SEÇİLMİŞ ÜLKELERLE KARŞILAŞTIRMALI
OLARAK TEKNOLOJİ YOĞUN İŞYERLERİNDE
UYGULANAN SİBER GÖZETİMİN HUKUKSAL BOYUTU

Yüksek Lisans Tezi

Ayça DENİZ

Eskişehir, 2019

SEÇİLMİŞ ÜLKELERLE KARŞILAŞTIRMALI OLARAK TEKNOLOJİ YOĞUN İŞYERLERİNDE UYGULANAN SİBER GÖZETİMİN HUKUKSAL BOYUTU

Ayça DENİZ

YÜKSEK LİSANS TEZİ
Çalışma Ekonomisi ve Endüstri İlişkileri Anabilim Dalı
Danışman: Doç. Dr. Fatma KOCABAŞ

Eskişehir
Anadolu Üniversitesi
Sosyal Bilimleri Enstitüsü
Temmuz, 2019

JÜRİ VE ENSTİTÜ ONAYI

Ayça DENİZ'e "Seçilmiş Ülkelerle Karşılaştırmalı Olarak Teknoloji Yoğun İşyerlerinde Uygulanan Siber Gözetimin Hukuksal Boyutu" başlıklı tezi **29 Temmuz 2019** tarihinde, aşağıdaki jüri tarafından Lisansüstü Eğitim Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca toplanan **Çalışma Ekonomisi Endüstri İlişkileri** Anabilim Dalında, **yüksek lisans tezi** olarak değerlendirilerek kabul edilmiştir.

İmza

Üye (Tez Danışmanı) : **Doç.Dr.Fatma KOCABAŞ**

Üye : **Prof.Dr.Verda CANBEY ÖZGÜLER**

Üye : **Dr.Öğr.Üyesi Barış ÖZTUNA**

Prof.Dr.Bülent GÜNSOY
Anadolu Üniversitesi
Sosyal Bilimler Enstitüsü Müdürü

ÖZET

SEÇİLMİŞ ÜLKELERLE KARŞILAŞTIRMALI OLARAK TEKNOLOJİ YOĞUN İŞYERLERİNDE UYGULANAN SİBER GÖZETİMİN HUKUKSAL BOYUTU

Ayça DENİZ
Çalışma Ekonomisi ve Endüstri İlişkileri Anabilim Dalı
Anadolu Üniversitesi, Sosyal Bilimleri Enstitüsü, Temmuz 2019

Danışman: Doç. Dr. Fatma KOCABAŞ

Gözetim kavramı, tarih boyunca en eski çağlardan günümüze kadar olan süreçte her zaman insan hayatının bir parçası olarak var olmuştur. Ancak teknolojide her geçen gün meydana gelen gelişmelerle birlikte gözetim mekanizmasında da değişme ve gelişmeler meydana gelmiştir. Günlük hayatta var olan gözetleme faaliyeti, çalışma hayatına da girerek yerini elektronik araçlarla gerçekleştirilen siber gözetim faaliyetine bırakmıştır.

Çalışma hayatında birçok amaçla işverenler tarafından işçilere siber gözetim faaliyeti uygulanmaktadır. Siber gözetim faaliyetinin uygulanmasında işçinin kişisel verilerinin ve özel hayatın gizliliğinin korunması esastır. Bu bağlamda gerek uluslararası mevzuatta gerekse de ulusal mevzuatta işçilerin korunması amacıyla birtakım hukuki düzenlemeler yapılmıştır. Bu hukuki düzenlemeler ise, dağınık bir görünüm arz etmektedir. Bu çalışmanın amacı da dağınık bir görünüm arz eden uluslararası ve ulusal belgelerde bir bütünlük sağlamak ve ülke uygulamalarından yola çıkarak siber gözetim faaliyetiyle ilgili mevzuatında hükümler bulunan ülkelerin, bu konuda hüküm bulunmayan ülkelere mevzuatlarını düzenlemesi konusunda yol göstermesidir.

Anahtar Sözcükler: Gözetim, Siber Gözetim, Kişisel Veri, İşçi, İşveren.

ABSTRACT

LEGAL DIMENSION OF CYBER SURVEILLANCE APPLIED IN TECHNOLOGY INTENSIVE WORKPLACES COMPARED TO SELECTED COUNTRIES

Ayça DENİZ
Labour Economics and Industrial Relations Program
Anadolu University, Graduate School of Social Sciences, July 2019

Supervisor: Assoc. Prof. Fatma KOCABAŞ

The concept of surveillance has always existed throughout history from the oldest ages to the present in human life. However, with the developments in technology every passing day, the surveillance mechanism has also changed and improved. The classic surveillance mechanism that exists in daily life has been replaced by the concept of cyber-surveillance which is implemented by electronic devices.

Cyber surveillance is implemented by employers for many purposes in business life. In the implementation of the cyber surveillance activity, it is essential to protect the privacy of the employee's personal data and private life. International and national legislation on the protection of the privacy of the employee's personal data and private life, and in some countries' domestic legal systems, include a number of legal arrangements to protect both workers and employers. The aim of this study is to provide integrity in international and national documents, which are scattered, and to provide guidance for countries that do not have regulations on cyber surveillance activities based on country practices to regulate their legislation.

Keywords: Monitoring, Cyber-Surveillance, Personal Data, Employee, Employer.

TEŞEKKÜR

Bu tez çalışmasının her aşamasında bana olan desteğini esirgemeyerek tezin bugünkü şeklini almasında çok büyük katkısı olan, bilgileri ve deneyimleriyle akademik hayatıma ışık tutarak ilerlememi sağlayan Sayın Doç. Dr. Fatma KOCABAŞ'a,

Tez çalışmamın değerlendirilmesinde jüri üyesi olarak yer alan ve aynı zamanda önerileri ve destekleriyle bana yardımcı olan Sayın Prof. Dr. Verda CANBEY-ÖZGÜLER'e,

Karşılaştığım her engelde elimden tutarak bana destek olan, bütün olumsuzluklara karşı beni koruyan, her zaman en iyisini yapabileceğimi bana hatırlatarak moralimi yükselten en kıymetli varlığım annem Serpil ALBENLİ'ye,

Bana doğduğum günden beri kol kanat gererek etrafımda olan bitenlerden etkilenmemem için elinden geleni yapan, mantıklı ve olgun bir birey olarak ayaklarımın yere sağlam basmasında en büyük katkısı olan, içimde ona duyduğun özlem asla bitmeyen canım anneannem Sabiha ALBENLİ'ye,

Benim için her türlü fedakarlığı yapan, kendi çocuklarından ayırmayan ve en güzel günlerimden en zor günlerime kadar daima desteklerini esirgemeyen dayılarım Selçuk ALBENLİ'YE, Sezen ALBENLİ'ye, Sezgin ALBENLİ'ye ve Saner ALBENLİ'ye,

Beni öz yeğenlerinden ayırmayan, her problemimde elimden tutarak yol gösteren benim için birer yenge olmaktan çok öz teyzelerim olan Sibel ALBENLİ ve Sevim ALBENLİ'ye,

İlkokuldan bu yana birlikte büyüdüğüm, ağladığımda moral veren mutlu zamanlarımda birlikte kahkaha attığım, okul hayatım boyunca en ufak bir sorunda karşılıksız destek olan, yardıma ihtiyacım olduğunda elinden geleni yapan, bu zorlu tez döneminde bana hem psikolojik açıdan hem de teknik açıdan devamlı olarak moral vererek hiçbir zaman yalnız olmadığımı hissettiren, kız kardeşim Ayşenur ALTUNSOY'a,

Eskişehir'deki yıllarımı güzelleştirip keyifli hale getiren, duygularıma yenik düşüp mantıklı düşünmekten uzaklaştığımda soğukkanlılıkla bana destek olan, sadece başıma gelen iyi olaylarda değil en karamsar olduğum zamanlarda bile yanımdan ayrılmayan, pes etmeye en yakın hissettiğim anlarda moralimi yükselten ve tez

yazdığım süre boyunca ihtiyacım olan her konuda bıkmadan usanmadan beni bilgilendiren kız kardeşim Kübra SARPER'e ve

Son olarak bu zorlu süreçte benim nazımı, değişken ruh halimi, stresimi çekerek asla elimi bırakmayan, umutsuzluğa kapıldığım zamanlarda bana olan inancını ve desteğini koşulsuz göstermiş olan, ne zaman ihtiyacım olsa yardımıma tereddütsüz koşan çok kıymetli biricik sevgilim Ozan Can YÜKSEL'e

en içten teşekkür ve sevgilerimi sunarım.

Ayça DENİZ

Temmuz, 2019

.../.../2019

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Anadolu Üniversitesi tarafından kullanılan "bilimsel intihal tespit programı"yla tarandığını ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

Ayça DENİZ

vii

İÇİNDEKİLER

Sayfa

BAŞLIK SAYFASI i

JÜRİ VE ENSTİTÜ ONAYI..... ii

ÖZET iii

ABSTRACT iv

TEŞEKKÜR..... v

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ vii

İÇİNDEKİLER..... viii

SİMGELER VE KISALTMALAR DİZİNİ xi

GİRİŞ ……. 1

1. SİBER GÖZETİM KAVRAMINA GENEL BAKIŞ ……. 3

1.1. Gözetim ve Siber Gözetim Kavramı ……... 3

1.2. Siber Gözetim Kavramının Tarihsel Gelişimi ……... 7

1.2.1. Sanayi Devrimi Öncesi Dönem …….. 8

1.2.2. Sanayi Devrimi Sonrası Dönem ……. 11

1.2.2.1. *Panoptikon ve Büyük Kapatılma Dönemi* ……. 11

1.2.2.2. *Sanayi Devrimi'nden Günümüze Uzanan Dönem* …… 13

1.3. İşyerinde Kullanılan Siber Gözetim Aracı Türleri …… 16

1.3.1. Bilgisayar ……. 17

1.3.1.1. *Birinci Nesil Bilgisayarlar Dönemi* …… 17

1.3.1.2. *İkinci Nesil Bilgisayarlar Dönemi* …….. 22

1.3.1.3. *Üçüncü Nesil Bilgisayarlar Dönemi* …… 22

1.3.1.4. *Dördüncü Nesil Bilgisayarlar Dönemi* …… 23

1.3.1.5. *Beşinci Nesil Bilgisayarlar Dönemi* …… 24

1.3.2. İnternet ……... 26

1.3.3. Elektronik Posta (E-Posta) …… 30

1.3.4. Kamera …… 32

1.3.5. Telefon ……. 35

1.4. İşyerinde Yapılan Siber Gözetim Faaliyeti ……. 36

2. ULUSLARARASI BELGELER İLE KARŞILAŞTIRMALI HUKUKTA İŞYERİNDEKİ SİBER GÖZETİM MEKANİZMASINA YÖNELİK YASAL DÜZENLEMELER …… 44

