Maddi değer barındıran her türlü kart ve bu kartlarla ilişkilendirilen karta ilişkin numara, şifre, güvenlik kodu gibi kimlik hırsızlığına ve dolandırıcılığa açık veriler kişisel veri kapsamında tutulmaktadır. Ancak hukuka uygun olarak yasal takip ve inceleme olarak kullanılabilecek bu bilgilerin ticari katma değer üretecek şekilde, hukuk dışı kişilerin alışveriş profillerinin çıkartılması ve bu bilgilerin ticari faaliyetler için kullanılması da kişisel verilerin suiistimalidir.[24]

4.1.4 MSISDN Bilgileri

Msisdn bilgilerinin kişisel veri olması, yönetmeliğin ve veri korumanın en tartışılan kısmıdır. Değerlendirme kapsamında MSISDN verisi üzerinden kişiler hakkında lokasyon bilgilerine ulaşabiliyorsak ve bu verilerin bir takım veri işleme metotlarıyla anlamlandırılmasıyla bir ticari değer ortaya çıktığı için MSISDN bilgisi bu destekleyiciliği sebebiyle kişisel veri olarak kabul edilmektedir. Ayrıca MSISDN bilgilerinin pazarlama amaçlı olarak toplu paketler halinde satışıyla birlikte istenmeyen bir reklam/pazarlama sektörü oluşturulmaktadır.

4.1.5 E-posta Bilgileri

Anlamlandırılan verilerle birlikte tüketici davranışlarını elde etmek suretiyle spam ismini vermiş istenmeyen e-posta trafiği oluşturularak verilerin direktif ve yönetmelik çerçeveleri dışı işlenmesi özel hayat gizliliği ilkesiyle uyuşmamaktadır.

---

[24] Dinc, E 2006:9

4.1.6 IP Bilgileri

Dolaylı yol sadece kişilerin otomobil plakalarını bulup ikametgâh adreslerine ulaşmak gibi daha fiziksel yönelimli bir süreç takip edebileceği gibi internet erişim sağlayıcıları tarafından loglarda tutulan IP adresi, tarih ve erişim bilgileri gibi internet kullanıcılarının belirlenebildiği Internet protokol bilgileri kişisel veri olarak değerlendirilmektedir.

IP numaraları dört hanelik 8 sayıdan oluşmaktadır. İnternet işletmecisi tarafından ISDN kartları vasıtasıyla söz konusu numaralar aktarılarak istenen bağlantı sağlanmaktadır.[25]

IP adreslerinin Avusturya, Belçika, İspanya, Almanya ve İsveç tarafından kişisel veri olarak kabul edilirken bazı AB üyesi ülkeler ise kabul ettikleri halde farklı yönde emsal teşkil edecek kararlar ile IP adreslerini kişisel veri kapsamında tutmamıştır. (Fransa'da bu örneğe rastlanmıştır.)

4.1.7 Kamu Kurumlarındaki Bilgiler

Birçok kamu kurumu ve kanuni makamlarca yetkilendirilmiş banka, hastane, tapu kadastro ve noter gibi merkezler e-devlet, MERNIS, POLNET, UYAP ya da MOBESE, Adrese Dayalı Nüfus Kayıt Sistemi gibi sistemler üzerinden hizmet vermektedirler. Bu sistemler kapsamında tutulan veriler kişisel veri kapsamında bulunmaktadır ve gizliliğine, korunmasına önem verilmesi gerekmektedir.

Özetlemek gerekirse kişisel veri kavramı kişilerin hayatlarına ışık tutacak formatı fark etmeksizin her türde başkaları tarafından o kişinin direk veya dolaylı yoldan tanınmasını veya tanınmasına imkân sağlayacak bilinmemesi gereken her türlü bilgi olarak değerlendirilebilir.

---

[25] Özdemir, H 115

Türkiye, veri koruması alanında Avrupa'nın oldukça geride olarak lanse edilerek bu durum Avrupa Birliği'nin 2002 ve 2003 tarihli ilerleme raporlarında da belirtilmiştir. Ancak yayınlanmış olan BTK yönetmeliği ile direktifleri kapsayıcı bir noktaya ulaşılmıştır.

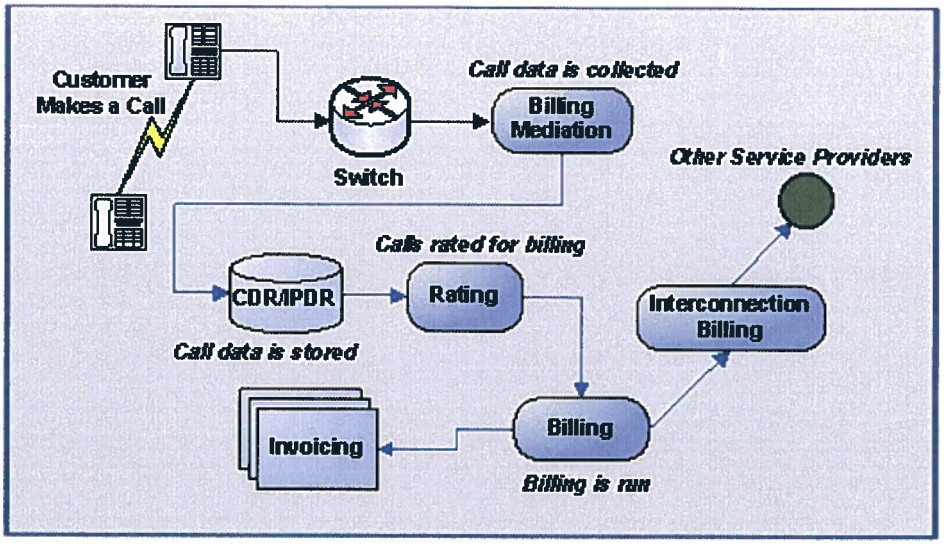
4.2 Trafik Verileri ve İşlenmesi

BTK tarafından yayınlanan yönetmelik, M. 2/b de trafik verisi, "Bir elektronik haberleşme şebekesinde haberleşmenin iletimi veya bu haberleşmenin faturalandırılması amacıyla işlenen veri" olarak tanımlanmaktadır.

Geçmişte sadece trafik yani iletişim amaçlı olarak tanımlanan bu verinin ücretlendirme, haberleşmenin zamanı, haberleşmenin türü, haberleşmenin akışı ve bu akış için tercih edilen protokol, haberleşmenin gerçekleştiği operatör baz istasyonu gibi haberleşmenin iletildiği format hakkında bilgiler içerebilmektedir (E-Gizlilik Direktifi, dibace 15).

Format farklı benzer varyasyonları olsa da genel itibariyle CDR (Call Data Record) tipinde bulunur ve raporlama, faturalandırma gibi farklı sistemler için bir türden farklı bir türe Mediation Grubu tarafından formatlanabilir ve hücre kimliği (Cell ID) bilgisi yer alır.

Basit bir arama için arama talebinin başlamasıyla Network üzerinden gelen bilgi ile bu arama kaydını içeren CDR kayıtları üremeye başladıktan sonra, Mediation CDR'ları faturanızın oluşması için Billing sisteme, raporlarınızın oluşması için DWH sisteme, Interconnection, Wholesale gibi mahsuplaşma ve ücretlendirme bilgisinin crosscheck yapılacağı sistemlere ileterek mobil haberleşmenin faturalandırmasının oluşması sağlanmış olur.



Resim – 1

Arama yaptığımızda gerçekleşen CDR akışı:

Abone ve kullanıcılara ilişkin trafik verileri bir haberleşmenin iletimi için gerekli olmadıkları takdirde silinmeli ya da anonim hale getirilmelidir.

Trafik verisi, ilgili mevzuat hükümlerine uygun olarak, trafiğin yönetimi, ara bağlantı, faturalama, yolsuzluk tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile ara bağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır. (M. 8/1)

Trafik verileri madde metninde belirtilen amaçlar çerçevesinde işletmeciler tarafından işleme tabi tutulmalıdır.

İşletmeciler müşteri rızası olmaksızın bir işleme gerçekleştiremeyecek olup müşterinin bu rızası istenildiğinde iptal edilebilmektedir.

Kişisel trafik verileri haberleşmenin temini için kullanılmakta olup ihtiyaç halinin ortadan kalktığı durumlarda, silinmeli veya maskelemek suretiyle anlamsız hale getirilmelidir.

Kişisel trafik verilerin bu haller dışında işlenmesi, hukuka aykırılık teşkil etmektedir.

Trafik verisi, ara bağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü, tüketici şikâyetlerinin değerlendirilmesi ve denetim faaliyetlerinin gerçekleştirilmesi amacıyla yazılı olarak talep edilmesi halinde kanunların yetkili kıldığı mercilere verilir. (Elektronik Haberleşme yönetmeliği M.10/1)

4.2.1 Aboneler İçin Hazırlanan Rehberler

MADDE 19 – (1) Aboneler, basılı ve/veya elektronik abone rehberlerinin, yayımlanma amaçları ve bu rehberlerde yer alacak kişisel veriler ile bu rehberlerin elektronik sürümlerinde olabilecek sorgulama seçenekleri ve kullanım imkânları hakkında rehbere kaydedilmeden önce ücretsiz olarak bilgilendirilirler.

(2) Kamuya açık rehberlerde yer alan kişisel veriler, rehberlik hizmetinin amaç ve kapsamına uygun olarak belirlenir.

(3) Abone rehberlerinde yer almayı kabul eden aboneler, rehberlerde yer alan kişisel verilerinin düzeltilmesini, teyit edilmesini ve/veya çıkarılmasını ücretsiz ve basit bir yöntemle talep edebilirler.

(4) Rehberlik hizmeti kapsamında yapılacak sorgulamalarda, Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği'nin Elektronik Haberleşme Hizmet, Şebeke ve Altyapılarının Tanım, Kapsam ve Süreleri ile ilgili 27. maddesi kapsamında yapılan düzenlemeler esastır.

Ülkemizde yayımlanan ilk telefon rehberi (kılavuz) 1916 yılına aittir. E-Haberleşme Yönetmeliği 19. madde ile gündeme alınan konu Elektronik Veri Koruma direktifinin 12. maddesinde abone rehberleri konusuna, telekomünikasyon alanında kabul edilen önceki direktife (97/66/EC) nazaran daha ayrıntılı yer verilmiştir, ancak günümüz teknolojisi ve ihtiyaçlarını göz önünde bulundurularak günümüzde bu rehbere eskisi kadar rağbet edilmemektedir.

4.2.2 Ayrıntılı Fatura

MADDE 20 – (1) İşletmeciler, ayrıntılı fatura gönderdikleri abonelerin talep etmeleri halinde, fatura ayrıntısında yer alan telefon numaralarının bazı rakamlarının gizlenmesini sağlar.

Arayan numaraların tam olarak gösterilmesi ile ilgili olarak ortaya çıkan diğer bir sorun da, firmaların müşteri hizmetleri için kullandıkları 444'lü hatlardır. Bu hatlardan arayan kişilerin tespit ve kontrol edilebilmesi alanında sorunlar ortaya çıkmaktadır. Bu tür sorunların çözümü için aranan numaraların son üç rakamları silinerek faturalarda yer almaktadır. İşletmeci burada, aranan numaraların tam olarak silinmesi veya kaydedilmesi yönündeki seçim hakkını aboneye tanımamaktadır. Çünkü bu tür numaraları kullanan işletmeler, kendi pazar araştırmalarını ve kendi reklâmlarını yaparak kar oranlarını artırmak istemektedirler. Diğer taraftan, aboneler de, bu tür numaraların son üç rakamlarının silinmesinde, Anayasa'da yer alan haberleşme özgürlüklerinin teminini sağlamaktadırlar.[26]

Kişisel verilerin işlenmesinde hâkim olan ilkelerin, kişisel veri niteliği taşıması durumunda trafik verilerinin işlenmesinde de geçerli olacağı şüphesizdir.

4.3 Ara bağlantı Ödemeleri ve Abonelerin Faturalandırılması

Trafik verilerinin işlenmesi, yasal olarak faturaya itirazların yapılabileceği 08.09.2009 tarih ve 27343 sayılı Resmi Gazete'nde yayımlanan Erişim ve Ara bağlantı Yönetmeliğinde ara bağlantı; "bir işletmecinin kullanıcılarının aynı veya farklı bir işletmecinin kullanıcılarıyla irtibatının veya başka bir işletmeci tarafından sunulan hizmetlere erişiminin sağlanmasını teminin, aynı veya farklı bir işletmeci tarafından kullanılan elektronik haberleşme şebekelerinin birbirlerine fiziksel ve mantıksal olarak bağlantısı" olarak tanımlanmaktadır.

---

[26] Königshofen, 83; Elbel, 170.

4.3.1 Elektronik Haberleşme Hizmetlerinin Pazarlanması, Katma Değerli Hizmetler

Verinin ilgili olduğu abone veya kullanıcının rıza vermesi durumunda trafik verileri, elektronik haberleşme hizmetlerinin pazarlanması veya katma değerli hizmetlerin sunulması için gerekli olan kapsam ve sürede işlenebilir. Abone veya kullanıcılara söz konusu verilerin işlenmesi için verdikleri rızayı geri alma imkânı her zaman sağlanmalıdır.[27] İşletmeciler, abone veya kullanıcıları belirtilen amaçlar için işlenecek trafik verilerinin türü ve işlenme süreleri hakkında bilgilendirmelidir. Elektronik haberleşme hizmetlerinin pazarlanması veya katma değerli hizmetlerin sunulması amacıyla yapılacak bu bilgilendirme, abone veya kullanıcıların rızaları alınmadan önce yapılmalıdır.[28]

Haberleşme hizmetlerinin pazarlanması veya katma değerli hizmetlerin sunulması amacıyla işlenen trafik verileri bu hizmetlerin temininden sonra silinmeli veya anonim hale getirilmelidir.[29] Trafik verileri özellikle ara bağlantı ve faturalandırma konularındaki uzlaşmazlıkların çözümünde ilgili mevzuata uygun olarak yetkili makamlara bildirilebilir.[30]

4.4 Konum Verileri ve Konum Verilerinin İşlenmesi

Konum verisi; kamuya açık elektronik haberleşme hizmeti kullanıcısına ait bir cihazın coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde veya elektronik haberleşme hizmeti aracılığıyla işlenen belirli veri olarak tanımlanmıştır, Vatandaş Hakları Direktifi'nde ise tanım, "elektronik haberleşme hizmeti aracılığıyla" işlenen verileri de kapsayacak şekilde genişletilmiştir.[31]

MADDE 11 – (1) İşletmeciler, abonelerin/kullanıcıların konum verisini ancak, katma değerli elektronik haberleşme hizmetlerinin sunumu halinde

---

[27] E-Gizlilik Direktifi, M. 6/3
[28] E-Gizlilik Direktifi, M. 6/4
[29] E-Gizlilik Direktifi, dibace 26
[30] E-Gizlilik Direktifi, M. 6/6
[31] Şahin O,50

abonelerin/kullanıcıların rızasını alarak bu hizmetlerin sunumu için gerekli olan ölçü ve sürede ya da anonim hale getirmek suretiyle işleyebilir.