2.1. Uluslararası Belgelerdeki Yasal Düzenlemeler …… 45

2.1.1. Ekonomik Kalkınma ve İş Birliği Örgütü (OECD) ……. 45

2.1.2. Birleşmiş Milletler (BM) …… 49

2.1.3. Uluslararası Çalışma Örgütü (ILO) …….. 53

2.1.4. Avrupa Konseyi …… 57

2.1.4.1. *Avrupa İnsan Hakları Sözleşmesi* …….. 57

2.1.4.2. *108 Sayılı Avrupa Konseyi Sözleşmesi* ……... 59

2.1.4.3. *185 Sayılı Siber Suçlar Sözleşmesi* …….. 63

2.1.5. Avrupa Birliği (AB) …….. 64

2.1.5.1. *Avrupa Birliği Temel Haklar Şartı* …….. 65

2.1.5.2. *95/46/EC Sayılı Direktif* ……... 66

2.1.5.3. *97/66/EC ve 2002/58/EC Sayılı Direktifler* ……... 68

2.1.5.4. *95/46/EC Sayılı Direktif'in Çalışma Grubu Kararları* …… 69

2.1.5.5. *2016/679 Sayılı Genel Veri Koruma Yönetmeliği* …… 75

2.2. Karşılaştırmalı Hukuktaki Yasal Düzenlemeler …… 76

2.2.1. Fransa …….. 77

2.2.2. Almanya ……... 81

2.2.3. İtalya ……. 85

2.2.4. Amerika Birleşik Devletleri (ABD) …… 87

2.2.5. İngiltere …… 92

3. TÜRK HUKUKUNDA İŞYERİNDEKİ SİBER GÖZETİM MEKANİZMASINA YÖNELİK YASAL DÜZENLEMELER …….. 98

3.1. 1982 Anayasası …… 98

3.2. 4721 Sayılı Türk Medeni Kanunu (TMK) …..……...……...…….. 101

3.3. 6098 Sayılı Türk Borçlar Kanunu (TBK)……..……...…….……. 103

3.4. 5237 Sayılı Türk Ceza Kanunu (TCK) ……..……...……..…… 106

3.5. 5271 Sayılı Ceza Muhakemesi Kanunu (CMK) …..…..……...…….…… 108

3.6. 4857 Sayılı İş Kanunu ……..…….... 111

3.7. 6331 Sayılı İş Sağlığı ve Güvenliği Kanunu (İSGK) …..……...…..... 116

3.8. 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) .....……. 117

SONUÇ ……..…….. 124

KAYNAKÇA……..... 127

ÖZGEÇMİŞ

SİMGELER VE KISALTMALAR DİZİNİ

AAET : Avrupa Atom Enerjisi Topluluğu
AB : Avrupa Birliği
ABC : Atanasoff-Berry Computer (Atanasoff-Berry Bilgisayarı)
ABD : Amerika Birleşik Devletleri
ADSL : Asymmetric Digital Subscriber Line (Asimetrik Sayısal Abone Hattı)
AET : Avrupa Ekonomik Topluluğu
AİHM : Avrupa İnsan Hakları Mahkemesi
AİHS : Avrupa İnsan Hakları Sözleşmesi
AK : Avrupa Konseyi
AKÇT : Avrupa Kömür ve Çelik Topluluğu
AMA : American Management Association (Amerikan Yönetim Örgütü)
ARPA : Advanced Research Projects Agency (Gelişmiş Araştırma Projeleri Dairesi)
ARPANET : The Advanced Research Projects Agency Network (Gelişmiş Araştırma Projeleri Dairesi Ağı)
AT : Avrupa Topluluğu
BfDI : Der Bundesbeauftragte für den Datenschutz und dieInformationsfreiheit (Federal Veri Koruma ve Bilgi Özgürlüğü Komisyonu)
BM : Birleşmiş Milletler
BTM : British Tabulating Machine Company (İngiliz Tablolama Makinesi Şirketi)
CCTV : Closed Circuit Television (Kapalı Devre Televizyon)
CERN : Conseil Européen pour la Recherche Nucléaire (Avrupa Nükleer Araştırma Merkezi)
CMK : Ceza Muhakemesi Kanunu
CNIL : Commission Nationale de L'informatique et des Libertés (Ulusal Bilgi İşlem ve Özgürlükler Komisyonu)
CPU : Central Processing Unit (Merkezi İşlem Birimi)
DEC : Digital Equipment Corporation (Dijital Ekipman Şirketi)
DNS : Domain Name System (Alan Adı Sistemi)

ECPA : The Electronic Communications Privacy Act (Elektronik Haberleşmenin Gizliliği Kanunu)

EDVAC : Electronic Discrete Variable Automatic Computer (Elektronik Ayrık Değişken Otomatik Hesaplayıcı)

ENIAC : Electronic Numerical Integrator and Computer (Elektronik Sayısal Entegreli Hesaplayıcı)

E-Mail : Electronic Mail

E-Posta : Elektronik Posta

EPİS : Elektronik Performans İzleme Sistemi

FTP : File Transfer Protocol (Dosya Transfer Protokolü)

FWA : Federal Wiretap Act (Telefon Konuşmalarının Gizlice Dinlenmesine Yönelik Federal Kanun)

GE : General Electric (Genel Elektrik)

HTML : Hyper Text Mark-up Language (Hiper Metin İşaretleme Dili)

IBM : International Business Machines (Uluslararası İş Makineleri)

ICO : Information Commissioner's Office (Bilgi Komiserliği Ofisi)

ILO : International Labour Organization (Uluslararası Çalışma Örgütü)

IP : Internet Protocol (İnternet Protokolü)

İK : İş Kanunu

İSGK : İş Sağlığı ve Güvenliği Kanunu

KVKK : Kişisel Verilerin Korunması Kanunu

LAN : Local Area Network (Yerel Alan Ağı)

m. : Madde

MGK : Milli Güvenlik Konseyi

MIME : Multipurpose Internet Mail Extensions (Çok Amaçlı İnternet Posta Uzantıları

ODTÜ : Orta Doğu Teknik Üniversitesi

OECD : Organisation for Economic Co-operation and Development (Ekonomik Kalkınma ve İş Birliği Örgütü)

OEEC : Organisation for European Economic Cooperation (Avrupa Ekonomik İş Birliği Örgütü)

NSA : National Security Agency (Ulusal Güvenlik Ajansı)

SLR : Single-Lens Reflex (Tek Mercek Yansıtma)

TÜBİTAK : Türkiye Bilim ve Teknik Araştırma Kurumu

TBK : Türk Borçlar Kanunu

TCK : Türk Ceza Kanunu

TDK : Türk Dil Kurumu

TMK : Türk Medeni Kanunu

ULAKBİM : Ulusal Akademik Ağ ve Bilgi Merkezi

ULAKNET : Ulusal Akademik Ağ

UNIVAC : Universal Automatic Computer (Evrensel Otomatik Hesaplayıcı)

WWW : World Wide Web (Dünya Çapında Ağ)

WAN : Wide Area Network (Geniş Alan Ağı)

GİRİŞ

İnsanlığın var olduğu en eski çağlardan günümüze kadar toplumsal düzen ile disiplinin sağlanması ve insanların korunması amacıyla gözetime başvurulmuştur. Teknolojik gelişmelerin yadsınamaz etkisiyle toplumlarda meydana gelen değişiklikler sonucunda hem gözetim faaliyetinin kendisi hem de gözetimin yapılmasını sağlayan araçlar değişmiş ve gelişmiştir. Sanayi Devrimi'nden günümüze kadar uzanan dönemde, teknolojik gelişmelerin ışığında işyerlerinde işin yapılması sırasında bilgisayar, telefon, kamera, ses kayıt cihazı ve cep telefonu gibi elektronik araçların kullanılması yaygınlaşmıştır. Dolayısıyla, işyerinde kullanılan bu elektronik cihazların aracılığıyla işverenlerin işçilerine yönelik siber gözetim faaliyetinde bulunmasının gerekliliği ortaya çıkmıştır. Bu bağlamda, çalışmanın temelini *siber gözetim* kavramı oluşturmaktadır.

Siber gözetim faaliyetinin içeriğini oluşturan işçinin kişisel verilerinin korunması ile özel hayatın gizliliğinin sağlanması hakkına ilişkin gerek uluslararası belgelerde gerekse ulusal belgelerde yer alan düzenlemeler dağınık bir görünüm arz etmektedir. Bu çalışmanın amacı da bu belgelerde bir bütünlük sağlamaktır.

Uluslararası ve ulusal mevzuatlar incelendiğinde işyerinde yapılan siber gözetim faaliyetine yönelik düzenlemeler yerine kişisel verilerin ve özel hayatın gizliliğinin korunması hakkında düzenlemelere ağırlık verildiği görülmektedir. Uluslararası düzenlemelerde işyerinde gerçekleştirilen siber gözetim faaliyetine yönelik olarak işçiyi ve işvereni koruyan hükümlere az şekilde yer verilmesi sebebiyle ülkelerin ulusal mevzuatlarında da bu alanda yapılan düzenleme sayısı benzer şekilde az sayıdadır. Oysa ki, çalışma hayatında hem işçilerin hem de işverenlerin haklarının korunması önemlidir. Çalışma hayatında işçinin siber gözetim faaliyetine karşı korunabilmesi için hem uluslararası hem de ulusal mevzuatta daha fazla düzenlemenin yapılarak bu konudaki eksikliklerin giderilmesinin gerekliliği bu çalışmada vurgulanmak istenmiştir.

Çalışma üç ana bölümden oluşmaktadır. Birinci bölümde bu çalışmanın temelini oluşturan gözetim ve siber gözetim kavramlarına değinilerek gözetim faaliyetinin tarih boyunca hangi evrelerden geçerek siber gözetim kavramına dönüştüğü tarihsel süreç içerisinde ele alınmıştır.

Çalışmanın ikinci bölümünde, siber gözetim faaliyetine yönelik uluslararası mevzuatta ve seçilmiş beş ülkenin mevzuatında yer alan yasal düzenlemelere değinilmiştir. Bu bağlamda uluslararası kuruluşlardan Ekonomik Kalkınma ve İş Birliği Örgütü (OECD), Birleşmiş Milletler (BM), Uluslararası Çalışma Örgütü (ILO), Avrupa

Konseyi (AK) ve Avrupa Birliği (AB)'nin yapmış olduğu siber gözetim faaliyetine yönelik düzenlemeleri ele alınmıştır.

Çalışmanın üçüncü bölümünde ise, ülkemizdeki yasal düzenlemelere değinilmiştir. Bu bağlamda, 1982 Anayasası, 4721 sayılı Türk Medeni Kanunu (TMK), 6098 sayılı Türk Borçlar Kanunu (TBK), 5237 sayılı Türk Ceza Kanunu (TCK), 5271 sayılı Ceza Muhakemesi Kanunu (CMK), 4857 sayılı İş Kanunu, 6331 sayılı İş Sağlığı ve Güvenliği Kanunu (İSGK) ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) çerçevesinde işyerinde yapılan siber gözetim faaliyetine yönelik düzenlemeler incelenmiştir.

1. SİBER GÖZETİM KAVRAMINA GENEL BAKIŞ

1.1. Gözetim ve Siber Gözetim Kavramı

Gözetim kavramının ortaya çıkışı insanlık tarihi kadar geçmişe dayanan bir olgudur. İnsanlar, çok eski dönemlerden bu yana hayatları boyunca çeşitli gözetim uygulamalarıyla karşılaşmıştır. Gözetim; kişilerin doğrudan doğruya izlenmesi ile davranışlarının, hareketlerinin, kurdukları cümlelerin izlenmesi gibi iki farklı şekilde ortaya çıkmaktadır. Literatüre bakıldığında *izleme (monitoring)* ve *gözetim (surveillance)* kavramlarının sıklıkla kullanıldığı görülmektedir. İzleme, "Bir işletme ya da kurumda özel bir amaç güdülmeksizin otomatik olarak bilgi edinme" faaliyetidir (İbiş ve Batman, 2014, s. 2). İzleme faaliyetine bir işletmede işverenin, işçisinin primlerini kayıt altına alması, yıllık izin sürelerini takip etmesi, örnek olarak gösterilebilir (Yılmaz, 2005, s. 3). Gözetim ise; "Bir kişinin bir başka kişinin davranışlarını kontrol etmesi eylemidir". Örneğin; işverenlerin, çalışma sırasında işçilerinin davranışlarını bilgisayar, kamera gibi çeşitli siber gözetim araçlarıyla takip etmeleri, gözetim kavramına örnek verilebilir (İbiş ve Batman, 2014, s. 2).

Literatür tarandığında hem izleme kavramının hem de gözetim kavramının birbiri yerine kullanıldığı görülmektedir. İzleme kavramı, yukarıda açıklandığı üzere, *kişilerden bilgi toplama faaliyeti* olarak özetlenmektedir. Günümüzde işverenler, işçilerinden yalnızca bilgi edinme amacıyla değil, aynı zamanda işçilerini kontrol altında tutma amacıyla da siber gözetime başvurmaktadır. Dolayısıyla gözetim kavramı, izleme kavramına nazaran daha geniş bir içeriği temsil etmektedir. Bu nedenle çalışmamızda, gözetim kavramına yer verilmiştir.

Gözetim kelimesinin İngilizce karşılığı olan *surveillance* kelimesi, aslında Fransızcadaki *surveiller* fiilinden gelmektedir. Surveiller, "Tehlikeli durumların önüne geçmek için dikkatli ve sürekli olarak izlemek" anlamına gelen bir fiildir ve bu fiilden gözetim kavramı türetilmiştir (Özger, 2016, s. 14). Aynı zamanda bu kelime, Latince *vigilare* kelimesiyle bağlantılı olarak; "Gözetleme kulesi ya da şehir duvarlarının dışında belirli olmayan veya tehdit edici nitelikteki bir şey" anlamını taşımaktadır (Marx, 2015, s. 734).

Gözetim kavramının hangi anlamlarda kullanıldığının anlaşılabilmesi için sözlüklere bakmak yerinde olacaktır. The Concise Oxford Sözlüğü'nde gözetim kelimesi; "Denetim, yakın gözetim ve çalışırken güvenilmeyen bireylerin gözetlenmesi" şeklinde yer almaktadır (Zureik, 2003, s. 37). The Shorter Oxford English Sözlüğü'ne

göre gözetim kavramının anlamı; "Şüphe edilen bir kişi ya da benzerine göz kulak olmak, izlemek" olarak verilmiştir (Weatherall ve Haskey, 1976, s. 39). Cambridge Sözlüğü de diğer sözlüklerle benzer bir biçimde gözetimi; "Bir yerin ya da bir kişinin, özellikle polis ya da askeri ordu tarafından, daha önce gerçekleşmiş ya da gerçekleşmesi muhtemel olan bir suç sebebiyle özenli bir biçimde izlenmesi" şeklinde tanımlamıştır (http-1).

Dünya literatürü tarandığında gözetim kavramının tanımlanmasının 1791 yılına dayandığı görülmektedir. İngiliz filozof ve hukukçu olan Jeremy Bentham yazdığı *Panoptikon* adlı kitabında gözetimi; "Şimdiye kadar örneği görülmemiş, zihin üzerinde zihinsel iktidar yaratan yeni bir yöntem" şeklinde tanımlamıştır (Mattelart, 2012, s. 13). Bentham'ın gözetim kavramını tanımlamasının akabinde, bu kavramdan etkilenerek çalışmalar yapan birçok kişi tarafından gözetimin yeniden anlamlandırılması gerekli görülmüştür. Bu bağlamda literatürde yer edinmiş diğer gözetim tanımlamalarına bakılması yerinde olacaktır.

Ball ve Webster (2003, s. 1) tarafından yapılmış tanıma göre; "Kişilerden elde edilen bilgilerin toplanması, saklanması, incelenmesi ve aktarımı" gözetim olarak adlandırılmaktadır. Gözetimin ilk ortaya çıktığı dönemlerde tehdit edici nitelikteki şeylerin gözetlenmesi söz konusuyken, günümüzde gözetim kavramının bu anlamından sıyrılıp derinleştiği görülmektedir. Gary T. Marx, gözetim kavramının sadece tehdit edici, şüpheli bireylerin gözetlenmesi anlamına gelecek şekilde kullanılamayacağını belirtmektedir. Marx'a göre; "Gözetim tek bir kişiye indirgenemez; belirli bir zaman dilimi, şebekeler, sistemler, belirli bir konum ve aynı zamanda kişiler de gözetlemeye maruz kalabilir". Böylece, yaşanılan dönemin koşulları değiştikçe gözetimin tanımı ve uygulanma biçiminde değişiklerin olması kabul edilebilir bir durum halini almıştır (Güven, 2012, s. 18-19).

Anthony Giddens (2000, s. 185) ise; gözetim kavramını açıklamada iki kavrama vurgu yapılmasını gerekli görmektedir. Bu kavramlardan birincisi; enformasyon birikimidir. Diğer bir ifadeyle, şifrelenmiş bilgilerin birikmesi gözetimi oluşturur. Gözetlenen kişiler, birer nesneymiş gibi kodlanırlar. Bu kişilerden sağlanan bilgiler aynı zamanda sınıflandırıldığı için de bu durum nitelikli bilgi depolama olarak açıklanabilir (Avcı, 2015, s. 254-255). Gözetim kavramını açıklamayla ilişkili diğer olgu ise; "Bir grubun mensubu olan alt kademedeki kişilerin, onlardan daha üst kademede bulunan kişiler tarafından denetlenmesidir" (Giddens, 2000, s.185). Demek oluyor ki iktidar,

gözetlemek istediği kişileri izler, kontrol eder ve denetler. Günümüzde gözetimin bu şekli hastane, hapishane, işyeri gibi alanlarda gerçekleştirilmektedir. Burada gözetimi yapan kişiler, güvenlikli bir toplum yaratma fikrini öne sürerek bu işlemi gerçekleştirirler (Avcı, 2015, s. 255). Sonuç itibarıyla, geniş bir çerçeveden bakıldığında Giddens'ın ilk tanımının depolayarak bilgi toplamaya dayalı gözetim, ikinci tanımının ise izlemeye dayalı gözetim olduğu ifade edilebilir. Değinilen bu iki olgu, birbiriyle ilişkilidir ve özellikle gözetim kavramının tanımını yapmak söz konusu olduğunda birbirinden ayrılamazlar. Günümüzde ise gözetim, her iki şekilde de hayatın olağan akışı içinde görülmektedir (Giddens, 2000, s. 185).

Yakın dönemde gözetimle ilgili yapılan çalışmalara bakıldığında, sosyolog David Lyon'ın gözetim kavramının tanımlanmasında literatüre büyük katkılar sağladığı görülmektedir. Lyon (2013, s. 31-32)'ın tanımına göre gözetim; "Sistemli ve düzenli bir biçimde yapılan bir faaliyettir. Bu faaliyet aracılığıyla kişilerden çeşitli bilgiler elde edilmektedir. Böylece, gözetimin önemli bir ayağını bireylerin oluşturduğu söylenebilmektedir. Söz konusu bireylerden kasti olarak bilgi toplanmaya çalışılır ve bu işlem belli teknikler ve kurallar çerçevesinde yapılır. Lyon'a göre gözetim; "Modern toplumların olağan bir parçasıdır ve onlar için artık bir hastalık şeklindedir".

Aynı zamanda Lyon, gözetimin iki türünün var olduğunu savunur. Bunlardan biri *koruma*, ikincisi de *kontroldür*. Örneğin; sokakta top oynayan çocuğu, karşılaşabileceği tehlikelerden uzak tutmak için gözetlemek *koruma* kavramını karşılamaktadır. *Kontrol* kavramı ise; çocuğun hareketlerini kısıtlamak, gözetim yoluyla onun davranışlarına müdahale etmek ve birtakım şeyleri yapmasını yasaklamak şeklinde ifade edilebilir. Dolayısıyla koruma kavramıyla kastedilen, çocuğu masumca korumak ve onun güvenliğini düşünmektir. Ancak kontrol kavramıyla açıklanmak istenen ise müdahale ve gözetim olgusudur (Çetin ve Asıl, 2017, s. 183).

Gözetim tanımlanırken bazı kriterlere dikkat edilmesi gerektiğini ise Brian Martin savunmaktadır. Gözetimi yapan kişi ile gözetime maruz kalan kişi arasında önemli ölçüde güç farkı olması birinci kriterdir. Örneğin; işveren ile işçi arasında böyle bir güç farkı bulunmaktadır. İkinci kriter; gözetim faaliyetinde bulunan ile gözetlenen kişi arasında güvensizlik oluşturacak bir olayın var olmasıdır. İşçinin, işyerinde daha önce hırsızlık vakasına karışması sebebiyle gözetime tabi tutulması buna örnektir. Sonuncu kriter ise hem güç farkının hem de güvensizliğin aynı anda mevcut olmasıdır. Brian Martin (1998, s. 64), bu kriterler sebebiyle yapılan izleme faaliyetine gözetim denmesi

gerektiğini düşünmektedir. Martin'in savunduğu düşünceye bakıldığında her izlemenin veya takip etmenin gözetim olarak adlandırılmaması gerektiği fikri ortaya çıkmaktadır. Bir kişinin izlenmesinin gözetim olarak düşünülebilmesi için gereken birinci kriter izleyen kişinin belli bir amaca sahip olmasıdır. Bu bağlamda güvenli bir ortam yaratabilmek, suçluları yakalamak, suçluların davranışlarını kontrol etmek veya iktidarın ortaya koyduğu kurallara halkın uyup uymadığını denetlemek gibi eylemler gözetimin amacı olarak kabul edilebilir. İkinci kritere göre; gözetim, günlük hayatla iç içe bir olgudur. Dolayısıyla gözetimi insanların günlük hayatından soyutlayarak düşünmek mümkün değildir (Çetin ve Asıl, 2017, s. 183). Sonuncu kriter ise, gözetimin, sistematik bir biçimde insan hayatında yer almasıdır. Sonuç itibarıyla, tüm bu kriterlerin mantıksal olarak bir araya getirilmesi ve programlanmasıyla gerçekleştirilen izlemelerle gözetim faaliyetine ulaşılmış olunmaktadır (Çetin ve Asıl, 2017, s. 183).

Literatürde mevcut olan tüm tanımların yanı sıra gözetime bir başka bakış açısı da William G. Staples'tan gelmektedir. Staples'a göre gözetim güç ilişkilerinden ibarettir. Güç ilişkileriyle kastedilen, gözetim faaliyetinin çok yönlü şekilde ve isteğe bağlı olarak gerçekleştirilebilir olmasıdır. Örneğin; bir trafik polisi, hız limitlerine uyup uymayan sürücüleri izlerken aynı zamanda kendisi de bir üst birim tarafından izlenebilmektedir (Güven, 2016, s. 16).

Gözetim kavramı tanımlanırken sıklıkla kullanılan ifade; "Şüphe duyulan kişinin kapalı gözetimi" şeklindedir. Ancak günümüzde hem gözetimin tanımı hem de gözetim araçları gelişerek teknoloji temelli hale gelmiştir. Bu nedenle günümüzde bu kavram sadece bir kişinin gözetim altında tutulması olarak sayılmamalıdır aynı zamanda kalabalık gruplara da uygulanabilen, zamana ve mekâna bağlı bir şekilde geliştirilen, insanların yanı sıra ağ sistemlerine de uyarlanabilen bir faaliyeti ifade etmektedir (Özçağlayan ve Çelik, 2014, s. 195).

Ülkemiz açısından bakıldığında Türk Dil Kurumu (TDK) Büyük Türkçe Sözlüğü incelendiğinde gözetim kavramının; "i. Gözetme işi, nezaret; ii. Himaye; iii. Gözaltı" olmak üzere üç farklı şekilde kullanımı söz konusudur (http-2). TDK'nin Yöntembilim Terimleri Sözlüğü'ne bakıldığında ise; "Bir çalışma ya da uygulama sürecini etkinlik ve amaca uygunluk bakımından yakından denetleme" şeklinde bir gözetim tanımıyla karşılaşılmaktadır (Sencer, 1981, s. 74). Anayasa Sözlüğü'ndeki gözetim kelimesinin karşılığı, TDK'nin Büyük Türkçe Sözlüğü'ndeki gözetim tanımıyla aynı şekilde; "Nezaret, himaye" olarak verilmiştir (Eren ve Zülfikar, 1985, s. 71). Yasa Dili

Sözlüğü'nde ise gözetimin; "Nezaret" kavramıyla örtüştüğü görülmektedir (Önder, 1966, s. 86). Bu tanımlardan farklı olarak, Sinema ve Televizyon Terimleri Sözlüğü'nün yaptığı tanıma göre gözetim; "Mesleğe yeni başlayan, yapımcının tam güvenini taşımayan ya da çok büyük bir yapıma girişen bir yönetmenin çalışmalarının güvenilir bir kimsece denetlenmesi" şeklinde ifade edilmiştir (Özön, 1981, s. 140). Bir başka gözetim kavramı tanımı da Ceza Yargılama Yöntemi Yasası Terimleri Sözlüğü'nde; "Küçüklerin, ana babalarınca korunması ve idarenin her türlü eylem ve işleminin de yargının denetimi altında olması durumu" olarak yapılmıştır (Erdoğdu, 1972'den aktaran Bölükbaş, 2014, s. 7).

Teknolojik gelişmeler ışığında ortaya çıkan siber gözetim Tremblay (2010, s. 1) tarafından; "İnternet ve bilgisayar gibi veri aktarımını gerçekleştirebilen araçlar ile çeşitli gözetim yazılımı programları kullanılarak yapılan izleme faaliyeti" olarak tanımlanmaktadır. Siber gözetim faaliyetinin uygulanmasında bilgisayar, internet, cep telefonu ve kamera gibi araçlar kullanılmaktadır. Bu araçlar yardımıyla kişilere ait bilgilerin toplanması, depolanması, analiz edilmesi ve raporlandırılması yoluyla siber gözetim faaliyeti uygulanmaktadır (Petersen, 2001, s. 17).

Günümüzde teknolojinin her geçen gün önlenemez yükselişiyle birlikte siber gözetimin uygulanması da giderek kolaylaşmaktadır. İçinde bulunduğumuz bilgi ve teknoloji çağında hem insanların özel alanlarında hem de kamusal alanlarda siber gözetim çeşitli araçlarla birlikte sıklıkla kullanılmakta ve bu durum toplumların her an gözetlenebilir olmasını mümkün kılmaktadır. Dolayısıyla siber gözetim kavramı, insan hayatından ayrı düşünülemeyecek bir olgu haline gelmiştir. Böylece kişilerin hareketleri tıpkı günlük hayat içerisinde olduğu gibi çalışma hayatında da anlık olarak, her zaman ve her yerden izlenebilir bir hal almıştır (D'Urso, 2006, s. 284; Bajc, 2007, s. 1578).

1.2. Siber Gözetim Kavramının Tarihsel Gelişimi

Gözetim kavramı, genellikle modern dönemlerde teknolojinin de gelişmesiyle hayatımıza girmiş gibi gözükse de aslında günümüzde ortaya çıkmış bir kavram değildir. İlk Çağ döneminde var olmuş toplumlardan itibaren günümüze kadar gelmiş tüm toplumlarda kabileler, imparatorluklar, monarşiler ya da devletler sahip oldukları egemenliği kaybetmemek ya da güçlendirmek adına gözetimi, toplumsal denetimi muhafaza etmeye yönelik bir araç olarak kullanmıştır (Dolgun, 2005b, s. 25).

Ancak Sanayi Devrimi sonrasında gözetim farklı bir boyutta karşımıza çıkmaktadır. Bu dönem itibarıyla iktidar, kuşku duyduğu bireyleri izleyerek denetim

altında tutabilmek için gözetime başvurmuştur. Gözetim, bu yönüyle günlük hayatın bir parçası halini almış ve dolayısıyla sadece devletin vatandaşlarını gözetlemesi değil, aynı zamanda işverenlerin de işçilerini gözetlemesi söz konusu olmuştur. Bu dönemin bir parçası haline gelen gözetim faaliyeti, halkın sosyal hayatta da denetime maruz kalmasını beraberinde getirmiştir (Dolgun, 2008, s. 17-22).

Günümüzde modernleşen bilgi toplumuna geçişle birlikte gözetim de enformatik boyuta geçmiş bulunmaktadır. Bu yönüyle gözetim, artık bireylerin hayatında kaçınılmaz bir şekilde var olmaya başlamış ve gündelik hayatın bir parçası haline gelmiştir. Teknolojinin gün geçtikçe gelişmesiyle hem gözetimin uygulanış biçimi hem de kullanılan araçlar farklılaşmaktadır (Dolgun, 2005b, s. 25).