(2) İşletmeciler; aboneleri/kullanıcıları, rızalarını almadan önce, işlenecek konum verisinin türü, işlenme amacı ve süresi hakkında bilgilendirir.

4.4.1 Konum Verilerinin İşlenmesi

Son yıllarda özellikle GIS (Coğrafi konum belirleme) sistemleriyle mobil cihazların gelişmesi paralellik göstererek konum verilerinin önemini artırmıştır. Ne nerede gibi uygulamalarla daha önceden işaretlenmiş nokta POI'ler (Point of Interest) yardımıyla yakınında hangi hastane ve kafenin olduğunu öğrenme imkânı sunulmaktadır. Kişinin konum bilgilerinin GPS destekli ve LBS destekli navigasyon uygulamaları ile belirlemek mümkündür.[32]

Bu verilerin işlenmesi müşteri rızasına bağlı olup, işlenecek konum verisinin türü, veri işlenmesinin amacı ve süresi, verilerin katma değerli hizmet sunulması amacıyla üçüncü taraflara aktarılıp aktaramayacağı, abone veya kullanıcıların konum verilerinin işlenmesi için verdikleri rızayı her zaman geri alabilmelerine de imkân sağlanmalıdır.

Konum verisini işleme yetkisi sadece, işletmecinin veya katma değerli elektronik haberleşme hizmetleri sağlayan üçüncü tarafın yetkisi altında bulunan kişilerle sınırlı olup, bu yetki söz konusu hizmetlerin sağlanmasının gerektirdiği kapsamda kullanılmalıdır.[33]

4.4.2 Kişisel Verilerin İstek Dışı Haberleşme Amacıyla Kullanılması

Verilerin kolay ulaşılabilirliği ve sanal ortam vasıtasıyla hızlıca işlenip iletilebilmesi ile iletişimin farklı türleri ortaya çıkmıştır. Bu veriler listeler halinde bazı reklam firmaları tarafından pazarlama konusu haline getirilmiş ve kişilerin bu

---

[32]LBS:Location Based Service konum bilgisinin baz istasyonları cell bilgileri yardımıyla hesaplanması,Wikipedia

[33]E-Gizlilik Direktifi, M. 9/3

rahatsızlıklarından doğan memnuniyetsizliklerinde önlenmesi amacıyla yapılan istek dışı telefon çağrısı almamaları için optout sisteminin uygulanması konusunda işletmecilere yükümlülükler getirilmiştir.

4.4.2.1 Optin - Optout

Doğrudan pazarlama yani istek dışı haberleşmeyle ilgili mücadele yöntemlerindendir.

Kullanıcılara whitelist/blacklisk mantığıyla almak veya engellemek istedikleri iletişim şekillerini belirttikleri kişi bazlı akıllı filtrelere optin ve optout adı verilir. Bu sistemlerin veri tabanlarında header (mesaj başlığı) bazlı olarak gönderimlerin engellenmesi mümkündür. Abonelerin tercih etmediği durumlarda tüm haberleşme ortamlarınca haberdar edilebilirsiniz.

Ülkemizde merkezi bir veri tabanı olmamakla beraber operatör bazlı olarak filtreleme yapılabilmektedir. AB'de ise Gizlilik Direktifi kapsamında merkezi veri tabanı kurularak tüm gönderimlerin engellenmesi abone tercihine bırakılmıştır.[34]

Bilgisayarlar tarafından otomatik olarak birden fazla noktaya arama yapabilen otomatik cihazlarda yine bu kapsamda müşteri tarafından engellenebilmektedir.

4.5 Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi Veri Koruma Direktifinde, "Kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi veya tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen bir işlem ya da işlemler bütünü" şeklinde tanımlanmaktadır. E-Haberleşme Yönetmeliğinde detaylıca incelenecektir.

---

[34] Şahin,O, 62

4.5.1 Bir Kişisel Veri Olarak DNA Analizi Verileri

Kişinin dokunulmazlığı, maddi ve manevi varlığının düzenlendiği Anayasa'nın 17. maddesinde, tıbbi zorunluluklar ve kanunda yazılı haller dışında kişinin vücut bütünlüğüne okunulamayacağı, rızası olmaksızın bilimsel ve tıbbi deneylere tabi tutulamayacağı hüküm altına alınmıştır. Tüm temel hak ve özgürlüklerde olduğu gibi, Anayasa'nın 17. Maddesi kapsamındaki vücut dokunulmazlığı hakkı da Anayasa'nın 13. Maddesindeki güvencelere sahiptir. DNA analizi esasen bağımsız bir tedbir değildir, bir yönden vücudun muayenesi koruma tedbirinin bir parçası, diğer yönüyle keşif veya olay yeri incelemesinin bir uzantısıdır.[35]

Olay yeri incelemesi ve adli tıp kavramlarıyla günümüzde sıklıkla karşılaşır olduk. Buralardan elde edilen verilerinde kişisel veri olduğu aşikârdır.

Günümüz teknolojiler arası yakınsama (convergency) mantığıyla birlikte katma değerli servisler altında sağlık sektörüne yardımcı servisler bulunmaktadır. Tansiyon, nabız bilgilerini şeker hastaları için kan şeker durumunu ölçümleyip hekiminizle acil durumlarda iletişim kurabilen ve zaman periyodlarında sizin bu verilerinizi analiz etmek üzere istenildiğinde çıktı veren bu uygulamalarda Veri koruması direktifinde yer alarak hassas veriler arasında tutulmaktadır.

4.5.1.1 DNA Verileri ve DNA Veri Bankası Kanunu Tasarısı

AİHM'ye göre, kişisel ve tıbbi bilgilerin korunması Sözleşme'nin 8. maddesindeki özel ve aile hayatının korunması kavramı içinde yer almaktadır. Bu açıdan bakıldığında genel olarak tıp mesleği ve sağlık hizmetlerini de ilgilendiren sağlık bilgilerinin güvenliğinin sağlanması devletler açısından hayati önemde görülmektedir. Şüpheli veya sanığın parmak izinin, fotoğraflarının ya da kanının alınması gibi tıbbi testler ya da bireyin cinsel hayatına ilişkin bilgiler özel hayata müdahale kapsamında değerlendirilmektedir. DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı kimlik saptanması veya adli amaçlarla DNA

---

[35] Okur, N, 270

örneklerinin alınması, analiz edilmesi verilerin saklanması ve verilerden yararlanılması amaçları ile bir kamu kurumu kurulması için hazırlanmış elli üç maddeden oluşan bir tasarıdır.[36]

DNA verilerinin kullanılmasının gerekliliği ve kişisel veri niteliği ile özel hayatın korunması arasındaki ilişki tasarı ve gerekçesi:

DNA verilerinin kullanılması, sadece suç şüphesi altında bulunanların tespit edilmesini değil, aynı zamanda suç şüphesi altında bulunan masum kişilerin de bu zandan kurtulmasını sağlamaktadır. Ceza yargılaması dışında da DNA verileri kullanılabilmektedir. Örneğin; deprem, tsunami, maden göçmesi gibi doğal afetlerde çoğu zaman ölenlerin cesedi bozulduğundan bu kişilerin kimliklerinin tespitinde en güvenilir yöntemlerden biri olarak DNA verileri kullanılmaktadır. Yine, pek çok ülkede yaş, akıl sağlığı, hastalığı veya ölümü nedeniyle kimliği belirlenemeyen kişilerin kimlikleri de aynı yöntemlerle belirlenebilmektedir. Türkiye'nin de bir deprem ülkesi olması gerçeği konuyu ülkemiz açısından da önemli kılmaktadır. Ülkemizde gelişmekte olan turizm aktivitesi nedeniyle, birçok ülke vatandaşlarının belirli merkezlerde birlikte bulunabilmeleri söz konusudur. Dolayısıyla, böyle bir ortamda meydana gelebilecek doğal afetlerde kimliklendirme açısından da oldukça önem taşımaktadır. Kayıp kişilerin aileleri, bunların hayatta olup olmadıklarını bilmediği durumlarda büyük sıkıntılar yaşamaktadırlar. DNA teknolojisi sayesinde bu kişilerin kimliklerinin daha önce verdikleri örneklerden veya kendilerine ait eşyalardan ya da anne babalarından elde edilen örneklerin eşleştirilmesi suretiyle tespit edilmesi mümkündür.

Bilindiği üzere, DNA verileri, ait olduğu kişiyle ilgili kalıtsal pek çok bilgiyi de içermektedir. Bu bakımdan Anayasanın 20. maddesi ile ülkemizin de taraf olduğu, Avrupa İnsan Hakları Sözleşmesinin 8. maddesinde koruma altına alınan "Özel hayatın gizliliği" ile ilgili bir husustur. Hür ve demokratik bir toplumda kişi dokunulmazlığı, hem devletin hem de kişi ve organizasyonların kişinin özel

---

[36] Okur, N, 272

hayatına girmesinin önünde bir engeldir.

Günümüz teknolojisiyle tamamen olmasa da bilim ve teknikteki gelişmelere bağlı olarak, DNA verilerinden örneğin; kişinin saç rengi, göz rengi, yapısı, hastalıkları, etnik kökeni, diğer kalıtsal özellikleri, kardeşi, çocukları veya anne babasının tespit edilmesinin mümkün olabildiği düşünüldüğünde, verilerin elde edilmesi, saklanması ve kullanılmasının sıkı yasal koşullara bağlanması zorunluluğunu ve ihtiyacını ortaya çıkarmaktadır.

DNA verilerinin kullanım amacı ve kişisel verilerin korunması, uluslararası sözleşmelerde ve Avrupa Birliği müktesebatında da yer almıştır. Bu konuda ülkemiz tarafından da imzalanan "Kişisel Verilerin İşleme Tâbi Tutulması Karşısında Bireylerin Korunması"na ilişkin 108 sayılı Avrupa Konseyi Sözleşmesi, 95/46 EC sayılı Avrupa Birliği Direktifi, Avrupa Konseyi Bakanlar Komitesinin Ceza Adaleti Sistemi Uygulamasında DNA Analizlerinin Kullanılmasına ilişkin 1992 tarihli R(92)1 tavsiye kararı, "DNA Analiz Sonuçlarının Değişimine Dair" 9 Haziran 1997 tarihli ve 25 Haziran 2001 tarihli Avrupa Birliği Konseyi Kararları sayılabilir. Türkiye, Avrupa Konseyinin "Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesini 3.12.2003 tarihli ve 5013 sayılı uygun bulma kanunuyla kabul etmiştir. Avrupa Birliği Konseyinin 25 Haziran 2001 tarihli kararında, üye ülkelere, DNA verilerini karşılaştırmak amacıyla birbiriyle uyumlu veri tabanı kurmaları tavsiye edilmiştir"

"DNA Verileri ve Türkiye Milli DNA Veri bankası Kanunu Tasarısı"nın 1. maddesine göre, Yasa'nın amacı; kimlik tespiti veya adlî amaçla DNA örneklerinin alınması, analiz yapılması, verilerin saklanması, verilerden yararlanılması ile Türkiye Millî DNA Veri Bankasının kuruluş ve görevlerine ilişkin esas ve usulleri düzenlemektir. Bu yasa hükümleri, tıbbî etik kuralları çerçevesinde bir hastalığın teşhis ve tedavisi ile bilimsel araştırma ve deney amacıyla yapılan DNA analizleri hakkında uygulanmaz. Tasarı'nın 7. maddesinde DNA analizi yapmaya yetkili kurumlar belirtilmiştir; 9. maddesinde banka

bünyesinde kayıtlı olan DNA profillerinden ancak, bir soruşturma, kovuşturma veya özel hukuk uyuşmazlığında gerçeğin ortaya çıkarılabilmesi veya kimlik tespiti amacıyla yararlanılabileceği hüküm altına alınmış; 14. maddesinde suç soruşturması ve kovuşturmasına ilişkin hükümler saklı kalmak kaydıyla bu Kanun hükümlerine göre, banka bünyesinde oluşturulan sistem, DNA veri tabanında tutulan profillerin karşılaştırılması, yurtdışına aktarılması veya eşleştirilmesi ile DNA verilerinin elde edilmesine ilişkin yapılan her türlü işlemler ile bunların sonuçlarının gizliliği kuralı benimsenmiştir DNA analizi yapanların Türk Ceza Kanununun 135. maddesinin birinci fıkrası hükmüne göre; hukuka aykırı olarak DNA verilerini; açıklayan, yayan, bir TCK'nın 135. maddesinin birinci fıkrasında; "Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir" denilmektedir.