Sonuç olarak, Sanayi Devrimi öncesinde yapılan gözetimlerde gücü elinde tutma, gruplara hükmetme ve askeri amaçlar ön plandadır. Sanayi Devrimi sonrasında, baskı kurularak yapılan gözetimin yerini birtakım modern yöntemler almıştır. Günümüz toplumlarında yer alan gözetimde ise, teknolojinin etkisi oldukça fazla şekilde hissedilmektedir. Ancak, en eski dönemlerden günümüze kadar geçen sürede değişmeyen tek şey, gözetim uygulamalarının birtakım kişiler, kurumlar ya da grupların amaçlarını gerçekleştirme doğrultusunda yapılmasıdır (Dolgun, 2005b, s. 25). Bu nedenle, günümüz bilgi toplumunda yoğun bir biçimde yer alan gözetimin, ne tür aşamalardan geçerek hayatımızın merkezine oturduğunu incelemek yerinde olacaktır.

1.2.1. Sanayi Devrimi Öncesi Dönem

Anthony Giddens'a göre gözetim hakkındaki ilk ibareler yazının bulunmasıyla eş zamanlı olarak karşımıza çıkar. M.Ö. 3200 yılında yazının bulunmasıyla birlikte devletler, vatandaşları hakkındaki çeşitli bilgileri toplamaya başlayarak kişileri ya da mekânları gözetlemekte ve böylece idari denetim gücünü artırmaktadır (Karahisar, 2011, s. 2). Aynı zamanda devletler, bu gözetimi yaptıkları sırada birtakım şifreleme tekniklerine de başvurmuşlardır. Devleti yöneten kişiler vatandaşlara ait bilgiler toplamakta, depolamakta ve bu bilgilerden meydana gelmiş birer liste hazırlamaktadırlar. Yazıyı keşfetmesiyle bilinen Sümer uygarlığında hükümdarlar ya da devlet adamları gün içinde yaşadıkları olayları yazmak suretiyle kaydetmekteydiler. Aynı şekilde, Babil İmparatorluğu'nun katiplerinin de devleti yakından ilgilendiren birçok olayı not ettiği bilinmektedir. Örneğin, imparatorlukların tahta çıktığı, öldüğü, savaşa girdiği ya da devlet içinde çıkan isyanların tarihleri, halkın geçirdiği açlık ve veba salgını gibi hastalıkların olduğu dönemler ve bunun gibi devleti yakından

ilgilendiren birçok mühim olayın katipler tarafından kayda geçirildiği bilinmektedir (Giddens, 1985, s. 45-46).

David Lyon'ın gözetim hakkındaki çalışmaları göz önüne alındığında, M.Ö. 3100'lü yıllarda var olan Antik Yunanistan ile M.Ö. 756 yılında kurulan Mısır uygarlığında gözetimin ilk örneklerine rastlandığı görülmektedir. Sümer ve Babil uygarlıklarında olduğu gibi bu uygarlıkları yönetenler de vatandaşlarının vergilerini ödeyip ödemediklerini, askerlik görevlerini ya da göç bilgilerini kontrol etmek amacıyla nüfus kayıtlarını toplamışlardır (Lyon, 1994, s. 22).

1450 yılına gelindiğinde, matbaa makinesinin icat edilmesi ve kullanılması da gözetimin gerçekleştirilmesinde rol oynayan önemli bir etken olmuştur. Böylece, iletişimin daha fazla teknolojik bir hal almasının ve devletlerin gözetim etkinliklerinde bulunabilmesinin önü açılmıştır (Giddens, 1985, s. 178-179). 1400'lü yıllarda halkın evlilik tarihleri, doğum yaptıkları günler, doğan bebeklerin vaftiz edilmesi ve ölüm tarihleri devlet tarafından kayıt altına alınmıştır (Güven, 2016, s. 175-176).

1600'lü yıllar itibarıyla geleneksel yöntemler kullanılarak yapılan gözetim, Staples'a göre iki temel özelliği içinde barındırır. Bunlardan birinci özellik; gözetimin sürekli tekrarlanarak kesintisiz bir şekilde yapılmasıdır. İkinci özellik ise; gözetimin insanların hayatında alışkanlıklar gibi bir sıradanlıkla yer almasıdır. İnsanların güven içinde, toplumun veyahut devletin kurallarını ihlal etmeden yaşayabilmesi bu dönemde uygulanan geleneksel gözetimin temel amacını oluşturmaktadır (Güven, 2016, s. 178).

On altıncı yüzyılın sonları ile on yedinci yüzyılın ilk yıllarında Fransa, Almanya ve İngiltere gibi ülkeler aylak gezen işsizleri ve isyan çıkartanları kontrol altında tutmak için kapatmaya başlamıştır. Hapishanede kapalı tutulmamak için halk, en kötü şartlarda ve en düşük maaşlı işleri bile kabul etmeye başlamıştır. Dolayısıyla kapitalizmin yayılması kolaylaşmıştır. 1789 yılında ise, hapishanede tutulan kişiler bir isyan çıkartarak hapishaneden çıkmıştır. Bu ayaklanma Fransız Devrimi'ni hızlandıran bir eylem olmuştur (Çakır, 2015, s.209).

Foucault'nun *Büyük Kapatılma* olarak ifade ettiği yeni gözetim sistemine göre, insanlar kapalı bir yerde ve belirli bir amaç doğrultusunda gözetlenmeye başlanmıştır. Tehlike yaratacak potansiyele sahip suçlular, akıl sağlığını yitirmiş kişiler, sarhoşlar, cüzzam ya da veba gibi hastalıkları taşıyanlar ve işsiz bir şekilde boş gezen kişiler gözetim faaliyetini yapmakla görevlendirilmiş kişiler tarafından denetlenmiştir (Çetin ve Asıl, 2017, s. 185).

On yedinci yüzyılın en temel gözetim faaliyetini niteleyen Büyük Kapatılma uygulamasını detaylandırmak, bu dönemi anlamlandırabilmek açısından yerinde olacaktır. Foucault'nun tanımladığı Büyük Kapatılma'nın 1600'lü yılların sonlarına doğru veba salgınının yayılmasıyla başladığı bilinmektedir. Büyük Kapatılma sırasında uygulanan gözetim faaliyetine Foucault (1995, s. 201-202) tarafından değinilmiştir. Buna göre; her şeyden önce, veba salgınının görüldüğü kasaba ve bu kasabanın yakınlarında bulunan yerleşim yerleri kapatılmıştır. Bu alanlarda başıboş şekilde gezen hayvanlar öldürülmüştür. Denetimi yapmakla görevlendirilmiş kişiler, kolaylık olması açısından, her bir kasabayı bölgelere ayırmıştır. Burada yaşayan kişilerin yalnızca belirli günlerde dışarı çıkabilme izni vardır. Bu günler dışında evden çıkarak kuralı ihlal eden kişiler ya veba salgınına yakalanmış ya da görevliler tarafından ölüme mahkûm edilmiştir. Üstelik bu denetim o kadar sıkı bir biçimde yapılmıştır ki; denetimi yapan görevliler, insanları evlerine kilitlemiş ve evlerin anahtarlarını da kendi amirlerine teslim etmiştir. Veba salgını geçene kadar da bu anahtarlar amirler tarafından saklanmıştır.

Büyük Kapatılma döneminde uygulanan gözetim, sürekli devam eden sistematik bir özelliğe sahiptir. Her şeyden önce insanların evlerine kapatılarak denetlenmesiyle devlete itaat etmeleri, devletin siyasi ve idari gücünün artması, toplum düzeninin daha iyi sağlanması ve hırsızlık eylemlerinin önüne geçilmesi sağlanmaya çalışılmıştır. Bu gözetimle birlikte sadece halk değil, aynı zamanda gözetimi gerçekleştirmesi için görevlendirilen kişiler de amirleri tarafından denetlenmektedir (Foucault, 1995, s. 202). Bütün bunlara ilave olarak gözetimle birlikte elde edilen bilgiler de kayıt altına alınmaktadır. Büyük Kapatılma öncesinde, bu şehirde yaşayan herkesin ad, soyad, yaş ve cinsiyet bilgileri toplanarak not edilmiş, vatandaşların hastalıkları, ortaya çıkan sorunlar ve ölümler gibi bilgiler de kaydedilerek üst amirlere ulaştırılmıştır (Foucault, 1995, s. 202).

Kapatılma işlemi hem hasta kişiler için hem de suçlular için yapılmaktadır. Hastane ve hapishane gibi kurumlarda amaç; hasta kişilerin iyileştirilmesi ya da suçluların terbiye edilmesi değildir. Her iki kurum da kişilerin bir an evvel üretim sisteminde yer almasını sağlama amacını gütmektedir. Foucault, hastaneler ile hapishanelerin ortak bir gözetim faaliyetine sahip olduğunu savunmaktadır (Baştürk, 2016, s. 43-44). 1600'lü yıllarda meydana gelen bu kapatılma uygulaması, o

dönemlerde henüz inşa edilmemiş hapishanelerin temelinin atılmasına öncülük etmiştir (Dolgun, 2005b, s. 55).

1.2.2. Sanayi Devrimi Sonrası Dönem

1.2.2.1. Panoptikon ve Büyük Kapatılma Dönemi

Günümüzde de geçerliliğini kaybetmeyerek gelişmeye devam eden gözetim uygulamaları, *Panoptikon Hapishane* tasarımı olarak Jeremy Bentham tarafından gündeme getirilmiştir (Dolgun, 2008, s. 106). Bu tasarımla kişilerin hem toplu bir biçimde hem de tek tek gözetlenebilmesi sağlanmaktadır. Modele adını veren Panoptikon da buradan gelmektedir. Kelime incelendiğinde *pan* bütün anlamına gelmekteyken, *opticon* ise gözetim anlamını taşımaktadır (Baştürk, 2016, s. 38).

Panoptikon sistemi üzerine araştırmalar yapıldığında, bu gözetim faaliyetinin asıl olarak Bentham'ın hayal gücünün bir ürünü olduğu görülmektedir. 1787 yılında Jeremy Bentham, bir arkadaşına yazdığı mektuplarla Panoptikon sisteminin şeklinin ve özelliklerinin tasvirini öyle güçlü bir biçimde yapmıştır ki, bu mimari yapının soyut bir hayal ürünü olduğuna inanmak zorlaşmıştır. Panoptikon sisteminde insanların denetlenmesinin yanı sıra, sorunlu kişilerin ıslah edilmesi de planlanmıştır. Bu sistemle birlikte toplumun refahının artması ve kişilerin yanlış davranışlarının ıslah edilerek eksikliklerinin giderilmesi hedef alınmıştır (Pease-Watkin, 2003, s. 1-2; Bentham vd., 2008, s. 12).

Panoptikon'un ne tür mimari özelliklerde inşa edilmesi gerektiğini Bentham, yazdığı mektuplarda açıkça anlatmıştır. Bu mektuplardan anlaşılacağı üzere Panoptikon Bentham tarafından, yarım daire biçiminde tasarlanmış bir hapishane olarak düşünülmüştür. Aşağıdan yukarıya doğru çıkan her bir katta, yan yana tek kişilik hücreler bulunmaktadır. Bu hücreler, mahkûmların birbirini duyamayacağı ve göremeyeceği şekilde yalıtılmıştır. Hücrelerin hepsini görebilecek şekilde, hapishanenin ortasında konumlandırılmış bir gözetim kulesi vardır. Bu kulede teftiş yapan bir kişi oturmaktadır. Ancak hücrelerdeki mahkûmlar denetimi yapan kişinin yüzünü hiçbir zaman görememektedir (Whitaker, 1999, s. 32-33).

Bentham, Panoptikon'un uygulanabileceği grupları; "İşçiler, deliler, tembeller, davranışlarından kuşku duyulan kimseler, hastalığı olanlar ve yanlış davranışlarının düzeltilmesi için gönüllü olan kişiler" olarak tanımlamıştır. Bu gruptaki insanların yanlış davranışlarının değiştirilmesi ve kendilerinin ıslah edilmesi için gözetimin şart olduğunu savunmuştur (Bentham vd., 2008, s. 12).

Başlangıçta fabrikada çalışan işçilerin denetlenmesi maksadıyla tasarlanan Panoptikon, Jeremy Bentham tarafından daha çok hapishane modeli olarak düşünülmüştür. Bentham bu modelin Londra'da hayata geçirilmesi için hükümete başvuru yapmıştır. Ancak bu öneri hükümet tarafından kısa bir süre sonra reddedilmiştir. Bu nedenle Bentham'ın Panoptikon'u, hayal dünyasında yer alan bir gözetim modeli olmaktan ileri gidememiştir (Pease-Watkin, 2003, s. 3; Werrett, 1999, s.3).

Bentham'ın tasarlamış olduğu Panoptikon ne Bentham'ın hayatı boyunca ne de daha sonrasında gerçekleşmemiştir (Whitaker, 1999, s. 33). Panoptikon tasarımı, toplumsal hayat içinde insanların kurallara uyarak itaatkâr bir biçimde yaşamasını amaç edinerek tasarlanmıştır. Kurallara uyup uymadığının kontrol edilebilmesi adına insanların adeta birer nesneymiş gibi izlenmesi, yönetilmesi gerekmektedir. Böylece kişiler hem topluma uygun davranışlar sergileyecek hem de üretim faaliyetlerinde yer alarak devlete yarar sağlayacaktır (Baştürk, 2016, s. 45). Bu mimari tasarım, Bentham'dan sonra birçok düşünürün gözetim hakkındaki fikirlerini geliştirmelerine öncülük etmiştir (Whitaker, 1999, s. 33).

20. yüzyılda yaşamış olan Foucault'nun gözetim bağlamındaki Büyük Kapatılma çalışmaları, 18. ve 19. yüzyılda yaşamış Jeremy Bentham'ın Panoptikon hapishane tasarımının bir parçası niteliğindedir (McGrath, 2004, s. 1). Foucault'nun esinlendiği Panoptikon tasarımı gözetim, denetim ve iyileştirme üzerine kurulmuştur. Panoptik sistemdeki kişiler gözetim altındadır. Böylece gözetim altındaki kişilerin her türlü davranışı denetlenebilmekte ve buna göre kişiler ödül ya da ceza alabilmektedir. Bu denetlemeyle beraber kişiler, topluma uygun davranmayı öğrenerek adeta tedavi edilmektedirler (Dolgun, 2008, s. 105).

Panoptikon tasarımı, Foucault tarafından başlarda hapishanelerde kullanılacak şekilde düşünülmüştür. Buna karşın daha sonraları yazdığı *Disiplin ve Ceza* adlı kitabında gözetimin sadece hapishanelerde değil okul, işyeri ve askeriye gibi insanları sınırlandıran mekânlarda da yoğun olarak ortaya çıktığını belirtmektedir (Whitaker, 1999, s. 36-37; Lyon, 2007, s. 59). Foucault'ya göre Panoptikon modelinin temel amacı, bu sistemle gözetlenen kişileri gözaltında tutmak, hücrelerde tek başına tutarak disipline etmek, aylak bir şekilde oturtmayarak çalışmalarını sağlamak ve onları eğitmektir. Panoptikon sisteminde suçlu olanlara ceza verilmekte, ruh sağlığı bozuk olanlar gözetlenmekte, kötü davranışları olanlar disipline edilmekte, işsiz gezenlere iş

verilmekte, hastalığı olanlar tedavi görmekte ve çalışmak için istekli olanlara fabrikalarda istihdam sağlanmaktadır (Bauman, 1997, s.20-21). Foucault'ya göre modern toplumların hepsi aslında birer disiplin toplumundan ibarettir. Başlangıçta hapishane, hastane ve fabrika gibi kurumlarda uygulanan gözetim, zamanla yerini insanların günlük hayatının izlenmesine bırakmıştır (Lyon, 1994, s. 26).

Panoptikon sistemi, olumlu ve olumsuz özellikleri bir arada barındırmaktadır. İnsanları kötü davranışlardan uzaklaştırarak disipline etme işlevi için gözetim yapılırsa olumsuz, insanların üretimde yer alabilmesi ile verimliliğin artması için yapılırsa olumlu hale gelmektedir (Baştürk, 2016, s. 44-45). Böylece, 1700'lü yıllardaki gözetimin, eski dönem gözetiminden farklı yönleri olduğu görülmektedir. Büyük Kapatılma'nın olduğu dönemde amaç; bazı grupların kapatılarak diğer insanlardan ayrıştırılmasıdır. Bu nedenle kapatılmayı uygulayan iktidarlar, negatif bir baskı gücüyle gözetimi gerçekleştirmektedir. Ancak daha sonraki dönemde ise gözetimi yapanlar, kişilerin maksimum verimliliğe ulaşması amacıyla bu gözetimi gerçekleştirmektedir. Söz konusu olan gözetim faaliyeti, her dakika devam eden kesintisiz bir gözetim olma özelliğini taşımaktadır. İşçilerin yaptıkları işin gözetlenmesiyle hem işçilerin üretimdeki verimliliğinin hem de üretimin miktarının arttırılması hedeflenmiştir (Bentham vd., 2008, s. 114).

1.2.2.2. Sanayi Devrimi'nden Günümüze Uzanan Dönem

İnsanlık tarihini etkileyen en önemli değişim Sanayi Devrimi ile meydana gelmiştir. Buhar makinesinin ve telgrafın icadı ile kullanımlarının yaygınlaşması gibi gelişmelerin üretim sisteminde kullanılmasıyla sosyal, kültürel ve ekonomik değişimler yaşanmıştır. Bu değişimler sonucunda tüm dünyadaki teknolojik gelişmeler ivme kazanmıştır (Canbey – Özgüler, 2018, s. 373; Ryan, 2010, s. 7).

Sanayi Devrimi'nin ardından kapitalizmin ortaya çıkıp yaygınlaşmasıyla birlikte devletlerde de gözetimin etkisi artmış ve böylece on dokuzuncu yüzyıl itibarıyla modern gözetim uygulamaları literatürde yer almaya başlamıştır. Sanayileşmenin artması sonucunda gözetimin amacı fabrikaların kâr oranını ve üretimdeki verimliliği arttırmak olmuştur. Özellikle bu dönemde fabrikalarda çalışan işçilerin gözetlenmesi ön plana çıkmıştır. İşçilerin işlerini tamamlayabilmesi için yeterli sürenin belirlenmesi, yapacakları işe göre çalışma alanlarının tespit edilmesi ve çalıştıkları süre zarfında işverenlerinin kesintisiz gözetim yapması bu dönemde uygulanmıştır (Bentham vd., 2008, s. 114; Lyon, 1994, s. 25; Çakır, 2015, s. 219; Dolgun, 2005b, s. 65).

Fordizm ve Taylorizm'in etkisiyle fabrikalarda işçilerin her adımı gözetlenmeye başlanmıştır. Fabrikalara montaj hattının gelmesinin ardından, işçilerin bu hat üzerinde üretime dair yaptığı işlemler ile bu işlemlerde meydana gelen kesintiler anlık olarak kayıt altına alınmıştır. Frederick Winslow Taylor'a göre, her işin kendine özgü analizi yapıldıktan sonra parçalara ayrılmalı ve en verimli şekilde yapılacağı yol seçilmelidir. Taylor, işçilerin bir işi ne kadar sürede ve kaç adımda gerçekleştirdiğini ölçmek için kronometreyle zaman tutup panolara not alan verimlilik uzmanı kişileri görevlendirerek gözetimi gerçekleştirmiştir. Gözetim uygulamasıyla her bir işin en kısa zamanda içerisinde, en az miktarda aşama kullanılarak ve en verimli şekilde yapılması amaçlanmıştır. Yapılan bu gözetimle aynı zamanda, her işçi için en uygun işin tespit edilmesi de mümkündür (Whitaker, 1999, s. 38-39).

Gözetimin sistematik hale gelerek insan hayatında olağan bir şekilde yer alması kapitalizmin, sanayileşmenin, şehirleşmenin artmasının ve ulus-devlet anlayışının gelişmesiyle eş zamanlıdır (Lyon, 1994, s. 24). Karl Marx'a (1992, s. 13) göre; kapitalist sistemle birlikte gözetim, emek ve sermaye mücadelesi arasında konumlanmıştır. Kapitalizm, köleliğin ortadan kalkmasına, diğer bir ifadeyle, kişilerin baskı ve zorlama gibi unsurlar dışında çalışabilmesine olanak sağlamıştır. Bu nedenle kendi iradeleriyle çalışma kararını alan işçilerin, işverenleri tarafından gözetlenerek kontrol altında tutulması ihtiyacı doğmuştur (Lyon, 1994, s. 7-24; Dolgun, 2005b, s. 74-75).

Gözetimle ilgili Sanayi Devrimi sonrası yapılan çalışmalara bakıldığında Max Weber'in belirleyici olduğu görülmektedir. Weber, fabrikalarda işçilerin izlenmesini kabul etmektedir. Ancak Weber'e göre gözetim, temelde bürokrasiyle yakından bağlantılıdır (Lyon, 1994, s. 25). Weber, modern devletin bütün vatandaşlarının bürokratik kurumlarca gözetlenmesi gerektiğini savunmaktadır. Hem bürokratik kurumlar hakkında hem de devleti yönetenler ile vatandaşlar hakkında bilgiler toplanmalı ve dosyalar halinde depolanmalıdır (Dolgun, 2005b, s. 83-84).

Anthony Giddens'a (2006, s. 300) göre ise, modern örgütlerde gözetim iki şekilde yapılmaktadır. Bunlardan birincisi; üst kademedeki yöneticilerin işçilerini gözetlemesidir. Diğeri ise; işçilere ait bilgilerin dosyalar haline getirilerek muhafaza edilmesi, işçilerin kayıtlarının tutulması ve işçilerin geçmişiyle ilgili bilgilerin değerlendirilmesidir. Bu işlemle birlikte işçilerin daha önce yaptıkları işler, kendileriyle

ilgili bilgiler, karakterleri ve davranış biçimleri incelemeye alınmaktadır (Küzeci, 2010, s. 28).

Modern dönemde yapılan gözetim uygulamalarının temelini ise, işyerlerindeki işçilerin gözetlenmesinin oluşturduğu görülmektedir (Dolgun, 2008, s. 77). İşçilerin fabrikalarda çalışmaya başlamasıyla birlikte çalışma saatleri önem kazanmıştır. Gözetim de işçinin çalışma saatleri üzerinden yapılmaya başlanmıştır. Ancak 1980'li yıllardan sonra bilgisayar, telefon ve kamera gibi bilişim teknolojilerine ait cihazların gelişmesiyle çalışma saatleri üzerinden yapılan gözetim faaliyeti yerini bilgisayar, telefon, internet gibi siber gözetim araçlarına bırakmıştır (Lyon, 1994, s. 34).

Modern gözetim faaliyeti, bilgisayar ağlarının gelişmesi sonucunda günümüzde post-modern gözetim kavramına evrilmiştir. Böylece gözetimin her an, her yerde kolaylıkla uygulanabilir olması kaçınılmaz bir hal almıştır (Lyon, 2006, s. 180-181). 1700'lü yılların sonunda Panoptikon adıyla bilinen; insanların hapishane, işyeri, okul ve askeriye gibi mekânlarda izlenmesini mümkün kılan sistem, teknolojik gelişmelerin ve küreselleşmenin etkisiyle yerini Süper Panoptikon kavramına bırakmıştır. Süper Panoptikon kavramı, Mark Poster tarafından ortaya atılmış ve David Lyon aracılığıyla da daha ileri bir boyuta taşınmıştır. Süper Panoptikon kavramına göre, bilgisayarların veri tabanları aracılığıyla kişilerin gözetimi anlık olarak sağlanabilmektedir. Hapishanelerde başlayıp okul ve hastane gibi mekânlarda da uygulanabilir hale gelmiş olan Panoptikon sistemi, Poster'ın geliştirdiği Süper Panoptikon modeliyle beraber bilgisayar veri tabanları yardımıyla mekândan bağımsız bir hal almıştır. Böylece gözetimi gerçekleştirenler gözetimin öznesi halini alırken, bu gözetime maruz bırakılan kişiler ise gözetimin en temel nesnesi haline dönüşmüştür. Dolayısıyla gözetimin nesnesi olan insanların günlük hayatta kesintisiz bir biçimde ve sistematik olarak kamera, telefon, bilgisayar gibi elektronik araçlarla gözetlenebilmesi mümkün kılınmıştır (Lyon, 2006, s.232-234; Öztürk, 2013, s. 138-139).

Sonuç olarak, teknolojinin gelişmesiyle birlikte Bentham'ın Panoptikon modeliyle ortaya atılan gözetim olgusu yerini bilgisayar, telefon, kamera ve internet gibi siber gözetim araçlarıyla kişilerin bilgilerinin toplanmasına, depolanmasına ve bu araçlar arası bilgi aktarımının sağlanmasına bırakmıştır. Böylece sürekli bir şekilde gözetim yapılmaktadır. Bu yönüyle gözetim, günlük hayatın vazgeçilmez bir parçası halini alarak, sistematik bir şekilde insan hayatında yer edinmiştir (Bentham vd., 2008, s. 141; Dolgun, 2005b, s. 124).

Bu bilgiler ışığında gözetimin bu elektronik biçimi zaman ve mekân fark etmeksizin uygulanabilir hal almıştır. Gözetim faaliyetinin etkisi altında kalan bireyler, izlendiklerinin bilincinde olmadan da bu uygulamaya maruz kalabilmektedir. Siber gözetim, toplumda giderek daha az fark edilir bir biçime kavuşmaktadır ve aynı zamanda kişilerin istekleri ya da kararları dışında uygulanabilmektedir. Bu nedenledir ki, günümüzde gözetim uygulamaları, bazen kişilerin onayı alınarak yapılırken bazen de gayri resmi şekillerde gerçekleştirilebilir olmuştur. Dolayısıyla dünya üzerinde yaşayan tüm insanlığa ait verilerin gizliliği risk altına girmiştir (Lyon, 1994, s. 53; Bozkurt, 2000, s. 77; Çaycı ve Çaycı, 2017, s. 164).