Tasarının beden bütünlüğünün dolayısıyla özel hayatın korunmasında devletin pozitif yükümlülüğü çerçevesinde ileri bir adım olduğu anlaşılmaktadır.[37]

4.5.2 Mobese

Mobil Elektronik Sistem Entegrasyonu (Mobese), Emniyet Genel Müdürlüğü araçları için tasarlanmış iletişim altyapısı olarak GPRS teknolojisini kullanan, yazılım ve mobil donanım birimlerinden oluşan, Coğrafi Bilgi Sistemleri ve Bilgi Yönetim Sistemlerinin (GIS / MIS) entegrasyonudur.[38]

Mobil iletişim teknolojisinin kamu hayatına olan desteği olarak kolluk kuvvetleri ve belediyeler, valilikler gibi yerel hizmet kullanıcılarına asayiş ve hizmet sağlanması anlamında fayda sağlamaktadır. Operatörlerde kişisel verilerin işletme tarafından yetkilendirilmiş kişi ve kişiler tarafından kontrol edildiği düşünüldüğünde mobese verilerinin özel hayat gizliliğine özgürlüklere engel teşkil edici bir şekilde kullanılmaması gerekmektedir.

TCK'nın 136. maddesinde "(1) Kişisel verileri, hukuka aykırı olarak bir başkasına

---

[37] Okur, N, 272
[38] http://www.datateknik.com.tr/tr/content.asp?ctID=471

veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır." hükmüyle bu verilen amaç ve önemleri belirtilmektedir. Mobese görüntüleri kayıt altına alınarak suçlulara karşı delil olmaktadır. Ceza muhakemesinde denetim sonucunda elde edilen delillerin kötüye kullanılmasının önlenmesi açısından ihtiyaç duyulmayan delillerin imha edilmesi gerekmektedir.[39]

4.6 Verilerin Saklanması

Veri Saklama Direktifi ciddi suçların tespiti, soruşturulması ve kovuşturulmasında kullanılmak üzere gerçek ve tüzel kişilere ilişkin trafik ve konum verilerinin belirli bir süre saklanmasına yönelik olarak üye ülkelere yükümlülük getirmektedir.

Veri saklama yükümlülüğü E-Gizlilik Direktifinde olduğu gibi kamu haberleşme şebekesi veya kamuya açık elektronik haberleşme hizmet sağlayıcılarını kapsamasına rağmen Finlandiya ve İngiltere gibi ülkelerde, küçük işletmecilere veri saklama yükümlülüğü getirilmemiştir. Zira küçük işletmeciler, bu yükümlülüğü yerine getirmek amacıyla veri saklama konusunda uzmanlaşan şirketlerle iş ortaklığı kurabilmekte ya da hizmeti dış kaynaktan temin edebilmektedir. Bu durum ise veri işleme faaliyetlerinin denetlenmesi ve gerekli güvenlik tedbirlerinin alınması gibi yükümlülüklerde küçük işletmeciler için sorun oluşturabilmektedir. Bu nedenle, veri güvenliği konularının küçük ve orta ölçekli işletmeler üzerindeki etkileri göz önüne alınarak Veri Saklama Direktifinin tadil edilmesinin değerlendirileceği, AK tarafından belirtilmektedir. (EC, 2011).

Ciddi suç kavramının Veri Saklama Direktifinde tanımlanmamış olması, Direktif hükümlerini ulusal mevzuata aktaracak AB üyesi ülkelerin uygulamalarında farklılıklara neden olmuştur. Bu kapsamda, bazı ülkelerde ciddi suç kavramı hapis cezası gerektiren suçlara veya ulusal kanunlarda belirtilen suçlara hasredilirken bazı ülkelerde ise sadece ciddi suçlar hakkında değil ulusal güvenlik veya kamu

[39] CMK 135-137 Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilir.

güvenliğinin sağlanması gibi amaçlar için de veri saklama yükümlülüğü getirilmiştir (EC, 2011).

4.6.1 Sabit ve Mobil Telefon Hizmetleri

Sabit ve mobil telefon hizmetleri için saklanması gereken veriler şu şekilde sıralanmaktadır:[40]

1) Haberleşmenin takibi ve kaynağının belirlenmesi için; arayan tarafın telefon numarası, adı ve adresi.

2) Haberleşmenin sonlandırılacağı noktayı belirlemek için aranan tarafın adı, adresi, numarası, çağrı iletme ve çağrı transferi gibi ek hizmetlerin olması durumunda çağrının yönlendirildiği numara veya numaralar.

3) Haberleşmenin tarihi, zamanı ve süresini belirlemek için haberleşmenin başlangıç ve bitiş tarih ve saati.

4) Haberleşmenin türünü tanımlamak için kullanılan telefon hizmeti. Kullanıcıların haberleşme cihazlarını veya bunların ekipmanlarını tanımlamak için sabit şebeke telefonu ile ilgili olarak arayan ve aranan telefon numaraları. Mobil telefonla ilgili olarak aranan ve arayan telefon numaraları, arayan ve aranan tarafa ait IMSI ve IMEI; abone kaydı olmayan arama kartlı hizmetlerin olması durumunda hizmetin aktif hale getirildiği tarih ve zaman ile hizmetin aktif hale getirildiği hücre kimliği.

5) Mobil haberleşme cihazının konumunu tespit etmek için haberleşmenin başladığı hücre kimliği, haberleşme verilerinin saklandığı sure boyunca hücre kimlikleri ile ilgili olarak hücrelerin coğrafi konumlarını tanımlayan veriler.

---

[40] Veri Saklama Direktifi, M.5

4.6.2 İnternet Hizmetleri

İnternet hizmetleri için saklanması beklenen veriler ise şu şekildedir:[41]

1) Haberleşmenin takibi ve kaynağının belirlenmesi için internet ortamına erişim, internet e-posta ve internet telefonu ile ilgili olarak kullanıcı kimliği ve/veya telefon numarası, haberleşmenin gerçekleştiği zaman diliminde kendisine IP adresi, telefon numarası veya kullanıcı kimliği tahsis edilen abonenin adı ve adresi.

2) Haberleşmenin sonlandırılacağı noktayı belirlemek için internet, e-posta ve internet telefonu ile ilgili olarak aranan/alıcı tarafa ait telefon numarası ve/veya kullanıcı kimliği, adı ve adresi.

3) Haberleşmenin tarihi, zamanı ve süresini belirlemek için internet erişimi ile ilgili olarak oturum açma, kapatma tarih ve saati, internet servis sağlayıcısı tarafından tahsis edilen dinamik veya statik internet protokol adresi, abone ve kullanıcı kimliği, elektronik posta veya internet telefonu ile ilgili olarak oturum açma ve kapatma tarih ve saati.

4) Haberleşmenin türünü tanımlamak için internet ortamına erişim ve internet telefonu ile ilgili olarak kullanılan internet hizmeti.

5) Kullanıcıların haberleşme cihazlarını veya ekipmanlarını tanımlamak için sayısal abone hattı numarası ya da haberleşmenin kaynaklandığı diğer son noktalar ile çevirmeli ağ erişimi için arayan telefon numarası.

"AB üyesi ülke uygulamaları incelendiğinde sabit ve mobil telefon hizmetlerine ilişkin saklanan trafik verilerinin genel olarak Veri Saklama Direktifi ile uyumlu olduğu dile getirilmektedir. Öte yandan, internet hizmetlerine yönelik saklanan trafik verilerinde farklılıklar olduğu örneğin; internet sayfalarının URL adresi gibi haberleşmenin içeriği ile ilgili verilerin saklanabildiği VKCG (2010) tarafından

[41] Veri Saklama Direktifi, M.5

ifade edilerek Veri Saklama Direktifinin M.5'te yer alan verilerin yeterince kapsamlı olduğu ve bu nedenle direktif kapsamında işletmecilere ilave veri saklama yükümlülüğü getirilmemesi gerektiği belirtilmektedir.

Trafik verisinden ziyade içerik verisi sağladığı göz önüne alındığında İnternet Arama Motorlarının Veri Saklama Direktifi kapsamında değerlendirilmemesi

gerektiği VKCG tarafından ifade edilmiş olmasına rağmen, Avrupa Parlamentosu AK'ye gönderdiği yazılı bildirimde çocuk pornografisi ve cinsel suçlarla mücadele etmek için direktifin arama motorlarını da içerecek şekilde genişletilmesini talep etmiştir. AK, bu görüşleri değerlendirerek saklanacak veri türlerinde değişikliğe ihtiyaç olup olmadığını belirleyecektir (EC, 2011)."[42]

4.6.3 Saklanan Verilerin Korunması ve Güvenliği

"Veri Saklama Direktifi kapsamında saklanan verilere ulaşılabilirlik, kişilerin tercihleri, düşünceleri ve davranışları hakkında fikir verebildiğinden kişilerin özel hayatlarına müdahale edilme riskini içermekte ve haberleşmenin gizliliğini zedeleyebilmektedir. Örneğin, elektronik haberleşme ile ilgili konum verilerine yetkisiz erişim sağlanması ve/veya bu verilerin yetkisiz bicimde ifşa edilmesi ilgili kişilerin mahremiyetlerini önemli ölçüde etkilemektedir. Bu yüksek risk karşısında, uygun teknik ve idari tedbirlerin alınması gerekli olmaktadır (VKCG, 2010).

Veri Saklama Direktifinde saklanan verilere ilişkin olarak işletmeciler tarafından yerine getirilmesi gereken 4 veri güvenliği ilkesi şu şekilde sıralanmaktadır:

1) Saklanan veriler, şebekedeki diğer verilerle aynı kalitede olmalı, aynı güvenlik ve koruma tabirlerine tabi tutulmalıdır,

2) Saklanan verilerin istem dışı, yetki dışı ya da yasa dışı, erişim, tahrip, kayıp, değişiklik, depolama, işleme ve ifşa fiillerine karşı korunması için uygun teknik

---

[42] Şahin, O (82-90)

ve idari tedbirler alınmalıdır,

3) Verilerin sadece özel yetkilendirilmiş personel tarafından erişilebilir olmasının sağlanması için uygun teknik ve idari tedbirler alınmalıdır,

4) Veriler saklama süresi sonunda imha edilmelidir. Üçüncü maddede belirtilen veri güvenliği ilkesinin sağlanması için VKCG (2010) tarafından tavsiye edilen ancak mevcut durumda bütün işletmeciler tarafından uygulanmadığı belirtilen teknik ve idari tedbirlerin bir kısmı aşağıda yer almaktadır:

- Kullanıcı sorumlulukları ve profillerinin tanımlanmasıyla, saklanan verilere güçlü erişim kontrolü,
- Sisteme erişim için şifre+biyometri, şifre+simge (token) gibi çift kimlik denetimi mekanizmalarının kullanılması,
- En az, kullanıcı kimliği, erişim zamanı ve erişilen dosya bilgilerinden oluşan log kayıtlarının saklanmasıyla, veri işleme ve sisteme erişim faaliyetlerinin ayrıntılı olarak takip edilebilmesi,
- Log bütünlüğünün sağlanması için log yönetim sistemi kurulması,
- Veri saklama sisteminin, trafik verilerini ticari amaçlı işleyen sistemlerden mantıksal olarak ayrılması,
- Veri gizliliğini sağlayacak ilave tedbirler,
- İdari tedbirler açısından trafik verilerinin saklandığı sistemden sorumlu yöneticilere özel önem verilmesi, bu yöneticilerin görevlerinin detaylandırılması ve sistem üzerinde gerçekleştirilen faaliyetlerin kapsamlı biçimde denetlenmesi.

Yine işletmecilerin hangi verilerin ne zaman ve kim tarafından sisteme girildiğini, bu verilerin kimlere transfer edildiğini, üzerinde ne tur işlemler yapıldığına ilişkin bilgileri sağlayacak teknik tedbirleri temin etmesi gerekmektedir. Bu amaçla, kontrolörün işlemeyi yapan yetkililere ait isim, yetkilendirme tarihinin başlangıcı ve sonu, verilerin bir bilgisayar aracılığıyla işlenmesi durumunda kimlik tespitine yarayan araçları belirleyen tam listeyi tutması gerekir.

AB üyesi ülke uygulamalarına işletmeciler acısından bakıldığında ise büyük ölçekli işletmelerin uygun güvenlik seviyesi sağlamak için gerekli teknik ve idari tedbirleri almaya çalıştıkları ancak küçük ölçekli işletmelerin maliyet stratejileri nedeniyle daha düşük güvenlik standartları sağladıkları, bu kapsamda trafik verilerinin saklanmasına ilişkin risklerin farkındalığı hakkında bir standart olmadığı belirtilmektedir.[43]

AK, saklanan verilerin kişisel ve hassas niteliği nedeniyle depolanması, elde edilmesi ve kullanılması surecinde, veri ihlali riskini en aza indirmek ve AB vatandaşlarının güvenliğini sağlamak amacıyla yüksek standartlarda veri koruma ve güvenliğinin sağlanması gerektiğini, bu kapsamda EKG'nin tavsiyelerini de göz önüne alarak tasarımsal gizlilik ilkesinin benimsenmesi dahil veri koruma ve veri güvenliği standartlarının güçlendirilmesine ilişkin seçeneklerin değerlendirileceğini beyan etmiştir (EC, 2011).

4.6.3.1 Kişisel Verilerin Korunmasında Teknolojik Yaklaşımlar

Kişisel verilerin korunmasında yasal düzenlemelerin önemi tartışılmaz olmakla birlikte teknik yöntemlerin yasal düzenlemelere dahil edilmesinin gizliliğin korunmasında tamamlayıcı bir rol üstleneceği değerlendirilmektedir. Bu çerçevede tasarımsal gizlilik ilkesi ile gizliliği artırıcı teknolojilerden bahsetmek yerinde olacaktır.

4.6.3.1.1 Tasarımsal Gizlilik

Tasarımsal gizlilik, "Teknolojilerin tasarım, kurulum, kullanım ve kaldırılma safhalarını içeren yaşam döngülerinin tamamında kişisel verilerin ve gizliliğin tümleşik olarak bulunması" olarak tanımlanmaktadır (EU, 2010a).

"Sistemlerin işlevselliğine sıkıntı getirmeden, kişisel verilerin ayrıştırılması ya da gerektiği kadar kullanılması suretiyle kişisel verilerin gereksiz biçimde ya da istek dışı işlenmesini engelleyerek gizliliğin korunmasını sağlayan bilgi ve iletişim

[43] VKCG, 2010

teknolojileri sistemlerine yönelik önlemler."[44]

Kişisel verilere yetkisiz erişimin engellenmesi amacıyla alınan güvenlik tedbirleri gizliliğin önemli bir unsuru olmasına rağmen gizliliğin her zaman korunacağını taahhüt edememektedir. İşlenmek üzere açılmış veya başkaları tarafından böyle bir veri bahsi geçiyorsa belirlenen amaçlar doğrultusunda verilerin gereken ölçüde toplanması ve kullanılmasını teşvik etmek gerekmektedir, aksi durumda verilerin kontrolünü sağlamak güçleşecektir. Bu sebeple ilgili kişinin rızası olmadan ikincil kullanımlarının engellenmesi gibi daha geniş alanları korunması gerekmektedir.

İnternet, mobil telefonlar, RFID, sosyal ağ siteleri, biyometri, bulut bilişimi (cloud computing) gibi araçlarla sayısal ayak izlerinin bırakılabildiği bir ortamda her turlu verinin işlenip depolanabilmesi ihtimaline karşın alınabilecek en önemli önlemlerden birisi teknolojik yeniliklerle bir bireyin mahremiyetinin ihlal edilme olasılığını en aza indirmektir. Örneğin, bir takside kilometre ölçmek amacıyla yer alan ve aracın konum verisini sürekli olarak merkezi bir veri tabanına ileten cihazla, konum verileri sürücünün kontrolünde olacak şekilde tasarlanan bir cihaz arasında bireyin mahremiyeti açısından farklılık bulunmaktadır.[45]

E-Gizlilik Direktifinde işletmeciler, sundukları hizmetlerin güvenliğini garanti altına almak için uygun teknik ve idari tedbirleri almakla yükümlü kılınırken Veri Saklama Direktifinin 7. maddesinde ise saklanan verilerin tedbirsizlikle, hukuka aykırı veya yetkisiz olarak tahrip edilmesi, kaybolması, değiştirilmesi, depolanması, işlenmesi, ifşa edilmesi ve belirtilen verilere erişilmesine karşı uygun teknik ve idari tedbirlerin alınması gerekli görülmektedir. Bununla birlikte Veri Koruma Direktifinde teknik ve idari tedbirlerin, gerek sistemlerin tasarım aşamasında gerekse veri işleme esnasında alınması gereken tedbirleri kapsayacağı belirtilmektedir.[46]

Her ne kadar AB düzeyinde kişisel verilerin ve gizliliğin korunmasına yönelik

[44] Borking vd., 2003
[45] DUTCHDPA, 2009
[46] Veri Koruma Direktifi, dibace 46

güçlü bir yasal çerçeve bulunuyor olsa da bilgi ve iletişim teknolojilerindeki gelişmeler bireylerin haklarının korunması için yeni aksiyonların alınmasını gerekli kılmaktadır. Bunun için tasarımsal gizliliğin bir ilke olarak benimsenmesi ve mevcut yasal çerçeveye dahil edilmesi gizliliğin korunmasında önemli bir adım olacaktır.[47]

Bu ilke, veri kontrolörleri yanında teknoloji tasarımcıları ve üreticileri için de bağlayıcı olmalı, bilgi ve iletişim teknolojilerinin sadece güvenliği sağlamaları değil aynı zamanda kişisel verilerin gerekli kapsam ve ölçüde işlenmelerine imkan sağlamalıdır. Bu ilkenin gerekliliği, Almanya'da yaşanan örnekle desteklenmektedir.[48] Alman Federal Anayasa Mahkemesinin istihbarat birimlerince teknik araçların kullanılarak bilgi teknoloji sistemlerine gizlice erişmelerine olanak sağlayan kanun hakkında 27 Şubat 2008 tarihinde verdiği kararda "bilgi teknoloji sistemlerinin bütünlüğü ve gizliliğinin sağlanmasının" temel haklar arasında olduğu ve bu hakkın kanunla ihlal edildiği belirtilmiştir.[49]

"Tasarımsal gizliliğin ilke olarak benimsenmesi, gizliliği artırıcı teknolojilere olan ihtiyacın önemini artıracak olmakla birlikte kişisel verilerin korunmasını sağlayan araçların (örneğin varsayılan gizlilik ayarları, şifreleme, erişim kontrolleri) uygulanmasını sağlayacak aynı zamanda sosyal ağlar, arama motorları, Wi-Fi yönlendiricileri gibi üçüncü taraflara ve bireysel müşterilere sağlanan ürün ve hizmetler için kritik bir gereklilik olacaktır.

Tasarımsal gizlilik ilkesi hızlı gelişen teknolojik ve sosyal çevre karşısında sürdürülebilirliğini sağlamak için teknolojiden bağımsız tanımlanmalı, ayrıca "mümkün olan en kısa zaman" özelliğini barındırdığı vurgulanmalıdır.[50]

Zira gizlilik ilkeleri sistem geliştirmelerinin başlangıç aşamasında düşünülmezse ortaya çıkacak zararların bertaraf edilmesi için geç kalınmakta ve sistemlerin

---

[47] EDPS, 2010
[48] VKCG, 2009
[49] Hornung, 2009
[50] VKCG, 2009

onarılması ekonomik açıdan da maliyetli olabilmektedir. Son yıllarda artan sayıda yaşanan veri ihlalleri bu görüşü doğrularken tasarımsal gizliliğe olan gereksinimi de ortaya koymaktadır.[51]

Cavoukian (2011) tasarımsal gizliliğin hedeflerinin 7 temel unsur sayesinde gerçekleştirilebileceğini belirtmektedir:

- Proaktiflik: Gizliliğe aykırılık teşkil edebilecek vakalar, gerçekleşmeden önce engellenir,
- Varsayılan ayarlar: Herhangi bir IT sisteminde kişisel veriler otomatik olarak korunmalıdır. Bireylerin kişisel verilerini korumaları için ilave önlem almalarına gerek yoktur zira bu önlemlerin sistem içinde zaten var olmaları beklenmektedir,
- Tasarıma eklenme: Tasarımsal gizlilik IT sistemlerine tasarım aşamasında yerleştirilir, bu durumda gizlilik ihlalleri gerçekleştikten sonra sisteme ilave edilen bir eklenti olmaz,
- Tam işlevsellik: Tasarımsal gizlilik bütün meşru menfaatleri ve hedefleri (gizlilik ve güvenliğin aynı anda sağlanması gibi) barındırır,
- Baştan sona güvenlik: Veriler elde edilmeden önce sisteme gömülen tasarımsal gizlilik, verinin yaşam döngüsü boyunca güvenli biçimde saklanmasını ve sürecin bitiminde silinmesini sağlar,
- Görünürlük ve şeffaflık: Tasarımsal gizlilik, ilgili tarafların belirlenen amaçlar doğrultusunda işlem yapıp yapmadıklarını garanti altına almayı hedefler. Yapılan işlemler hem kullanıcılara hem de hizmet sağlayıcılara açıktır,
- Bireyin mahremiyetine saygı: Tasarımsal gizlilik, ilgili aktörlerin bireylerin menfaatlerini en üstte tutmalarını gerektirir.

VKCG (2009)'ye göre ise veri işleme özelliğine sahip sistemlerin tasarımı esnasında ve bu sistemleri çalıştırırken aşağıdaki özellikler göz önünde

[51] EDPS, 2010

bulundurulmalıdır:

- Verinin en aza indirilmesi: Veri işleme sistemleri gerekli olandan daha fazla kişisel veri içermeyecek biçimde tasarlanmalıdır,
- Kontrol edilebilirlik: IT sistemleri, kişisel verilerini kontrol edebilmeleri için bireylere etkili mekanizma sunmalı, bireylerin rıza ve ret durumları bu mekanizmalar tarafından desteklenmelidir,
- Şeffaflık: Sistemlerin etkinliği hakkında bireyler yeterince bilgilendirilmeli, elektronik erişim veya bilgilendirilme sağlanmalıdır,
- Kullanıcı dostu sistemler: Her seviyede kullanıcıya hitap etmeleri için sistemler basit ara yüzler sağlamalıdır,
- Verinin gizliliği: IT sistemleri kişisel verilere sadece yetkili kişiler erişecek şekilde tasarlanmalı ve güvenliği sağlanmalıdır,
- Veri kalitesi: Veri kontrolörleri gerektiğinde ilgili verilere yasal amaçlarla erişilebilmesini sağlamalıdır,
- Kullanımın sınırlandırılması: Farklı amaçlara hizmet eden (bulut bilişimi vb.) işlem ve veriler güvenli biçimde birbirlerinden ayırt edilmelidir.[52]

Bu kapsamda, tasarımsal gizlilik ilkesinin yasal düzenlemelerde yer alması işletmecilerin yeterli koruma tedbirleri almalarını tetikleyecek, olası veri ihlallerinin önüne geçilerek gerek tüketiciler gerekse işletmeciler açısından fayda sağlanmış olacaktır.

[52] Şahin, O, 92-97

5. TÜRKİYE İNCELEMESİ

AB uyum programları kapsamında imzalamış olduğu direktifleri hayat geçirmeyi planlayan Türkiye 2010 yılı Anayasa değişikliği paketiyle 1982 Anayasası'nın kişinin "Özel hayatın gizliliği" başlıklı ikinci bölüm 20. maddesinde, "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

1- 6 Şubat 2004 tarihli ve 25365 sayılı Resmi Gazete.

2- 13 Mayıs 2010 tarihli ve 27580 sayılı Resmi Gazete.

hükmüne yer verilerek en temel hak olan kişisel verilerin korunması ülkemizde kanun kapsamına alınmıştır.

Bu kapsamda kişisel verilerin korunması ancak kişiler verilerin işlenmesi kavramının, nitelikli olarak geniş bir içerikle değerlendirilebilmesiyle mümkündür. Çünkü korunma, kişisel verilerin toplanması ile başlar işlenmesinden silinmesine kadar devam eder. Kişisel verilerin işlenmesi, Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması Yönetmeliği (TSKVKY) M. 3'te, "Otomatik olsun veya olmasın, toplama, kaydetme, hazırlama, yükleme, uyarlama, değiştirme, geri çağırma, danışma, kullanma, aktarma yoluyla açığa vurma, yayma ya da bunların dışında erişilebilir hale getirme, düzenleme, birleştirme, engelleme, silme gibi yollardan, kişisel bilgiler üzerinden yürütülmekte olan herhangi bir işlem ya da işlemler bütünü" olarak belirtilmektedir. Kişisel verilerin toplanması, değiştirilmesi, saklanması ve silinmesi işleme kavramı içinde tutulmaktadır.

Kişisel verilerin işlenmesini isteme hakkını; kişisel veriler hakkında haberdar olma, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve hangi amaçlar doğrultusunda kullanımı hakkında bilgi edinebilme haklarını da anayasal güvence altında saklı tutmakta ve ancak kişinin acık rızasının bulunması kaydıyla işlenebileceği güvencesini içermektedir.

AB'nin 2010 yılı Türkiye ilerleme raporunda kişisel verilerin korunması ve bilgiye erişim konularında ilerleme kaydedildiği belirtilmiştir.[53]

12 Ekim 2004 tarihli ve 25611 sayılı Resmi Gazete'nde yayımlanan 5237 sayılı Türk Ceza Kanunu'nun (TCK) "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümünde 135. , 136. ve 138. maddeleri kapsamında haberleşmenin gizliliği yanında kişisel verilerle ilgili hükümlere yer verilmektedir.

- 135. maddesinde kişisel verileri hukuka aykırı olarak kaydeden kimse ile kişilerin siyasî, felsefî veya dinî görüşlerine, kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimseler hakkında altı aydan üç yıla kadar,
- 136. maddesinde kişisel verileri hukuka aykırı olarak elde eden, yayan veya bir başkasına aktaran kimse hakkında bir yıldan dört yıla kadar,
- 138. maddesinde kanunlarda öngörülen süreler bitmiş olmasına rağmen kişisel verileri silmekle yükümlü olanların görevlerini yerine getirmemeleri durumunda altı aydan bir yıla kadar hapis cezası öngörülmektedir.

---

[53] ABGS, 2010

5237 s. Türk Ceza Kanunu Md. 135,136, 138	Kişisel verilerin hukuka aykırı olarak verme veya ele geçirme (md.136)	Kişisel verileri hukuka aykırı olarak kaydedilmesi (135. Md.)	Verileri yok etmeme (md.138.)
Maddi Unsur	Kişisel verilerin kaydedilmesi	Başkasına verme, Yayma, Ele geçirme	Sistem içinde veriyi yok etmeme
Manevi Unsur	Kasıt	Kasıt	Kasıt
İşleme Sekli	Otomatik / Elle	Otomatik / Elle	Otomatik/ Elle işleme sistemin yorumuna bağlı
Uygulama alanı	Kamu / Özel	Kamu / Özel	Kamu / Özel
Şikayet şartı	Yok (Md. 139)	Yok (Md. 139)	Yok (Md. 139)
137. maddede yer alan ağırlatıcı nedenlerin uygulanma sebebi (cezada yan oranında artırım getiren)	-kamu görevlisi tarafından görevin verdiği yetkinin kötüye kullanılması -belli meslek/sanatın sağladığı yetkinin kötüye kullanılması	-kamu görevlisi tarafından görevin verdiği yetkinin kötüye kullanılması -belli meslek/sanatın sağladığı yetkinin kötüye kullanılması	
Ceza	6 aydan 3 yıla kadar hapis cezası (137. maddede sayılan ağırlatıcı nedenlerin varlığı halinde yan oranında artırılır)	1 yıldan 4 yıla kadar hapis cezası (137. maddede sayılan ağırlatıcı nedenlerin varlığı halinde yan oranında artırılır)	6 aydan 1 yıla kadar hapis cezası (137. maddede sayılan ağırlaştırıcı nedenlerin varlığı halinde yan oranında artırılır)
Tüzel kişilere özgü güvenlik tedbirleri (140. Md. dolayısıyla 60. Md.)	Evet	Evet	Evet

Bu düzenlemeler 10 Kasım 2008 tarihinde yürürlüğe giren Elektronik Haberleşme Kanunu (EHK) veri gizliliğine ilişkin hükümleri kapsamaktadır. BTK'nın görev ve yetkileri bu kanunda belirlenmiştir. "Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak" ve sektörel ihtiyaçları teknolojide meydana gelen değişikliklerle düzenleme ve kişisel veri gizliliği koruması durumunda yetkili kılmıştır.