1.3. İşyerinde Kullanılan Siber Gözetim Aracı Türleri

Gözetleme uygulamalarının eski dönemlere nazaran günümüzde daha az dikkat çekici ve kesintisiz bir biçimde gerçekleştiriliyor olduğu bilinmektedir. Önceki bölümde belirtildiği üzere, tarihsel dönemlere ve gözetim araçlarının geçirdiği değişimlere bağlı olarak gözetim uygulamaları birtakım değişikliklere uğramıştır. İlk Çağ döneminde halk, kendi güvenliğini sağlamak amacıyla birbirini izlemiştir. Ardından çeşitli uygarlıkların, vatandaşları hakkındaki bilgileri toplayıp kayıt altına aldığı gözetim şekli ön plana çıkmıştır. Sanayi Devrimi'nin etkisiyle gerek işyerlerinin verimliliğini ve kazancını arttırmak, gerekse işçilerin yaptığı işi kontrol etmek amacıyla işverenler ya da üst düzey yöneticiler tarafından gözetim faaliyeti uygulanmıştır. Ulus-devlet dönemiyle birlikte ise, gözetim uygulamaları günlük hayatın bir parçası halini alarak sürekli ve sistematik bir şekle bürünmüştür.

Teknolojik gelişmelerin etkisiyle ortaya çıkan yeni gözetim uygulaması çeşitlerinin neler olduğunu ABD Teknoloji Değerlendirme Bürosu açıklamıştır. Buna göre, yeni gözetim araçlarının işitsel, görsel, verilere dayalı, algılayıcı ve diğer araçlar olmak beş farklı tür olarak ele alındığı söylenmektedir. Gözetimin dinlemeye bağlı şekilde yapılan türünde telefonların dinlenmesi ya da mikrofon gibi araçlarla sesin gözetleyen kişiye aktarılması durumu mevcuttur. Gözetlenen kişinin fotoğraflarının çekilmesi ve kameralar aracılığıyla izlenmesi gözetimin görsel boyutunu kapsamaktadır. Veriler yardımıyla yapılan gözetimde, özellikle bilgisayar ağları üzerinden kişilerin bilgilerinin toplanması, depolanması ya da işlenmesi mümkün olabilmektedir. Algılayıcı teknoloji olarak tanımlanan gözetim boyutuna göre; manyetik ve kızılötesi gibi sistemlerin kullanılmasıyla siber gözetim faaliyeti gerçekleştirilmektedir. Son olarak, telsiz dinlemeleri, kişinin kullandığı aracın yerinin tespit edilmesi ve parmak izi

alınması gibi uygulamalarla da gözetim faaliyeti yapılabilmektedir (Lyon, 1994, s. 103-104).

İletişim kurmak için kullandığımız araçların elektronikleşmesi ve türlerinin gitgide artmasıyla siber gözetim faaliyetinin uygulanması da aynı oranda artmıştır. 1958 yılından itibaren internetin kullanılmaya başlanması ve ilerleyen yıllarda kullanımının giderek yaygınlaşması, birçok teknolojik iletişim aracının insan hayatında yer edinmesine olanak tanımıştır (Bölükbaş, 2014, s. 30-31; Mitchell, 1996, s. 158). Gözetimin uygulanmasında kullanılan siber gözetim araçları yalnızca günlük hayatta değil, aynı zamanda işyerlerinde çalışan işçilerin gözetiminde de kullanılmaktadır. İşyerlerinin gözetlenmesine olanak sağlayan bilgisayar, internet, telefon, elektronik posta (e-posta) ve kamera sistemlerinin siber gözetim faaliyetinde ne şekilde yer bulduğu bu bölümün alt başlıklarında açıklanmaya çalışılacaktır.

1.3.1. Bilgisayar

Kullanıcılarından birtakım veriler toplayıp, bu veriler aracılığıyla mantığa ve aritmetiğe dayalı işlemleri gerçekleştirebilen, bunlara ait sonuçları depolayabilen ve depoladığı verileri gerektiğinde ortaya çıkartabilen elektronik cihaza *bilgisayar* adı verilmektedir (Okur, 2005, s. 48-49).

Dünya çapında meydana gelen sosyal, politik, ekonomik ve kültürel değişmeler, teknolojik gelişmelerin hızlanmasını sağlamaktadır (Canbey – Özgüler, 2018, s. 372). İnsanlar, en eski dönemlerde özellikle avcılık ve toplayıcılık faaliyetleri için hesap yapmış ve hesapladıklarını kaydetmiştir. Önceleri parmaklarını kullanan insanlar, çağ ilerledikçe ekonomik, kültürel ve sosyal hayattaki gelişmeler doğrultusunda karmaşık işlemleri yapabilmek amacıyla gelişmiş araçlara ihtiyaç duymuştur. Teknolojik gelişmelerle birlikte hesap yapmak için üretilen cihazlar zamanla geliştirilerek bilgisayarlara dönüştürülmüştür. Hesap makinesi olarak kullanılan araçların geliştirilerek günümüzde kullanılan bilgisayarlara dönüştürülmesindeki sürecin iyi bir biçimde açıklanabilmesi için bilgisayarların gelişiminin dönemler halinde anlatılması yerinde olacaktır (Garfinkel ve Grunspan, 2018, s. 19).

1.3.1.1. Birinci Nesil Bilgisayarlar Dönemi

İlk Çağ'da yaşayan avcı ve toplayıcı insanlar, avladıkları hayvanları saymak amacıyla parmaklarını kullanmaktaydı. M.Ö. 4000 yılından 3000 yılına kadar geçen dönemde insanların parmaklarını kullanarak yaptığı bu sayma işlemi, insanlığın kullandığı ilk bilgisayar olarak varsayılmaktadır (Dönmez, 2001, s. 30). Çağın giderek

modernleşmesi ve yerleşik hayata geçilmesiyle birlikte insanlar, yaptıkları bu hesaplamaları kaydetme ve gerektiğinde tekrar kullanma ihtiyacı duymuştur. M.Ö. 3200 yılında yazının bulunmasıyla birlikte insanlar, kaya ya da tahta gibi cisimlerin üzerine avladıkları hayvan sayılarını not etmiştir. Yazının bulunması doğrultusunda insanlar çağın gelişimine ayak uydurarak duvarlara çeşitli semboller çizmeye ve hesap işlemlerini yazmaya başlamıştır (Sharp, 1996'dan aktaran İşman, 2001, s. 3).

İnsanların matematik işlemlerinde kolaylık sağlanması açısından M.Ö. 500 yılında Çinliler ve Japonlar *abaküs* adı verilen ilk hesap tahtasını icat etmiştir. İlk basit hesap makinesi olarak bilinen bu tahta üzerindeki tellere geçirilmiş boncuklar yardımıyla hesaplama yapılabilmektedir. Abaküs, çok yaygın bir biçimde kullanılarak insanların hesap yapmasını kolaylaştırmıştır. Bu nedenle bilgisayar tarihçesinde önemli bir yer edinmiştir (Erkan, 2015, s. 14; İşman, 2001, s. 3).

Abaküsle yapılan işlemlerin, daha karmaşık işlemlerde yetersiz kalması üzerine bilinen ilk sayısal (mekanik) hesap makinesini 1642 yılında Blaise Pascal icat etmiştir. *Pascaline* adıyla bilinen bu makineyle yalnızca toplama ve çıkartma işlemleri yapılabilmektedir (Binark, 1979, s. 185). Bu hesap makinesi, ondalık (decimal) sistemle çalışmaktadır. Her ondalık işlem için on dişten oluştan bir çark yardımıyla işlemler yapılabilmektedir (Erkan, 2015, s. 14; Dönmez, 2001, s. 31). Pascal, icat ettiği bu hesap makinesinin patentini 1649 yılında almasına rağmen makinenin pahalı olması sebebiyle seri üretim yapamamıştır. Pascal'ın yaptığı çalışmalar teknolojiye katkı sağladığı için yaygın olarak kullanılan bir programlama diline Pascal adı verilmiştir (Ekiz vd., 2000, s. 73).

Pascaline'in geliştirilmesi adına yapılan çalışmalar sonucunda, 1671 yılında Gottfried Wilhelm Leibniz tarafından *Leibniz Çarkı* icat edilmiştir. Pascal'ın hesap makinesinden farklı olarak bu makineyle, çarpma, bölme ve karekök alma işlemleri gerçekleştirilebilmektedir (Ekiz vd., 2000, s. 73). Leibniz Çarkı'nın çalışma prensibi, Pascal'ın hesap makinesinden farklı olarak günümüzdeki bilgisayarların da çalışma prensibini oluşturan ikili (binary) sisteme dayanmaktadır. Bu cihazın içerisinde derecelendirilmiş bir çark bulunmaktadır. Çarkın pozisyonları farklı basamakları temsil eder ve yapılan işlemin sonucuna ulaşılması için çarkın belli bir biçimde döndürülmesi gerekmektedir. İşlemi yapacak olan kişi, bu çarkı ne kadar ve nasıl döndüreceğini diğer bir ifadeyle, cihazın kendine has programlama dilini bilmek durumundadır (Erkan, 2015, s. 14; http-3; Dönmez, 2001, s. 37). Leibniz, ürettiği bu makine üzerinde birçok

çalışma yaparak geliştirmeyi amaçlamıştır. 1716 yılında yeni bir model üzerinde çalıştığı sırada öldüğü için Leibniz Çarkı'nın geliştirilmesi yarım kalmıştır (Morar, 2014, s. 132).

Günümüzde kullanılan bilgisayarın temellerinin atılmasında bu hesap makinelerinin katkısı büyüktür. Ancak ilk bilgisayarın üretimi sürecinde Charles Babbage'ın yapmış olduğu hesap makinesi tasarımları önemlidir. Babbage, hesap makinesi tasarımlarıyla ilk sayısal bilgisayarın mucidi olarak kabul edilmektedir. 1821 yılında Babbage, Greenwich Gözlemevi'nde çalıştığı sırada kaşiflerin gemilerinin rotasını ayarlamak için kullandığı tablolardaki birçok hatayı saptamıştır. Bu hataların düzeltilmesinde mekanik bir cihazın işini daha çok kolaylaştıracağını düşünen Babbage, *Fark makinesi (Difference engine)* tasarımını gerçekleştirmiştir. Bu makinenin işleyişi, makineye yerleştirilen delikli kartlar üzerinden iletilen komutlarla aritmetik birtakım işlemin yapılması şeklindedir. Fark makinesi komut işlemenin yanı sıra yaptığı hesaplamaları hafızasında tutabilme, komutları sıralı ve art arda olacak biçimde işleme ve trigonometrik ile logaritmik tablolar hazırlayarak sayısal çözümleme yöntemiyle hesap yapabilme özelliğine sahiptir. Modern bilgisayarın ilk örneği sayılan fark makinesinin tasarımı tamamlanamamıştır. Bunun en temel sebebi ise, bu makinenin yapımında kullanılacak olan metal parçaların üretilmesini sağlayan teknolojinin gelişmemiş olmasıdır (Erkan, 2015, s. 14; Dönmez, 2001, s. 29; Ekiz vd., 2000, s. 73).

1833 yılı itibarıyla Babbage *Analitik makine (Analytical engine)* üzerinde çalışmalar yapmıştır. Bu makinenin veri ve formülleri işleyebilmesi için delikli kartlar kullanılmaktadır. Analitik makinenin hem buhar gücü yardımıyla otomatik olarak işlemleri gerçekleştirebilmesi hem de delikli kartlar yardımıyla programlanabilmesi fark makinesinden ayrılan yönü olarak bilinmektedir. Babbage, yaşadığı maddi problemler sebebiyle bu makinenin tasarımı da hayata geçirememiştir. Ancak 1910 yılında Babbage'ın oğlu analitik makinenin bir bölümünü yapmış ve çalıştırmayı başarmıştır. Analitik makinenin üretilen kısmı günümüzde Londra Bilim Müzesi'nde sergilenmektedir. Babbage'ın yaptığı bu makine tasarımları veri girişine imkân tanıdığı, matematiksel denklemleri çözebildiği, tablo hesaplamasına yardımcı olduğu ve işlenen verileri depolayabildiği için modern bilgisayarın temelini oluşturmaktadır. Bu nedenle Babbage, bilgisayarın babası olarak bilinmektedir (Erkan, 2015, s. 14; http-3; http-4).

1890 yılı itibarıyla Hermann Hollerith, delikli kartlar aracılığıyla verileri işleyen bir makine geliştirmiştir. Bu cihazla birlikte yapılan veri işleme hızı artarken, işlemlerin

yapılması sırasında oluşan hataların azalmıştır. Hollerith'in geliştirdiği bu sistem, elektro-mekanik bilgi işleme sistemlerinin temelini oluşturmuştur. Mekanik bilgisayar sistemlerinin geliştirilmesi üzerine yapılan çalışmalar sonucunda 1896 yılında Hollerith, British Tabulating Machine Company (BTM) şirketini kurmuştur. 1924 yılı itibarıyla BTM, başka bir şirketle birleşerek International Business Machines (IBM) ismini almıştır (http-5; Binark, 1979, s. 186; Erkan, 2015, s. 15).