5.1 Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Taslağı

Yönetmeliğin hazırlanmasında 2002/58/EC ve 2006/24/EC sayılı Direktiflerin esas alınarak hazırlanan bu yönetmelikte kişisel verilerin saklanması, kişisel verilerin değiştirilmesi, şifrelenerek maskelenerek saklanması bu kapsamda, Taslak Yönetmeliğin bazı yönleri ile 2009/136/EC Direktifine uyumlaştırılması amacıyla 2009/136/EC sayılı Direktifte yer alan "kişisel veri ihlali" tanımının aşağıda yer verilen şekilde Taslak Yönetmeliğe eklenmesi uygun olacaktır.

Kişisel veri ihlali: İletilen, kaydedilen veya kamuya açık elektronik haberleşme hizmetinin teminiyle bağlantılı olarak başka şekilde işlenen kişisel verilere yetkisiz erişilmesine ya da söz konusu verilerin tedbirsizlikle veya hukuka aykırı olarak yok edilmesi, kaybolması, değiştirilmesi, yetkisiz olarak ifşa edilmesine neden olan güvenlik ihlali 2009/136/EC Direktifi ile konum verisi tanımına "elektronik haberleşme hizmeti aracılığıyla" ifadesi eklendiğinden, konum verisi tanımının da bu doğrultuda değiştirilmesi yerinde olacaktır.

Taslak Yönetmeliğin 4. maddesinde Kişisel VKKT'de düzenlenen kişisel verilerin işlenmesine ilişkin ilkelere yer verilmektedir.

Bu çerçevede,

MADDE 4 – (1) Kişisel verilerin;

a) Hukuka ve dürüstlük kurallarına uygun olarak işlenmesi,

b) İlgili kişinin rızasına dayalı olarak işlenmesi,

c) Elde edilme amacıyla bağlantılı, yeterli ve orantılı olması,

ç) Doğru olması ve gerektiğinde güncellenmesi,

d) İlgili kişilerin kimliklerini belirtecek biçimde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar muhafaza edilmesi esastır.

Elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin kişisel verileri işlerken uyması beklenen durumlar belirtilmek suretiyle 95/46/EC Veri Koruma Direktifi kabul kriterleri de sağlanmış bulunmaktadır.

"Güvenlik" ve "Riskin bildirilmesi" başlıklı 5. ve 6. maddeler mevcut yönetmelikle paralel ele alınmış olmakla birlikte 2009/136/EC Direktifiyle kişisel verilerin ihlali konusunda işletmecilere getirilen yükümlülüklerin düzenlenmediği görülmektedir. Bu itibarla, 5. maddenin birinci fıkrasından sonra aşağıdaki hüküm yer almalıdır:

Birinci fıkrada belirtilen tedbirler asgari,

a) Kişisel verilere sadece yetkili personelin yasal amaçlarla erişmesinin garanti altına alınmasını,

b) Kişisel verilerin tedbirsizlikle, hukuka aykırı veya yetkisiz olarak tahrip edilmesi, kaybolması, değiştirilmesi, depolanması veya başka bir ortama kaydedilmesi, işlenmesi, ifşa edilmesi ve söz konusu verilere erişilmesine karşı korunmasını,

c) Kişisel verilerin işlenmesine yönelik bir güvenlik politikası uygulamasının garanti altına alınmasını içermelidir.

MADDE 5 – Güvenlik

(1) İşletmeciler, kişisel verilerin işlenmesine ilişkin olarak güvenlik politikası belirler. İşletmeciler şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alır. Söz konusu güvenlik tedbirleri, teknolojik imkânlar göz önünde bulundurularak muhtemel riske uygun bir düzeyde sağlanır.

(2) Birinci fıkrada belirtilen tedbirler, asgari istem dışı, yetki dışı ya da yasa dışı olarak; kişisel verilerin tahrip edilmesi, kaybolması, değiştirilmesi, depolanması veya başka bir ortama kaydedilmesi, işlenmesi, ifşa edilmesi ve söz konusu verilere erişilmesine karşı kişisel verilerin korunmasını içerir.

(3) İşletmeciler, kişisel verilere sadece yetkili kişiler tarafından erişilebilmesini ve kişisel verilerin tutulduğu sistemlerin ve kişisel verilere erişim sağlamak için kullanılan uygulamaların güvenliğini sağlamakla yükümlüdür.

(4) İşletmeciler, kişisel verilere ve ilişkili diğer sistemlere sağlanan tüm erişimlere ve erişim yetkisi olan personelin yaptığı işlemlere dair detaylı işlem kayıtlarını beş yıl süreyle tutmakla yükümlüdür.

(5) Kurum, gerekli gördüğü hallerde işletmecilerden, kişisel verilerin tutulduğu sistemlere ve aldıkları güvenlik tedbirlerine ilişkin tüm bilgi ve belgeleri isteme, ayrıca söz konusu güvenlik tedbirlerinde değişiklik talep etme hakkını haizdir.

Kişisel verilerin hizmetinin üzerlerinden sunulduğu cihazların güvenlik tedbirlerinin alınması gerekmekte olup casus yazılımlar, Virüsler ve istenmeyen yazılımlar tarafından bu bilgilerin erişimi ve izlenmesine yönelik tedbir almak amaçlanmakla birlikte muhtemel risk ve önlem işletmeciler tarafından yeterince caydırıcılığı bulunmadığı için bir güvenlik zafiyeti oluşturabilecektir.

İşletmelerin yetkili kılmış olduğu kişilerin bu ortamlarda yaptığı işlemler de önemlidir. Bu işlem kayıtlarının yani logları'nın tutuluyor olması bu verilerin gizli bir takım ticari işlemlere dönüşmesinin önüne geçmektedir.

MADDE 6 – Riskin ve kişisel veri ihlalinin bildirilmesi

(1) İşletmeci, şebekenin ve kişisel verilerin güvenliğini ihlal eden belirli bir risk olması durumunda bu risk hakkında kurumu ve abonelerini/kullanıcılarını etkin ve hızlı bir şekilde bilgilendirmekle yükümlüdür.

(2) Bu riskin işletmeci tarafından alınan tedbirlerin dışında kalması halinde, söz konusu riskin kapsamı, giderilme yöntemleri ve yaklaşık maliyeti hakkında abonelerin/kullanıcıların etkin ve hızlı bir şekilde bilgilendirilmesi sağlanır.

(3) İşletmeci, kişisel veri ihlali olması durumunda söz konusu ihlalin niteliği ve sonuçları hakkında abonelere/kullanıcılara yapılacak bilgilendirmenin detayları ve ihlalin giderilmesi için alınan tedbirlere ilişkin olarak kurumu bilgilendirir.

(4) Kişisel veri ihlalinden abonelerin/kullanıcıların olumsuz yönde etkilenme ihtimalinin bulunması halinde işletmeci, kişisel veri ihlalinin niteliğine, daha fazla bilginin elde edilebileceği iletişim noktalarına ve ihlalin olası olumsuz etkilerini azaltmak için aboneler/kullanıcılar tarafından alınabilecek önlemlere ilişkin olarak aboneleri/kullanıcıları ücretsiz olarak bilgilendirir.

(5) İşletmeci, gerçekleşen kişisel veri ihlallerine ilişkin olarak söz konusu ihlalin sebeplerini, etkilerini ve çözüme yönelik tedbirleri içeren bilgileri gizliliğini ve bütünlüğünü sağlayarak kaydetmekle yükümlüdür.

Madde 5'te beklenilen güvenlik tedbirlerinden bahsedilirken madde 6 ise ihmal veya kasıtlı durumlarda işletmecileri bekleyen yükümlülüklerden bahsedilmektedir.

İşletmecilerin almış olması gereken güvenlik standartlarının ve bu kontrollerin sağlandığına dair bilgi ve belgeler ile birlikte ihlali oluşturacak durumun detaylarının da paylaşılmasını istemek faydalı olacaktır.

Verilerin İşlenmesi ve Saklanması

MADDE 7 – Haberleşmenin gizliliği

(1) Elektronik haberleşme ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve gözetimi yasaktır.

(2) Elektronik haberleşme şebekeleri, haberleşmenin iletimini gerçekleştirmek dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili kullanıcıların/abonelerin verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve rızalarının alınması kaydıyla kullanılabilir.

Madde 7/2 ye rıza alınması ibaresinin eklenmemesi durumunda NFC işlemlerinin yapılmasına engel teşkil edilecekti.

MADDE 8 – Trafik verisinin işlenmesi

(1) İşletmeciler, sundukları hizmetin kapsamı dışındaki amaçlar için trafik verisini işleyemez.

(2) Trafik verisi, ilgili mevzuat hükümlerine uygun olarak, trafiğin yönetimi, ara bağlantı, faturalama, yolsuzluk tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile ara bağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır.

(3) Elektronik haberleşme hizmetlerini pazarlamak veya katma değerli elektronik haberleşme hizmetleri sunmak amacıyla ihtiyaç duyulan trafik verileri, ilgili abonelerin/kullanıcıların işlenecek trafik verisinin türü ve işlenme süresi hakkında bilgilendirilmelerinden sonra rızalarının alınması kaydıyla, alınan rızaya uygun olarak sadece katma değerli elektronik haberleşme hizmetlerinin, pazarlama

faaliyetlerinin ve benzer hizmetlerin gerektirdiği ölçüde ve sürede işlenebilir.

(4) İşletmeci tarafından abonelere/kullanıcılara ait işlenen ve saklanan trafik verileri, bu verilerin işlenmesini ve saklanmasını gerekli kılan faaliyetin tamamlanmasından sonra silinir veya anonim hale getirilir.

(5) İşletmeciler, abonelerin/kullanıcıların, kısa mesaj, çağrı merkezi, internet ve benzeri yöntemlerle vermiş oldukları rızayı aynı yöntem ya da basit bir yöntem ile her zaman ücretsiz olarak geri almalarına imkân sağlar.

Trafik verisi tanımının daha net olarak belirtilmesi gerekmektedir, işletmeciler ve işletme yetkili personelleri tarafından abonelerin faturalandırılması ve ara bağlantı ödemeleri kontrolleri gerçekleştirilmektedir. İşletmecilerin ücretlendirme uygulamalarını outsource (dışkaynak) ile karşıladıkları durumlarda faturalandırma bu aracı firmalar (Vendor) üzerinden gerçekleşmektedir. Bazı vendor firmaların yurtdışında olduğunda düşünülürse o zaman bu maddenin verilerin yurtdışına çıkartılmaması ibaresi geçen madde 9 trafik verisi işleme yetkisi ile çelişmektedir. İşletmeci yurtiçinde veya yurtdışında bir vendor'ı yetkili tayin edebilir mi ? Edebildiği varsayımıyla bu veriler bir proxy server üzerinden yetkili vendor firmaya taşınırsa hangi kapsamda değerlendirilmesi gerekmektedir.

Ücretlendirmenin Vendor üzerinden gerçekleştiği durumlarda işletmecinin mi yoksa Vendor firmanın mı logları kabul edilecektir sorularının cevaplarına ulaşabilmek için trafik verisi işleme yetkilisi ve Vendor firma yetkili durumlarından detaylıca bahsedilmesi yerinde olacaktır.

MADDE 11 – Konum verisinin işlenmesi

(1) İşletmeciler, abonelerin/kullanıcıların konum verisini ancak, katma değerli elektronik haberleşme hizmetlerinin sunumu halinde abonelerin/kullanıcıların rızasını alarak bu hizmetlerin sunumu için gerekli olan ölçü ve sürede ya da anonim hale getirmek suretiyle işleyebilir.

(2) İşletmeciler; aboneleri/kullanıcıları, rızalarını almadan önce, işlenecek konum verisinin türü, işlenme amacı ve süresi hakkında bilgilendirir.

(3) İşletmeciler, abonelerin/kullanıcıların konum verilerinin işlenmesi için, kısa mesaj, çağrı merkezi, internet ve benzeri yöntemlerle vermiş oldukları rızayı aynı yöntem ya da basit bir yöntem ile her zaman ücretsiz olarak geri almalarına imkân sağlar.

(4) İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, ancak acil yardım çağrıları kapsamında abonenin/kullanıcının rızası aranmaksızın konum verisi ve ilgili kişilerin kimlik bilgileri işlenebilir.

MADDE 12 – (1) Konum verisini işleme yetkisi işletmeci tarafından yetkilendirilen kişilerle sınırlı olup, bu yetki söz konusu hizmetlerin gerektirdiği kapsamda kullanılır. Söz konusu veriler, maskeleme yapılmaksızın işletmeci bünyesi dışına çıkarılamaz.

(2) Konum verileri hiçbir şekilde yurt dışına çıkarılamaz.

Katma değerli bir servis hizmeti olarak işletmecilerin portföyünde bulunan bu uygulamaların kurumsal kullanımı da bulunmaktadır, bir işyeri satış personeli takibi gibi.

Konum verisinin işlenmesine bir sınır getirilmemesi özel hayat ilkesiyle ters düşmektedir. 7x24 saatine dayalı bir konumlandırma yapılacağı bilginizin yöneticiniz isteğiyle size iletilmesinde sizin bilginizin olması çokta bir anlam ifade etmemektedir. Ayrıca saha personelinin konumlandırma uygulamalarını kullanıyor olması işletmecilerin kendilerinde bu personel konumla bilgileri üzerinden farklı veri anlamlandırma varyasyonları ile veriyi işlenmemesi gerektiğinin belirtilmesi, sadece sizin konumunuzun sizin istediğiniz uygulama kapsamıyla sınırlandırıldığını belirtmeye yardımcı olacaktır. Acil yardım durumlarında ise yargı kararlarının çıkması çok zaman alabildiğinde müdahale etme yetkisi verilmiş kurumlara bu hakkın özel olarak verilmesinin

değerlendirilmesi hayat kurtarmada zamanın önemine yardımcı olacaktır.