1939 yılında John Vincent Atanasoff ve asistanı Clifford Berry delikli kartlarla veri işleyen makinelerden vakum tüpleriyle çalışan makinelere geçiş yaparak bilgisayar teknolojisine önemli bir yenilik getirmiştir. Ürettikleri Atanasoff-Berry Computer (ABC) adıyla bilinen bu cihaz ilk elektronik (dijital) bilgisayar olarak kabul edilmektedir. 1941 yılına kadar bu bilgisayar üzerinde çalışmalar gerçekleştirilmiştir. Ancak İkinci Dünya Savaşı'nın başlamasıyla bu çalışmalara ara verilmiştir (Boyanov, 2003, s. 2-5).

İkinci Dünya Savaşı süresince şifrelerin çözülmesi, lojistik işlemleri ve menzillerin hesaplanması gibi işlemlerin daha kolay ve hızlı yapılabilmesi için çok sayıda bilim insanı ve mühendis çalışmalar yürütmüştür. Bilgisayar teknolojinin gelişmesinde savaş dönemi oldukça etkili olmuştur (Erkan, 2015, s. 15). Bu çalışmalardan bir tanesi 1944 yılında Harvard Üniversitesi'nde gerçekleştirilmiştir. Howard Aiken ve IBM'nin ortak yürüttüğü çalışmalar sonucunda Mark-I isimli elektro-mekanik (dijital) ilk bilgisayar üretilmiştir. Bu bilgisayar; içerisine yerleştirilen delikli kartları, verilen kodlar yardımıyla delerek istenen bilgileri kaydedebilme ve bilgileri tekrar okuyabilme özelliğine sahip olmasıyla bilinmektedir. Mark-I, insan müdahalesi yardımıyla çalışabildiği için elektro-mekanik bilgisayar olarak kabul edilmiştir. Ancak Mark-I, beklenilen hızda çalışamamış ve doğru sonuç verme oranı düşük kalmıştır (http-6).

Mark-I'in icadından kısa bir zaman sonra Atanasoff'un elektronik bilgisayarından ilham alınarak 1945 yılında Pennsylvania Üniversitesi'nde ENIAC (Electronic Numerical Integrator and Computer) isimli bilgisayar üretilmiştir. Top mermilerinin kat ettiği mesafeyi ölçmek için tasarlanan ENIAC'ın üretiminde on yedi bin dört yüz altmış sekiz adet vakum tüp kullanılmıştır. Kullanılan tüp sayısının fazla olması, tüplerin boyutunun büyük olması ve dönemin teknolojisinin el verdiği şartların bir sonucu olarak üretilen bu bilgisayar, günümüzde giderek küçülen bilgisayarlar ve tabletlerin aksine otuz ton ağırlığında, otuz metre genişliğinde ve iki buçuk metre yüksekliğinde

tasarlanmıştır. Mark-I bilgisayarından bin kat daha hızlı olan ENIAC, saniyede yüz bin hesaplama işlemini gerçekleştirebilmektedir (Uzgören, 1999, s. 167; Lyon, 2006, s. 222; http-6).

ENIAC'ın içinde yer alan tüplerin ısınması ya da cihazın içerisine böceklerin kaçması sebebiyle sıklıkla bozulduğu için EDVAC ve UNIVAC isimli yeni bilgisayarlar üretilmiştir. ENIAC'ı geliştiren ekipte yer alan John Von Neumann'ın yönlendirmesiyle 1946 yılında EDVAC (Electronic Discrete Variable Automatic Computer) geliştirilmiştir. Yapılan geliştirme çalışmalarıyla birlikte EDVAC, ENIAC'tan on kat daha küçük ve yüz kat daha hızlı olacak biçimde tasarlanmıştır. 1951 yılı itibarıyla ise ENIAC'ın üretimini yapan ekip tarafından UNIVAC (Universal Automatic Computer) üretilmiştir. UNIVAC'ta ilk kez manyetik teyp sistemi kullanılarak daha fazla verinin depolanabilmesi sağlanmaya çalışılmıştır. Aynı zamanda bu bilgisayar hem teknik hem de ticari amaçla kullanılabilen ilk bilgisayar olması açısından önemlidir (http-5; Ekiz vd., 2000, s. 75-76).

1953 yılı itibarıyla IBM tarafından bilimsel çalışmalarda kullanılmak için tasarlanmış ilk büyük işlemciye sahip bilgisayar olan IBM 701 üretilmiştir. 701 serisinin hemen ardından yine IBM tarafından işyerlerinde kullanılabilecek şekilde tasarlanmış olan 702 serisine ait bilgisayarlar üretilmiştir. IBM'in ardından Bendix, Borroughs ve General Electric (GE) gibi birçok şirket bilgisayar üretimi yapmıştır. Dolayısıyla farklı şirketlerin bilgisayar üretimi piyasasına dahil olmasıyla şirketlerin arasındaki rekabet hem bilgisayarlara olan talebi hem de teknolojik buluşları arttırmıştır (Ekiz vd., 2000, 76; Binark, 1979, s. 186).

1946-1959 yıllarında geliştirilmiş olan birinci nesil bilgisayarlar aracılığıyla veri depolama işleminin ve bilgi üretiminin yapılabilmesi için yüksek oranda elektrik harcanması gerekmektedir. Harcanan elektrik miktarı arttıkça bilgisayarlar da ısınmaktadır. Bilgisayarların ısınması sonucunda daha hızlı bir biçimde arızalanması söz konusu olmaktadır. Buna ek olarak, birinci nesil bilgisayarların depolama kapasitesi maksimum iki kilobayt olabilmektedir. Bu olumsuzlukların giderilmesi amacıyla 1950'lerin sonunda bilgisayar üretiminde vakum tüpleri yerine transistör kullanılmıştır. Transistörlerin kullanılması ikinci kuşak bilgisayar dönemini başlatmıştır (Kılıç, 2005, s. 15; http-6).

1.3.1.2. İkinci Nesil Bilgisayarlar Dönemi

1959-1964 yılından itibaren üretilen bilgisayarlarda vakum tüpleri yerine transistörler kullanılmasıyla bilgisayarlar hem daha hızlı şekilde işlem yapar hale gelmiş hem de hacim olarak küçülerek daha az yer kaplamıştır (Binark, 1979, s. 187).

Transistör kullanılarak üretilen ilk bilgisayar, IBM tarafından 1959 yılında duyurulan 1401 numaralı modeldir (Campbell-Kelly vd., 2014, s. 84). IBM 1401 modeli, ticari amaçlı kullanım için üretilmiştir. Aynı yıl içinde üretilen IBM 1620 modeli ise bilimsel kullanım amacıyla üretilmiştir. İkinci dönem bilgisayarlarında yer alan transistörler sebebiyle bilgisayar hem daha az elektrik tüketmiştir hem de daha az ısınarak çalışmıştır (Binark, 1979, s. 187).

İkinci nesil bilgisayarlarında kullanılan transistörler, vakum tüplerine kıyasla daha küçük boyda ve daha güvenilir özelliğe sahiptir. Transistörler yardımıyla çalışan bilgisayarlar, bir önceki neslin bilgisayarlarından birçok konuda daha üstün konumdadır. İkinci nesil bilgisayarlar hem daha az ısınmaktadır hem de daha az enerji tüketerek çalışmaktadır. Depolama kapasitesi maksimum otuz iki kilobayta kadar çıkartılmıştır. Bu bilgisayarların işlemleri gerçekleştirme hızı da önceki nesle göre daha yüksektir. Aynı zamanda bu nesildeki bilgisayarların kapladığı yer azalmıştır ve daha ucuza üretilmeye başlanmıştır. İkinci nesil bilgisayarlarının dönemini kapsayan 1959-1964 yılları arasında COBOL, FORTRAN ve PCII gibi programlama dilleri geliştirilmiştir (Kılıç, 2005, s. 15; Ekiz vd., 2000, s 76).

Günümüzde kısa bir süre içinde ve çok hızlı bir biçimde çok sayıda işlemi yapabilme kapasitesine sahip olan süper bilgisayarların temeli de ikinci nesil bilgisayarların döneminde atılmıştır. 1964 yılında Symour Cray, CDC 6600 adındaki ilk süper bilgisayarın tasarımını gerçekleştirmiştir. Bu gelişmenin hemen ardından Cray, Cray-I ve Cray-II serisinin üretimi yapılmıştır. Günümüzde de en hızlı işlem yapan süper bilgisayarlar halen Cray şirketi tarafından üretilmektedir (http-7; Ekiz vd, 2000, s. 76).

1.3.1.3. Üçüncü Nesil Bilgisayarlar Dönemi

İkinci nesil bilgisayar döneminin önemli bir parçası olan transistörlerin sayısının artmasıyla bilgisayarlarda problemler oluşmuştur. Bu problemlerin giderilmesi için çok sayıda mini transistörün silikon ipler üzerine yerleştirildiği entegre devreler oluşturularak üçüncü nesil bilgisayarlarda kullanılmaya başlanmıştır. Entegre devrelerin üretilmesiyle bilgisayarların işlem yapma hızı yükselmiştir (Kılıç, 2005, s. 15-16).

1964-1970 yıllarını kapsayan bu dönemin en önemli özelliği, bilgisayarlarda ilk kez entegre devrelerin kullanılmış olmasıdır. Entegre devreler yardımıyla bilgisayarların yaptığı işlemler kontrol, işlem yapma, depolama ve taşıma şeklinde kategorilere ayrılmıştır. Bunun yanı sıra, bilgisayarlardaki verileri ve yazılım komutlarını işlemekle görevli Merkezi İşlem Birimi (Central Processing Unit – CPU) bu dönem içerisinde ilk kez üretilmiştir (Ekiz vd., 2000, s. 76-78; http-8).

Bu dönemdeki gelişmeler doğrultusunda birçok yeni bilgisayar üretilmiştir. Bunlardan en önemli iki tanesi; IBM şirketi tarafından üretilen IBM 360 modeli ve Digital Equipment Corporation (DEC) tarafından üretilen PDP-8 modelidir. 1964 yılında üretilmiş olan IBM 360 modeli, günümüzdeki bilgisayar sistemlerinin zeminini hazırlamıştır. Bu modelin üretilmesiyle birlikte gelecekte daha hızlı çalışan, daha yüksek bellek kapasitesine ve daha geniş yazılım desteğine sahip olan bilgisayarların geliştirilmesi amaçlanmıştır. 1965 yılında DEC şirketi tarafından üretilen PDP-8 modeli ise, ticari anlamda başarı sağlayan ilk mini bilgisayardır. IBM 360 modelinden hem daha ucuz hem de daha küçük boyutta olduğu için o yıl içerisinde yaklaşık elli bin adet PDP-8 model bilgisayar satılmıştır (http-9; Ekiz vd., 2000, s. 78).

Birinci ve ikinci nesil bilgisayarlarda yapılmak istenen her bir işlem için yalnızca tek bir program çalıştırılabilmektedir. Ancak üçüncü nesil bilgisayarlarda yapılan yeniliklerle bu durum değiştirilerek aynı anda birden fazla programın çalıştırılması sağlanmıştır (Kılıç, 2005, s. 16).

Üçüncü nesil bilgisayarların döneminde entegre devre işlemcilerin kullanılması, bilgisayarların üretim maliyetlerinin düşmesi ve dış yüzeyindeki manyetik kaydetme alanı sayesinde veri depolama işlemini gerçekleştirebilen manyetik disklerin üretilmesi gibi gelişmeler meydana gelmiştir. Bütün bunlara ek olarak 1963 yılı itibarıyla BASIC adıyla bilinen programlama dili geliştirilmeye başlanmıştır (http-10; Ekiz vd., 2000, s. 78).

1.3.1.4. Dördüncü Nesil Bilgisayarlar Dönemi

1970 yılından 1990 yılına uzanan dönemde dördüncü nesil bilgisayarlar üretilmeye başlanmıştır. Bu dönemde bilgisayarlardaki işlem ve kontrol birimlerinin bir arada yer aldığı çipler üretilmiştir (http-6). Bu çiplerin her birinde iki yüz bin ila bir milyon adet genişletilmiş entegre devre yer almaktadır. Devre sayısı arttıkça bu devrelerin de daha az yer kaplayacak şekilde konması gerekliliği ortaya çıkmıştır.

Böylece parmak büyüklüğünde üretilen çiplerin üzerine bu devreler yerleştirilmiştir (Kılıç, 2005, s. 16).

1968 yılı itibarıyla kurulmuş olan Intel şirketi, 1971 yılına gelindiğinde dünyadaki ilk mikroişlemci olan Intel 4004'ü üretmiştir. Intel 4004'te CPU yalnızca bir çip içerisine entegre edilmiştir (http-11). Bir düğmeyle eşit büyüklükteki bu çipin üzerinde iki binden fazla sayıda transistör yerleştirilmiştir. Bu gelişmeyle birlikte dördüncü nesil bilgisayarların üretiminin önü açılmıştır. 1971 yılı sonrasında bilgisayarlarda yer alan bu çipler gün geçtikçe geliştirilmiştir (Erkan, 2015, s. 16).

Intel şirketinin kurucularından biri olarak bilinen Gordon Moore, 1965 yılı itibarıyla bir makale yayımlatmıştır. Bu makalede yer alan teoriye göre bilgisayarda yer alan çiplerin üzerindeki transistörler her iki yılda kendini ikiye katlayacaktır. Moore teorisi olarak adlandırılan bu teori sayesinde günümüzde milyonlarca transistörden oluşan mikroişlemciler üretilmiştir (http-12; Tekeli, 1994'ten aktaran Erkan, 2015, s. 16).