Vendor ve verinin yurtdışına çıkarılması mevzusu burada da gündeme gelecektir. MPS (Mobile Positioning ismini verdiğimiz bu uygulamaların desteği vendorlar tarafından alınmaktadır.)

MADDE 13 – (1) Bu Yönetmelik kapsamında saklanması öngörülen veri kategorileri, aşağıda belirtilmiştir.

a) Haberleşmenin takibi ve kaynağının tanımlanması için:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; gerçekleşmeyen aramalar da dâhil olmak üzere haberleşmenin başlatıldığı hatta ait telefon numarası, abonenin adı ve adresi, hattın hangi tarihte hangi aboneye tahsis edildiğine ait bilgi.

2) İnternet ortamına erişim, elektronik posta ve internet telefonu ile ilgili olarak; tahsis edilmiş kullanıcı kimliği ve/veya telefon numarası, haberleşmenin gerçekleştiği andaki internet protokol adresi, abonenin/kullanıcının adı ve adresi.

b) Haberleşmenin sonlandırılacağı noktayı belirlemek için:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; haberleşmenin sonlandırıldığı/sonlandırılacağı numara veya numaralar, çağrı iletme ve çağrı transferi gibi ek hizmetlerin olması durumunda çağrının yönlendirildiği numara veya numaralar, abonelerin adı ve adresi.

2) Elektronik posta ve internet telefonu ile ilgili olarak; elektronik posta alıcılarına ait kullanıcı kimliği, internet telefonu ile aranan alıcılara ait kullanıcı kimliği veya telefon numarası, internet telefonu veya elektronik posta alıcılarının adı ve adresi.

c) Haberleşmenin tarihi, zamanı ve süresini belirlemek için:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; haberleşmenin başlangıç ile bitiş tarih ve zamanı.

2) İnternet erişimi, elektronik posta ve internet telefonu ile ilgili olarak; internet erişimi ile ilgili oturum açma, kapatma tarihi ve zamanı, tahsis edilen dinamik veya statik internet protokol adresi, abone/kullanıcı kimliği, elektronik posta veya internet telefonu ile ilgili oturum açma ile kapatma tarihi ve zamanı.

ç) Haberleşmenin türünü tanımlamak için:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; kullanılan elektronik haberleşme hizmeti.

2) Elektronik posta ve internet telefonu ile ilgili olarak; kullanılan internet hizmeti.

d) Kullanıcıların haberleşme cihazlarını veya bunların ekipmanlarını tanımlamak için:

1) Sabit telefon hizmetiyle ilgili olarak; haberleşmenin başlatıldığı ve sonlandırıldığı telefon numaraları.

2) Mobil telefon hizmetiyle ilgili olarak; haberleşmenin başlatıldığı ve sonlandırıldığı telefon numaraları, haberleşmenin başlatıldığı ve sonlandırıldığı tarafa ait IMSI ve IMEI numaraları; abone kaydı olmayan arama kartlı hizmetlerin olması durumunda hizmetin aktif hale getirildiği tarih ve zaman ile hizmetin aktif hale getirildiği hücre kimliği.

3) İnternet ortamına erişim, elektronik posta ve internet telefonu ile ilgili olarak; çevirmeli ağ erişimi için arayan telefon numarası, sayısal abone hattı numarası ya da haberleşmenin kaynaklandığı diğer nokta.

e) İlgili mevzuatın öngördüğü hallerde mobil haberleşme cihazının konumunu tespit etmek için; haberleşmenin başladığı hücre kimliği, haberleşme verilerinin saklandığı sürede hücre kimlikleri ile ilgili olarak hücrelerin coğrafi konumlarını tanımlayan veri, hücre adresi ve hücre kimliğinin o adrese atanma ve kaldırılma tarihleri.

(2) Bu Yönetmelik kapsamında, elektronik posta ve internet telefonu ile ilgili olarak verilerin saklanmasına ilişkin getirilen yükümlülükler, sadece işletmecilerin kendilerinin sundukları hizmetler ile sınırlıdır.

Veri saklama süresi

MADDE 14 – (1) 13 üncü madde kapsamında tanımlanan veri kategorileri, haberleşmenin gerçekleştiği tarihten itibaren işletmeciler tarafından bir yıl süre ile saklanır.

(2) Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler, ilgili süreç tamamlanıncaya kadar saklanır.

Verilerin 1 yıl süreyle saklanacak olması Adalet Sistemindeki yoğunluğun fazla olmasını da göz önünde bulundurarak az olduğu ifade edilmektedir. Ayrıca reklam/pazarlama amaçlı olarak kullanıcıların rızası olmaksızın haberleşme yapılmasının da optin optout kapsamına alınarak engellenebilir olması memnuniyet teşkil edecektir.

6. REGÜLASYON, REGÜLATÖR KURUM İHTİYACI

Regülasyon, yani düzenleme kavramına karşılık gelen kavram için farklı düzenleyici sistemlere ve ülkelere uygulanabilecek genel kabul görmüş tek bir tanım bulunmamakla beraber en çok kabul gören ifade şeklidir. En basit anlamıyla düzenleme, devletin temel kontrol aracını teşkil etmektedir.

Hukuk, siyaset, ekonomi, sosyal ve fen bilimler gibi farklı alanları esas alan regülasyonların günümüz teknolojiler arası yakınsama (convergence) yaklaşımlarıyla birlikte disiplinler arası oluşum eğilimleri de gözlenmektedir.
Bu olgu regülasyon sözcüğünün kavramsal olarak net bir disipliner alan şekilde tanımlanmasını zorlaştırmaktadır. Zorluk, bir kuralı yeniden belirlemekten ziyade kuralların denetlenmesini ve doğru kurallar ile oyunun sürmesini sağlamak durumundan kaynaklanmaktadır. GSM sektörü düzenleyici kurumu BTK, kurum yapısı incelendiğinde denetleme ve düzenleme fonksiyonları gözümüze çarpmaktadır.

Düzenlemelerin, düzenleyici yetkisi devlet tarafından verilmiş olan kurumlar, sivil ya da devlet kurumları olarak belirtilmektedir. Düzenlemeler Ekonomik, Sosyal ve İdari Düzenlemeler şeklinde değerlendirilebilmektedir.

Ekonomik Düzenlemeler; başlıca pazara giriş, fiyatlandırma, pazardan çıkış ve rekabet gibi piyasa koşullarına dolaylı veya doğrudan yapılan faaliyetlerdir.
Ekonomik düzenlemeler piyasa oyuncuları arasında yeterli rekabet oluşmasını sağlayarak piyasaları aboneler için uygun ve kaliteli hale getirerek etkin kılma amacı taşımaktır.
Etkinliği artırmak isteyen başta ENISA, FCC ulaşım, iletişim ve haberleşme alanlarında bir yakınsama stratejisi belirleyerek telekomünikasyon, tren yolu, elektrik, su ve gaz gibi temel endüstrilerin bütünleşmesi modeli uygulanmasını başlatmışlardır.

Ülkemizde henüz bu yönde bir bütünleşme yaşanmamış olup, geçtiğimiz yıllarda number portability (numara taşıma) kararı ile bu rekabete büyük katkı sağlayan BTK, kullanıcılar yararına rekabetin önünü bu kararı ile hayli açmıştır.

Bütünleşme modeli geniş anlamıyla kişi haklarının korunmasına ve toplum refahının artırılmasına yönelik düzenleme faaliyetleri olmak üzere planlanarak çevre, güvenlik, sağlık gibi konulara hızlı çözümler üretme sosyal yaklaşımlarını taşıyarak sosyal düzenlemenin gerekçelerini oluşturmaktadır.
Devlet denetimi olmaksızın faaliyet gösteren firmaların kendi faaliyetlerinden doğabilecek sosyal sıkıntıların ve kar güdüsü ile hareket edecek olası olumsuz etkilerinin önüne geçilmek istenmesidir.

Sosyal ve ekonomik düzenlemelerin uygulanabilirliğinin kanunlar nezdinde koruma altına alınmak istenmesi amacını taşıyan idari düzenlemeler, işleyişteki idari işlemlerin ne şekilde gerçekleşeceğine ve veri akışına ilişkin kurallar kapsamında barındırmakta, düzenlemekte ve denetlemektedir.

Devletin tekel olduğu dönemde, fiyatlar, ürünler, hizmetler yönünde Telekomünikasyon sektöründe doğrudan karar verici durumda bulunması ve ilgili kısıtlamaların, düzenlemelerin, devletin doğrudan yapabilmesi düzenlemeleri kolaylaştırmıştır. Ancak günümüzde sektörün farklı işletmeler halini alması düzenlemelerin yaygınlaşmasına ve önemine temel oluşturmuştur.
Bu durumun sağlanması için Regulatör Kurumda şu durumların,

- Düzenleyici kurumların idari acıdan bağımsız olmaları ve regülatör işlev görmeleri,
- Düzenleyici kurumların sektörel anlaşmazlıklara arabuluculuk yapmaları ve cezai yaptırım güçleri,
- Teknik uzmanlık gerektiren ve hassas verilerin, siyasi ve ticari beklentilerden soyutlanmış olarak tarafsız ve objektif şekilde denetlenmesi ve etkin müdahalede bulunulabilmesi,
- Doğal tekelliğin önüne geçilmesi,

gözetilmesi gerekmektedir.

Elektrik, Su, Telefon gibi şebeke niteliği gösteren hizmetlerin sunulduğu piyasalarda şebekenin kurulması için gereken yatırım maliyetinin çok yüksek olmasıyla bu tür bir piyasada birden fazla firmanın faaliyet göstermesi halinde, firmalar iflas ya da birleşme yoluna giderek abone çıkarlarına aksi fiyat politikaları belirleyebilecek olması,

- Telekomünikasyon hizmetlerinin etkin bir şekilde sunulması, hizmet kalitesinin arttırılması,
- Rekabetçi pazarların bulunmadığı ya da başarısız olduğu durumlarda, hakim konumdaki şirketlerin aşırı fiyatlandırma yapmak, rekabet karşıtı davranışlar sergilemek gibi piyasa gücünü kötüye kullandığı durumlara engel olunması, hizmetlerin geliştirilmesi ve etkin fiyatların oluşturulması amacıyla rekabetçi pazarların gelişmesine yardım edilmesi,
- Düzenleme ve lisanslama süreçlerinde şeffaflığın sağlanması ile telekomünikasyon piyasalarına kamunun güven duymasının sağlanması, yatırımı teşvik eden uygun bir ortam yaratılması,
- Tüm kullanıcıların telekomünikasyon hizmetlerine erişiminin sağlanması ve haberleşme özgürlüğü-gizliliği ilkelerine uygun kişisel verilerin gizliliği haklarının korunması,

Regülatör Kurumların var olma nedenlerini açıklamaktadır.

Kurumların kurulma nedenleri ülkelerce benzerlikler gösterse de, bağımsızlık derecesi ülkelere kurumlar için belirlenen tasarımlara göre değişkenlik göstermektedir. Ancak bu değişkenlik yakınsama kavramının merkezileşmesiyle birlikte Regülatör Kurumlar içinde farklı uygulamalar ihtiyaçlarını beraberinde getirmektedir.

Yakınsama, yönetim ve maliyetler açısından bazı durumlarda dezavantaj ve avantajları birlikte barındırmaktadır. Yayıncılık, ses ve veri olarak üçlü hizmet

sunmak isteyen bir kablo TV işletmecisinin tek bir genel lisans alması yerine her bir hizmet için ek üç farklı lisans almak zorunda kalmak zorunda olması maliyetler dengesi anlamında olumsuz bir örnek teşkil etmektedir. Bu durumun abonelere yansımaması ihtimal dışı bir durumdur. Ancak yakınsamanın şebekeler ara bağlantı rejimi oluşturmasıyla, bir işletmeci sahip olduğu şebekeden bağımsız olarak diğer işletmeciler ile ara bağlantı yapmaktadır, oluşan rekabet ile abonelerin daha düşük maliyetler ile kullanımının önü açılmaktadır.
VOIP (Voice Over Internet Protocol), internet ve telefon sistemlerinin birleştiği sistem ve Internet protokolü üzerinden televizyon (IPTV) yakınsama hizmetleri olarak değerlendirilmektedir.
Her iki yakınsama örneği de Ses ve Televizyon hizmetinin IP altyapısı kullanılarak internet şebeke altyapısı üzerinden iletilmesidir.

Yakınsayan pazarların düzenlenmesi farklı regülatör kurumlar tarafından yapılabileceği gibi farklı kurumların birleştirilmesi ve merkezi bir regülatör kurum ile de mümkündür.
Yakınsayan pazarların düzenlenmesi için farklı kurumların birleştirilmesinin bazı avantajları Uluslararası toplantılarda temsilin ve katılımının sürekliliğin sağlanması, farklı sektörler hakkında geniş bilgi sahibi olunmasının düzenlemelerde etkinliğin artırılması olarak ifade edilebilmektedir.
Ülkemizde bu merkezileşmeden bahsedememekte olmakla beraber çok sektörlü kurumlar *(multisector regulators)* ABD'de mevcut ve eyaletler seviyesinde ulaştırma, alt yapı ve enerji gibi birkaç sektörde aynı anda sorumludur. Yakınsamış regülatör kurumların *(converged regulators)* ve çok sektörlü kurumların kurulma gerekçeleri farklıdır. Yakınsamış Regülatör kurumlar, tüm IT sektörlerinde bir birliktelik hali olduğu düşüncesiyle kurulmaktadır.

GSM Sektöründe Kişisel Verilerin Korunması ile ilgili izlenmesi gereken yol ülkemiz için mevcut ülke otoriteleri de incelendiğinde fonksiyonlarına göre ombudsman ve regülasyon olmak üzere iki ana alanda karşılaştırılabilmektedir.

Ancak bu çalışma kapsamında Türkiye'de düzenleme regülasyon kavramı üzerinden ilerlendiği için ombudsmanlık üzerinde durulmamaktadır.
Regülasyon yaklaşımı uygulanan AB üye ülkeleri, ilgili direktiflerin ihlaline yönelik bir şikayetle karşılaşıldığında, düzenleyici kurum sadece ihlali gerçekleşen durum ve işletmeciye yönelik durumun düzeltilmesine gitmeyerek benzer vakalarda farklı kararlar verilmesinin önüne geçilmektedir.
Regülatör kurumun, işletmecilerden kanuna uygun hareket edilmesini sağlayıcı önlemler almalarını istemekle birlikte denetimini yapma yetkisinin bulunması, Kişisel Veri Koruma hukuku alanındaki uygulamaların işletmeciler tarafından netlik kazanmasına destek olmaktadır.

Türkiye'de telekomünikasyon sektörü dışında kalan Medya, Finans, Teknoloji gibi birbirine yakınsamış olan alanlarda Kişisel Veri Korumasının ve Gizliliğinin sağlanması yerleşik ve kabul edilmiş olan Merkezi bir Regülatör Kurumun bulunmasıyla yakından ilgi teşkil etmektedir. Veri koruma alanında gerekli olan bağımsızlığın ve sektörler arası iletişimin sağlanması ENISA – FCC benzeri bir regülatör yapının tesisinin sağlanmasıyla uygun olacaktır.
Kurulacak olan yapının düzenleyici olması önerisinin değerlendirilmesinden sonra, yetkinin verildiği kişi ya da gruba göre, bu yapı için neden "Kurul" yapısının önerildiği konusunda değerlendirmelere geçilmesinde yarar görülmektedir.

a) Kişisel Veri Gizliliğinin sektörler arası uygulanması açısından veri işleme operasyonlarının hukuka uygun olarak gerçekleştirilmesi şartlarının düzenlemesi ve denetlenmesi,
b) Kişilik hakları ve Gizliliğinin ihlal edildiği farklı sektörler için farklı başvuralar gerekmeksizin ilgili otorite tarafından konunun değerlendirilebilmesi ve tüm sektörler için görüş ve önerilerin yaptırıma dönüştürülmesi,
c) Sektörler bakımından olası ihmal durumlarında telafisiz bir zararın önüne geçmek ve olası zarar/kriz durumlarında geçici ve acil önlemlerin hızlıca alınabilmesi ve sektörler arası koordinasyonun sağlanması,

d) Kişisel verilerin işlenmesine ilişkin konularda düzenleyici işlemler tesis etmek, bu konuda hazırlanan düzenleme taslaklarına görüş vermek, vatandaşları bilinçlendirici eylemler planlanması gibi konuların uygulanabilirliğinin artırılması BTK'nın Merkezi Regülatör Kurum haline getirilmesiyle mümkün kılınabilmektedir.

Bir diğer bakış açışıyla dezavantajlı durumlar yaşamanın önüne geçmek için sektörel regülasyonların birleştirilmesi nedeniyle daha genel ve etkisi zayıf regülasyonlardan kaçınılması ve regülatör kurumun birden fazla bakanlık ve kurum nezdinde bürokratik ilişki içinde bağımsızlığını kaybedecek bir ilişki içinde bulunmaması durumları gözden kaçırılmamalıdır.

Aksi durumlarda düzenleyici kurumların yakınsama nedeniyle merkezileştirilmesiyle, beklenen kurumlar arası işbirliği, kaynakların paylaşılması ve ortak politika hedeflerinin belirlenmesi zafiyete uğramış olarak birleştirilmemesi yönünde güçlü bir direniş olacaktır.

7. ÖNERİLER

Veri koruma hukuku yatay bir düzenleme alanı olup, bu alandaki düzenlemelerin etkileri başta sağlık, sosyal güvenlik, bilişim, haberleşme, araştırma ve geliştirme sektörlerinde hissedilmektedir. Karşılaştırmalı hukuk ile de yoğun bağlantıları olan bu alanın yeni gelişmelere ve dolayısıyla bu gelişmeleri karşılayacak düzenlemelere açık olması için Türkiye'deki veri koruma düzenlemelerinin diğer hukuk sistemleriyle çatışmayacak ve kendi içinde gri alanlarıyla birlikte ele alınması gerekmektedir. Verilerin KVKK ile birlikte değerlendirilmesi ve öncelikle kişilerin "kişisel verilerini koruma hakkı" olduğunun ve bu durumun her koşulda istenilebileceğinin belirtilmesi ifade edilmelidir. Bu belirleme kişilerin sahip oldukları hakların takibini kolaylaştıracaktır.

Mevzuatımızda kişilik hakkının korunmasına ilişkin hükümler Türk Medeni Kanununda yer almaktadır. Türk Medeni Kanunu'nun 24. maddesine göre hukuka aykırı olarak kişilik hakkına saldırılan kimse, saldırıda bulunanlara karşı korunmasını isteyebilir.

Tasarıda bu durum şu şekilde ifade edilmektedir: Ayrıca Türk Ceza Kanunu'nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak kaydedilmesi üçüncü kişilere verilmesi, yayılması fiilleri yaptırım altına alınmış bulunmaktadır. Aynı şekilde, Türkiye'nin 1954 yılında onayladığı Avrupa İnsan Haklan sözleşmesinin 8. maddesinde, herkesin özel ve aile hayatına, meskenine ve muhaberatına saygı gösterilmesini isteme hakkı olduğu belirtilmiştir.

Temelde sektörde karmaşa yaratan başta kişisel veri kavramı olmak üzere, verilerin işlenmesi, maskelenerek anonim hale getirilmesi, saklanması gibi kavramların karışıklığa mahal vermeyecek şekilde tanımlanması gerekmektedir.

Unutulmamalıdır ki kişisel veriler ancak kanun nezdinde belirlenmiş haller içinde kamu yararının gözetilmesi, veri sahibinin yararı ve izni veya Kolluk Kuvvetleri'nin özel izinli halleri halinde herhangi üçüncü bir şahsın yararına

işlenebileceği vurgulanmalı ve ilgili işletmeci ve abonelere bu yönde bilgilendirmeler yapılması gerekmektedir.

Kişisel verilerin gizliliğinin sağlanmasını istemek bir haktır. Herkes bu haktan eşit bir biçimde yararlandırılmalı ve bu hakka karşı sürdürülebilecek aksi tutumlar ve hakkın koruması taleplerinin başta kamu kurum ve kuruluşları, sektörel meslek örgütleri, tarafından sürdürülebilirliği sağlamak önem teşkil etmektedir.

Tasarıda bu durum şu şekilde ifade edilmektedir: Ayrıca farklı sektörlerde yer alan mesleklerin, var olan mesleki davranış kurallarını kişisel verilerin korunması bakımından gerekli değişiklikleri getirmeleri ya da eğer henüz hiç düzenleme yapılmamışsa kişisel verilerin korunması bakımından mesleki davranış kurallarını belirlemeleri, sistemi bütünlüğü acısından önem taşıyacaktır. Ancak bu düzenlemeler yapılırken, tasarıda belirlenen ilkelerin dikkate alınması gerekmektedir.

Bu çalışmayı destekleyici kapsamda kişisel verilerin korunması, abone haklarını korumaya yönelik olarak denetim yapmak, ihlaller halinde şikayetleri almak ve karara bağlamak gerekmektedir. Bu sorumluluk GSM sektörü için BTK olarak adreslenmişse de yakınsamış sektörler arasında bir yetki zafiyetine mahal verilmesinin önüne geçilmesi gerekmektedir. Burada çok yakın zamanlara kadar kamuya açık olarak veri dosyalama sistemleri bulundurulması suretiyle basit bir internet araması yapıldığında personel sicil bilgilerine ulaşmak mümkündü. Bu parçalanmanın önüne geçebilmek için ülkede kişisel veri koruma konusunda düzenlemeler yapmak ve bu konuda düzenlenen taslaklara görüş vermek için uluslararası alanda gerekli işbirliği ve koordinasyon çalışmalarını yürütmek üzere bağımsız merkezi bir denetçi ve düzenleyici kurum kurulması ihtiyacı görülmektedir.

Tasarıda bu durum şu şekilde ifade edilmektedir: Tasarı hükümleri, kamu kurum ve kuruluşları tarafından, kendi sahalarında kişisel verilerin korunması ile ilgili ihtiyacın hemen tespit edilebilmesini sağlayacak şekilde hazırlanmıştır. Bu nedenle, örneğin sağlık alanında Sağlık Bakanlığı'nın, iletişim ve ulaşım alanında

Ulaştırma Bakanlığı'nın, turizm alanında Kültür ve Turizm Bakanlığı'nın, ekonomik hayatla ilgili Sanayi ve Ticaret Bakanlığı'nın, maliye ve vergi konulan ile ilgili olarak Maliye Bakanlığı'nın, yargı ile ilgili olarak Adalet Bakanlığı'nın, nüfus işlemleri ve kolluk faaliyetleri ile ilgili olarak İçişleri Bakanlığı'nın vakit kaybetmeden bu kanuna uygun mevzuatı hazırlamaları yararlı olacaktır.

Kurulacak olan Kurumun tasarıda belirtildiği gibi kişisel verinin silinmesi dışındaki tüm işlemlerde rızası alınmış olmalıdır. Kişinin hayati acil durumları dışında veriler kişinin rızası alınmaksızın da işlenebilir, ancak uygulamalarda görmekteyiz ki bir takım SMS (kısa mesaj) kampanyaları düzenlenerek bize daha iyi hizmet verebilmek adına hediye ses, data paketleri sunmak suretiyle abone rızası alınmaya çalışılmaktadır. Bu durum kişisel verilerin gizliliği ve rıza işlemini son derece basitleştirmektedir, özel hayatın gizliliğine ilişkin böylesi konularda reklam ve kampanya düzenlenebilme durumunun incelenmesi gerekmektedir.

Esasen veri işleme, kanundan kaynaklanan bir hakkın kullanılması veya görevin yerine getirilmesi ve rızası alınmış müşteriyle yapılmış olan sözleşmenin yerine getirilmesi olarak bilinmesi gerekmektedir.

Veri İşleme gerçekleştirilen hallerde rızası alınmış olsa dahi abonenin verilerinin özel hayatın gizliliğini tehlikeye düşürecek bir şekilde yetersiz teknik önlemler doğrultusunda, verilerin iletilme şekline ve iletildiği alıcıların durumlarına göre, kişisel veri işlemenin amaçları ve ihlal durumları hangi aracı organ (ajans, medya) tarafından faaliyette bulunabileceği ve dışında ki hallerde cezai durumları ve ifası açıkça belirtilerek, keyfi işlemelerin önüne geçilmesi gerekmektedir.

Kural olarak kişisel veriler üçüncü kişilere aktaramaz. Ancak bu kuralın istisnası maddede bentler halinde sayılmıştır. Birinci fıkranın (a) bendine göre, aktarma talebinde bulunan gerçek ve tüzel kişilerin belirli bir olayda kanundan doğan görevini yerine getirmesi için bu bilgiye ihtiyaç duyması halinde kişisel veriler, üçüncü kişiye aktarılabilecektir. (b) bendiyle hukuka uygunluk sebeplerinin varlığı halinde kişisel verilerin üçüncü kişiye aktarılabileceği düzenlenmiştir.

Maddenin üçüncü fıkrasında kamu kurum veya kuruluşlarının kamu yararı, sır saklama yükümlülüğü, ilgili kişinin meşru menfaati veya kişisel verilere ilişkin özel koruma kurallarının varlığından bahisle kişisel verilerin, üçüncü kişilere aktarılmasını reddetmesini, sınırlamasını veya şarta bağlamasını mümkün kılan bir düzenleme getirilmiştir.

Yine tasarıya göre veri kişisel veri toplanması ve işlenmesinin sınırlı olması ve ilkelere bağlılığı: Bu ilke ile kişisel verilerin toplanması ve işlenmesinin sınırları olması ve verilerin hukuka uygun, meşru yollarla ve mümkün olduğunca veri konusu kişinin bilgisi veya rızası ile elde edilmesinin gerekliliği vurgulanmıştır. Tasarı ile kişisel verilerin, toplanması ve işlenmesi konusunda belirtilen ilkelere uyulmuştur.

Kişisel veride kalite ilkesi: Bu ilke ile, kişisel verilerin işlenmesiyle ilgili gerekli nitelikler vurgulanmaktadır. Buna göre, kişisel verilerin güncel tutulması, tam ve doğru olması, kullanılacağı amaçla bağlantılı ve bu amacın gerekleriyle sınırlı olması şartlarına işaret edilmektedir. Tasarının kişisel verilerin işlenmesine ilişkin ilkelerin belirlendiği 5. maddesi kapsamlı düzenleme tarzı ile aranan şartlan karşılamıştır.

Kişisel veri toplama ve işlenmesinde amacın belirginliği ilkesi: Kişisel verilerin toplanmasından önce, bu verilerin toplanmasının amaçlarının belli olması, sonraki kullanımların da bu amaçlarla sınırlı tutulması gereğine değinilmektedir. Toplanma amacının değişebileceği her durumda da, söz konusu değişen amaçların aynı şekilde belirgin olması gerektiği belirtilmektedir.

Amaca uygun kullanım ilkesi: Yukarıda sözü geçen ilke ile doğrudan bağlantılı olan bu ilke gereğince; veri konusu kişinin rızası veya kanunun yetki verdiği haller hariç olmak üzere, kişisel verilerin toplandığı ve işlendiği amaçlar dışında kullanılmaması, elde edilebilir hale getirilmemesi veya açıklanmaması öngörülmektedir.

Kişisel verilerin korunması için gereken tedbirlerin alınması ilkesi: Bu ilke ile

kişisel verilerin, yetkisiz olarak erişilmesi, imhası, kullanılması, değiştirilmesi veya açıklanması ya da kaybolması gibi risklere karşı uygun güvenlik tedbirleriyle korunması gerektiğine dikkat çekilmektedir. Tasarının 15. maddesi ile kişisel verilerin işlenmesinin güvenliği bakımından tedbir alınması yükümlülüğü getirilmiştir.

Ayrıca, kişisel verilere bilimsel, tarihi, akademik, istatistik veya kamu araştırması gibi sebeplerle ihtiyaç duyuluyorsa kişisel veri işlemenin kişi hak ve özgürlüklerini ihlal etmediği varsayımıyla söz konusu bilgilendirmenin yapılmasına gerek olmayabilecektir. M.7 (ç) bendinde, vakıf, demek, sendika ve siyasi partiler gibi kamuya yararlı kurum ve kuruluşlar tarafından özel nitelikli kişisel verilerin işlenmesi düzenlenmektedir. Buna göre bu verilerin, ilgili kuruluşların kuruluş amaçlarına, tâbi oldukları mevzuata uygun, faaliyet alanlarıyla sınırlı ve üyelerine yönelik olarak işlenmesi, ilgili kişilerin rızası olmadan üçüncü kişilere açıklanmaması gerekmektedir.

Tedbirlerin alınması yükümlülüğü M.26 ile kişisel verileri kontrol edenleri denetlemek ve Kanunla verilen görevleri yapmak üzere Kişisel Verileri Koruma Kurulunun oluşturulması öngörülmektedir, şeklinde açıklanmaktadır. Avrupa Komisyonunun söz konusu 95/46/EC sayılı direktifinin 28. maddesinde de üye devletlerin, kişisel verilerin işlenmesine ilişkin ilkelerin uygulanmasını izlemek ve yönlendirmek üzere bir veya birkaç kamu kuruluşunu görevlendirmeleri gereğine işaret edilmiştir. Avrupa Birliği üyesi ülkelerin tümünün, bu alanda yasama veya yürütme organlarına karşı bağımsız bir şekilde görev yapacak kurullar oluşturduğu gözlenmiştir. Örneğin, Almanya'da, Federal Verileri Koruma Görevlisi (Bundesbeauftragter fur Datenschutz), Avusturya'da Verilerin Korunması Komisyonu (Kommission fur Datenschutz), İsveç'te Verileri Denetim Kurulu (Data Inspection Board), Fransa'da Enformatik ve Özgürlükler Mitli Komitesi (Commission Nationale de 1 'Informatique et des Libertés), İngiltere'de Veri Koruma Komisyonu (Data Protection Commissioner) gibi kuruluşlar, milli kanunlar ve sözleşmelerde yer alan verilerin korunması ilkelerinin uygulanmasını izleyen ve yönlendiren bağımsız kuruluşlardır.

Ülkeler bu şekilde öngörülen ilkeleri iç hukuklarında yaşama geçirmek üzere bu amaçla birer kurumsal yapı oluşturmuşlardır. Aynı şekilde bir yapılanma ve yapılanmaya destek veri kontrolörlüğü çalışmalarının bu kapsam değerlendirilmesi yerinde olacaktır. Rızası alınmış olsa dahi doğrudan kişisel verilerin işlenmek veya saklanmak üzere toplandığı durumlarda, m.11 de belirtildiği üzere bu toplamayla ilgili rızası alınan abonenin aydınlatılması yükümlülüğü bulunmaktadır. Bu yükümlülüğün ülkemizde işletmeciler tarafından ihlalini önlemek içinse kapsamlı bir loglama yapılması gerekmektedir.

Loglama kapsamında işletme yetkilisinin, veri toplama amacına uygun olarak davranması sağlanmalıdır. Abonelerin diledikleri durumlarda "aydınlatma yükümlülüğü" ile bu kapsamda inceleme yapabilmeleri gerekmektedir.

Bu kontrollerin aboneler tarafından da yapılabilmesinin önü açıldığında verinin hukuka uygun olarak işlendiğini, bu verilerin belirlenmiş ve hukuka uygun amaçlarla toplandığını, bu verilerin toplandıkları amacın dışında kullanılmadığını, verilerin işleme amacıyla uygun ve yeterli olduğunu, verilerin işlendikleri amaç sona erdikten sonra kişilerin kimliklerini tespite izin vermeyecek şekilde tutulduğunu temin etmek kolaylaşacaktır.

Kanunda ayrıca birçoğu hassas veri niteliğinde olan ırk, etnik köken, siyasi düşünce, dini ve felsefi inanç, ticaret birliği üyeliği, sağlık, genetik kod, cinsel hayat, kişi hakkında verilen mahkeme kararları gibi verilerin işlenmesi belirli istisnalar dışında yasaklanmalıdır. Kişinin yazılı rıza verdiği, veri öznesinin veya üçüncü kişinin hayati çıkarlarının söz konusu olduğu veya o kişinin fiziksel olarak ya da hukuken rızasını belirtebilecek durumda olmadığı durumlarda kişinin veli ya da vasisinin izni alınıncaya kadar bu verilerin işlenmesi hali istisna olarak kanunda sayılmalıdır.

İstisna olarak belirtilmesi gereken bir diğer durum ise kişisel veriler üzerinde devlet sırrı, milli savunma ve güvenlik, kamu düzeni, devletin ekonomik ve finansal faaliyetleri gibi konularda kamu kurum ve kuruluşlarının çalışma gösterebilecek olmasıdır. Ancak bu durumun kişisel verilerin yetkisiz olarak

açıklanması, kanuna aykırı olarak işlenmesi gibi risklere karşı işletmecinin gerekli teknik ve kurumsal tedbirleri almaya mecbur tutulmalıdır.

Kanunda yer alması gereken bir diğer önemli konu ise müeyyidelerdir. Bu müeyyideler, kişisel verilerin hukuka aykırı kullanımının etkisinin büyüklüğüne göre, idari para cezası ve hapis cezasını da mümkün kılan yargı müdahalesini harekete geçirecek araçlarla birlikte ele alınmalıdır. Bu çerçevede Türk Ceza Kanunu'nun ilgili maddelerine atıflar yapılarak bütünlük sağlanmalıdır. Cezaların miktarının tayininde ise kişi hak ve özgürlüğüne olan müdahale sonucunda elde edilen haksız menfaat ve hukuka aykırılığın niteliği dikkate alınarak caydırıcı nitelikte cezalara hükmedilmesi önem arz etmektedir. Bu kanun kapsamında işlenen suçların başlıcaları; amacın gerçekleşmesine hizmet etmenin üstünde bir oranda kişisel veri depolama, verileri yetkisiz kişi veya kişilerle paylaşma veya erişime acık hale getirme, kasıtlı olarak veya ihmal ile verilerin güvenliğini tehlikeye atma, verilere zarar verme, Kurum nezdinde tutulan sicile kayıt yaptırmamış olma, aydınlatma yükümlülüğünü ihlal olarak sayılabilir. Her bir durumda suçun yarattığı ekonomik değer ve ihlalin büyüklüğüne, bu suçların işlenmesinde işleyenin teknik bilgi ve birikimine, yetki ve suçun manevi unsuru olarak kastın var olup olmadığına göre uygun cezalar verilmelidir.[54]

Bu itibarla, tasarıya kamuya açık alanların video ile gözetlemesinin ne tür hallerde yapılacağı, kayıtların hangi amaçla ve ne sürede tutulacağı ve hangi araçlarla kişilere bilgi verileceğine ilişkin olarak ek yapılması uygun olacaktır.

[54] Civelek, D, S.180-185

8. SONUÇ

Değişen çevre koşulları mıdır yoksa stratejiler midir ? Bunlara yanıt vermenin etkin yolları etkin stratejiler midir ? 1900'lü klasik yıllarda bu soruyu sormak ve böyle bir sorunun sorulabileceğini düşünmek imkansızken, bugün Kişisel Verilerden ve Teknolojiden bahsetmekteyiz.

Kapitalizmin bir dalga olmadığı klasik dönemden, ne oldu da modern döneme gelindi ve iletişim yaşam tarzımız, verimlilik ölçülmek istenilen kriterlerimiz oldu da bunun adına "verimlilik devrimi" denilir oldu?

Drucker verimlilik devrimi dediği o günleri şöyle anlatıyor makalesinde: "bu devrim verimlilik temeline dayalı olarak büyük işletmelerin kurulduğu, bireysel başarının kutsandığı bir ortamı" yansıtmaktaydı.[55]

İkinci Dünya savaşı döneminde ortaya çıkan ihtiyaçlar hiyerarşisi; tarım ekonomisine dayalı toplumlarda hızla gelişen, geliştirilmek zorunda bırakılan bir endüstriyel ekonomiyi ve bilgi gücünü meydana çıkarttı. Verimlilik önemliydi savaş yıllarında, halkın ekonomik buhranlar içerisinde bulunduğu dönemde 1 topu 3 ustanın değil seri olarak 1 makinenin üretebildiği sistemlere ihtiyaç vardı. Bu dönemde ayakta kalmaya çalışan firmalar varlık nedenini sorgulayan işlem maliyetleri kuramıyla tanışmış oldular.[56]

Kurumlar, kuramlar neticesinde birleşerek, bileşke üretimi ve toplu üretimde birim maliyetlerin düşürülmesine dayalı bir ekonomiyi benimseme yoluna gitmeye çalıştılar, ne yapıldıysa talep karşısında arz bir türlü karşılanamıyordu. Yapan ekonomilerin verileri, üretim modelleri illegal yollardan kopyalanmaya başlanmıştı. İnsanlar araba almak için aylar öncesinden sıraya giriyor, ücret ödeyip kuyrukta bekliyorlardı. Çevredeki zenginler bu şekilde çok kolay ayırt edilerek hırsızlık vakalarında açık hedef haline geliyorlardı. Nedenlerini

[55] Drucker, 1993
[56] Coase, 1939

incelediğimizde ise karşımıza iletişim yetersizliği ve ticari pazar ayrılıkları çıkıyordu.

Bilgi ekonomileri doğdu, veriler işlendi, üretim teknoloji koordinasyonu sağlandı, iletişim maliyetleri ucuzladı, pazarlar yaklaştı ve iştirakler doğmaya başladı. Parasal maliyeti düşük, istikrarı yüksek dayanıklı ürünler rekabeti doğurdu. Kurumlar pazarlamanın ve iletişimin önemi arttı: "Vizyon; fırtınalı bir denizde ihtiyaç duyulan bir pusuladır, gelişmeleri dikkate alamayarak uyum gösteremez ve topallarsa değerini pusula gibi kaybeder." diyor Peters.[57] Günümüzde uydu haberleşmenin olduğu bir dönemde pusulanın bir değeri var mıdır? Yüksek kapasitede hizmet vermek için kurulan çağrı merkezleri sadece müşteri memnuniyetini sağlamak içindir. Bürokrasinin ortadan kaldırılmaya çalışılması ve yönetim süreçlerinde yöneticiler ve üst yönetim arasında kademelerin kaldırılması, ARGE öneminin anlaşılmasıyla inovasyon çemberi dalgası şu anı özetlemektedir.

Türkiye'nin politikalarına da yansıtmış olduğu inovasyon olma vizyonu çerçevesinde, e-dönüşüm ve e-devlet alanında yürütülen çalışmalar bulunmaktadır.

Bu kapsamda kişisel verilerin hukuki korumasının sağlanmamış olması, bu girişimlerin güvenilirliği için elzemdir.

Küresel tehdit haline gelen terör saldırılarından koruduğu gibi siber saldırılara karşıda vatandaşlarını ve özel hayatlarını hiçbir insiyatife bırakılmaksızın farklı uygulamaların doğmasına sebep vermeden korunması gerekmektedir. Böylesi durumların önüne geçebilmek ekonomik ve sosyal kayıpların yaşanması bertaraf edecektir.

Ülkemizde kişisel verilerin korunması konusunda farkındalığın düşük olması, birtakım veri ve iletişim bazlı özel sektör çalışanlarında kuşku uyandırmaktadır.

---

[57] Peters, T, Search For Excellenge

Bu endişenin temelinde gelir kaybı ve denetimlerin artacak olmasının işletmeciler tarafında oluşturacağı kuşku yanı sıra denetimlerin kamu kurulumları tarafından yapılacak olmasının ise kişilerde bir gün fişlenme skandalıyla karşılaşabilme huzursuzluğu bulunmaktadır.

Bu iddiaları, AB Direktifleri kapsamıyla uyumlu olarak çalışılan Veri Koruma Kanunu ve Telekomünikasyon Sektörü Elektronik Haberleşme Yönetmeliği çürütmektedir.

Kişisel verilerin korunması yaklaşımının son yıllarda daha etkin bir şekilde ortaya çıkışına rağmen söz konusu yanlış anlamanın sebebinin, geçmiş projelerde bu alanların gündeme gelmeyişinin ve bu konunun hukuk için yeni bir çalışma alanı olmasının meydana getirdiği sezgisel yaklaşımlar olarak değerlendirilebilir.

Son olarak, "Avrupa Konseyi'nin küresel ekonomik krizin etkilerini azaltmak, akılcı, sürdürülebilir ve kapsayıcı büyüme dinamiklerini harekete geçirmek üzere 17 Haziran 2010 tarihinde resmi olarak kabul ettiği "Avrupa 2020: Akılcı, Sürdürülebilir ve Kapsayıcı Büyüme Stratejisi"nin (kısaca Avrupa 2020) yedi temel ekseninden birisi de "Avrupa için Sayısal Gündem" olmuştur. Avrupa Komisyonu'nun 19 Mayıs 2010 tarih ve COM (2010) 245 sayılı Bildirisi ile ortaya koyduğu söz konusu Sayısal Gündem, Avrupa'nın ekonomik büyümesinde sayısal ortamdaki "Güven ve Güvenlik" konusuna özel bir önem vermektedir. Bu çerçevede geliştirilen eylemler ile AB, 2020 yılına kadar, özellikle elektronik ortamda gerçekleştirilen iş ve işlemlerde kotu niyetli yazılımlar, siber saldırılar ve diğer tehlikeler karşısında kişisel verilerinin çalınması ve kötüye kullanılmasının önlenmesi konusunda veri koruma düzenlemelerini kişiler lehine güçlendirmeyi hedeflemektedir."[58]

Avrupalı'nın, AB'yi oluşturma mantığına bakıldığında güven tanzim eden bir ortam ticari birliktelik kurmak ve bu ortamın devamı bilinciyle Kişisel Veri Koruması düzenlemelerinin ülkemiz içinde ihtiyaç olduğu görülmektedir.

---

[58] Civelek, D