Bu gelişmeler ışığında bilgisayarlar hem daha güçlü hem de daha hızlı işlem yapabilen bir hal almıştır. Mikroişlemcilerin giderek daha ucuza üretilmesiyle beraber taşınabilir bilgisayarların geliştirilmesinin önü açılmıştır. İlk taşınabilir bilgisayar 1974 yılında üretilmiştir. Yirmi üç kilogram ağırlığında ve dokuz bin dolar değerinde olan bu bilgisayar IBM tarafından tanıtılmıştır (Ekiz vd., 2000, s. 78).

1977 yılında Steve Jobs ve Steve Wozniak, Apple-I isimli bilgisayarı üretmiştir. Böylece Apple Computer şirketi kurulmuştur. Apple-I bilgisayarının ardından aynı yıl içerisinde ilk kişisel bilgisayar olarak bilinen yaklaşık beş buçuk kilogram ağırlığındaki Apple-II bilgisayarı bin üç yüz dolarlık etiketle satışa sunulmuştur. Teknolojik gelişmeler ışığında hem kişisel bilgisayarların üretimi artmış hem de satış fiyatları düşerek ağ sistemleri aracılığıyla bilgisayarların birbirine bağlanması sağlanmıştır (Ekiz vd., 2000, s. 78; http-5 ve http-13).

1.3.1.5. Beşinci Nesil Bilgisayarlar Dönemi

1990 yılından günümüze kadar uzanan dönemde beşinci nesil bilgisayarlar yer almaktadır. Üretiminde yoğun paralel işlemci ve vektör işlemci kullanılan bu bilgisayarlar, belirlenmiş bir problemin birden fazla ögesi üzerinde eş zamanlı ve hızlı bir biçimde çalışabilmektedir (Kılıç, 2005, s. 17). Beşinci nesil bilgisayarın geliştirilmesinde yapay zekâ ve bulanık mantık teknolojilerinden yararlanılmaktadır (Ekiz vd., 2000, s. 80). "İnsan zekasıyla gerçekleştirilen zeki ve karmaşık işlemlerin

makineler tarafından yapılması" şeklinde tanımlanan yapay zekâ kavramının bilgisayarlarda ve bilgisayar temelli makinelerde kullanılmasıyla daha akıllı işlemler yapan, kendi denetimini sağlayan ve insanlarla uyum içinde çalışan bilgisayar sistemlerinin üretimi hedeflenmiştir (Pirim, 2006, s. 84; http-14). Bulanık mantık ise "İnsanların deneyimleri ve verileri üzerinden elde edilen değerlerin bazı algoritmalar kullanılarak işlenmesiyle sonuca ulaşılması" olarak ifade edilebilmektedir. Bulanık mantık teknolojisiyle bilgisayarlar, ikili (binary) sistem olarak bilinen 0 ve 1 değerlerinden oluşan sistemin yerine 0.4 ve 0.73 gibi ara değerleri kullanarak işlem yapabilmektedir (Keskenler ve Keskenler, 2017, s. 3). Günümüzde sadece bilgisayarlarda değil aynı zamanda elektrikli ev aletleri, arabaların bazı parçaları ve elektronik bazı cihazlarda da bulanık mantık teknolojisi kullanılmaktadır. Bulanık mantık teknolojisiyle bilgisayarların, karmaşık işlemleri daha kolaylıkla ve hızlı olarak çözebilmesi amaçlanmaktadır (Pirim, 2006, s. 88).

Beşinci nesil bilgisayarların etkili olduğu bu dönemde bilgisayar ve internet ağında meydana gelen gelişmelerle birlikte insanların bilgisayarı ve bilgiyi kullanma oranı artmıştır. Böylece bilgi çağına geçiş sağlanmıştır (Canbey – Özgüler, 2018, s. 376-377). Birçok araştırmacıya göre; bilgisayarların ağ sistemleri yardımıyla birbirine bağlanması ve *dünya çapında ağ (world wide web – www) sistemi* üzerinden internette yer alan bilgilere kolaylıkla erişilmesi toplumları dönüştüren ve geliştiren bir yenilik olarak kabul edilmektedir. Günümüzde bilgisayarlar, insanların sosyal hayatı içerisinde sıklıkla yer almaya başlamıştır. İnsanların sosyal hayatının yanı sıra çalışma hayatında da üretim sistemleri ve üretim ilişkileri içindeki en temel ögeyi beşinci nesil bilgisayarlar oluşturmaktadır. İşyerlerinde mal ve hizmetlerin üretilmesi, pazarlanması, tedarik edilmesi ve tasarlanması gibi faaliyetlerde bilgisayar temelli sistemler kullanılmaktadır (Erkan, 2015, s. 16).

Bilgisayarların siber gözetim faaliyetinde bir araç olarak kullanılması ise 1960'lı yılları bulmuştur (Uzgören, 1999, s. 167; Lyon, 2006, s. 222). *Bilgisayar eşleştirme sistemi* adı verilen bir sistem yardımıyla çokça kaynaktan edinilen kişisel bilgilerin türlü maksatlarla kullanılması için işlenebilir hale gelmesi sağlanabilmektedir. 1970'li yılların sonuna yaklaşırken, devlet daireleri gibi birtakım bürokratik kurumlar, bu bilgisayar eşleştirme sistemini kullanarak gözetimin bilgisayarlarla yapılabilmesinin önünü açmıştır. Bu sistemle, insanlar hakkında daha önceden toplanmış olan bilgiler birleştirilerek bir bütün haline getirilmekte ve böylece kişiyle ilgili daha fazla veri elde

edilmektedir. 1980'li yıllar itibarıyla bilgisayarlar siber gözetimde kullanılan en temel elektronik cihazlar halini almıştır. Bilgisayarlar; bir yandan uydu, kamera gibi izleme sistemleriyle, diğer yandan ise internet ağıyla ortaklaşa bir biçimde gözetimi gerçekleştirmiştir. Bundan on yıl sonra, 1990'lı yıllarda ülkeler vatandaşlarının kişisel bilgilerinin depolandığı veri bankalarını oluşturmuştur. Böylece gözetimin bilgisayarlar aracılığıyla depolanarak yapılması durumu ortaya çıkmıştır. Günümüzdeki bilgisayar yoğun teknolojilerin insanların hem günlük hem de çalışma hayatında kullanımının artmasıyla birlikte gözetim faaliyeti, fark edilmeden yapılabilir bir hal almıştır ve bilgisayarları kullanan kullanıcılar da bu görünmez denetimin uygulanmasına istemeden de olsa katkı sağlamıştır (Lyon, 1994, s. 50; Dolgun, 2005b, s. 129-131).

1.3.2. İnternet

Birden fazla bilgisayarın bağlanmasıyla aralarında bilgi aktarımını sağlaması ise bilgisayar ağı (network) aracılığıyla mümkün olabilmektedir. Bir şirket gibi aynı yerde bulunan ve birbiri arasında çok fazla mesafe olmayan bilgisayarlar *yerel bölge ağı (Local Area Network – LAN)* aracılığıyla birbirine bağlanabilmektedir. "Birbirine uzak olan ve aynı mekânda bulunmayan bilgisayarların meydana getirdiği sistem *geniş bölge ağı (Wide Area Network – WAN)*" şeklinde tanımlanmaktadır. "Farklı ülkelerde şubesi bulunan şirket bilgisayarlarının oluşturduğu yerel bölge ağlarının birleşmesiyle geniş bölge ağları" oluşmaktadır. "Milyonlarca bilgisayar ağını birbirine bağlayan küresel ağ bağlantısı" internet olarak bilinmektedir (Kaya, 2006, s. 309).

Uluslararası İletişim Ağı (International Network) kavramının karşılığı olan ve TDK tarafından genel ağ kavramıyla ilişkilendirilen *internet;* "Haberleşme için kullanılan birçok sayıda kablolu ve kablosuz bağlantılar, yönlendiriciler ve birtakım sunucular yardımıyla toplanmış olan bilgisayar ağı" olarak tanımlanmaktadır. İnternet sayesinde ortaya bir iletişim alanı çıkmaktadır (Okur, 2005, s. 49; Petersen, 2001, s. 895). İnternette yer alan bilgi ve hizmetler ağ erişimine sahip kullanıcılara sunulmaktadır. Geçerli bir internet adresine ve internet bağlantısına sahip olan tüm kullanıcılar dünyanın her noktasından bilgisayar, telefon ya da tablet gibi araçlar aracılığıyla bilgi ve hizmetlere erişebilmektedir (Başaran, 1998, s. 1).

İnternetin geçmişten günümüze uzanan yolculuğuna bakıldığında görülmektedir ki, 1947-1991 yılları arasını kapsayan Soğuk Savaş Dönemi'nde internet sistemi, ordunun iletişim gerçekleştirebilmesi amacıyla kullanılmak istenmiştir. 1969 yılında The Advanced Research Projects Agency Network (ARPANET) adlı bir sistem üretilmiştir.

Bu ağ sistemi adını Amerika Birleşik Devletleri Savunma Bakanlığı'nın Gelişmiş Araştırma Projeleri Ajansı'ndan (Advanced Research Projects Agency – ARPA) almıştır. ARPANET sistemi, herhangi bir askeri saldırı olduğunda iletişim kurulabilecek bir ağ bağlantısı olması amacıyla geliştirilmiştir (Güven, 2014, s.102-103; Castells, 2010, s. 52-53; Staples, 2007, s. 297-298).

"Birden fazla bilgisayarın aynı ağ sistemi üzerinden birbirine bağlanabilmesi için gerekli olan sistem" *protokol* olarak adlandırılmaktadır. Telnet protokolü yardımıyla 1972 yılında ilk kez uzaktaki bir bilgisayarla bağlantı kurulmuştur (http-15 ve http-16). Bu gelişmeden bir yıl sonra 1973 yılında *File Transfer Protocol (FTP)* aracılığıyla ilk kez bilgisayarlar arasında dosya transferi işlemi gerçekleştirilmiştir (Kutup, 2010, s. 12). İnternet ağının gelişmesiyle 1980'li yıllar itibarıyla üniversiteler gibi eğitim kurumlarında kullanılabilir hale gelmiştir (Güven, 2014, s.102-103; Castells, 2010, s. 52-53; Staples, 2007, s. 297-298).

1990'lı yıllara gelindiğinde www teknolojisi, Cenevre'deki Avrupa Nükleer Araştırma Merkezi (Conseil Européen pour la Recherche Nucléaire – CERN) bünyesinde Tim Berners-Lee tarafından geliştirilmiştir (Akçakaya, 2009, s. 525). Berners-Lee www teknolojisini, bilgisayarlarda saklanan bilgilere istenilen her yerden daha kolay bir biçimde erişilebilmesini sağlamak amacıyla üretmiştir. Ancak www teknolojisi üretildiği bu yıl içerisinde kişisel değil kitlesel bir kullanım amacına hizmet etmiştir. 1991 yılında ise yine Berners-Lee tarafından bir bilgisayar dili olan *Hyper Text Mark-up Language (HTML)'yi* geliştirilerek www teknolojisi kişisel olarak kullanılabilmeye başlanmıştır (Briggs ve Burke, 2011'den aktaran Cizmeci, 2015, s. 85).

Dünya çapında internetin gelişimi üç farklı dönem çerçevesinde ele alınmaktadır. 1995-2000 yıllar arasında etkili olan Web 1.0 döneminde interneti kullanan kişiler birbiriyle iletişim kuramamakta ve yalnızca internette var olan bilgileri okuyabilme imkanına sahiptirler. Dolayısıyla Web 1.0 döneminde kullanıcılarının bilgiyi alan kişi konumunda olduğu söylenebilmektedir (Kutup, 2010, s. 13, http-17).

2000 yılından 2010 yılına kadar Web 2.0 dönemi etkili olmuştur. Web 1.0 dönemindeki eksiklikler bu dönemde giderilmeye çalışılmıştır. Web 2.0 döneminin en temel özelliği, insanlar arasında bir etkileşime izin vermesidir. Bu dönemde kullanıcılar internete içerik yükleyebilmekte ve diğer kullanıcılara bu içerikleri gönderebilmektedir. Kullanıcılar içerik paylaşma ve birbirlerine gönderme işlemini sosyal ağ siteleri ya da

internet ansiklopedileri gibi internet sayfaları üzerinden gerçekleştirebilmektedir. Web 2.0 döneminde tasarımsal ve teknik açıdan gelişmeler meydana gelmiştir. Bu dönemde kişilerin kendi kişisel internet sayfalarını (bloglar) oluşturmalarıyla tasarımsal yenilikler ortaya çıkmıştır. Bir internet tarayıcısı olan Google da bu dönemde geliştirilmiştir. (Kutup, 2010, s. 13, http-17).

2010 yılından günümüze uzanan dönemde Web 3.0 etkili olmuştur. Web 3.0'dan önceki dönemlerde internette yer alan bilgiler, yalnızca insanların anlayacağı şekilde tasarlanmıştır. Dolayısıyla internet ortamındaki bilgiyle kullanıcı arasında bir ilişki mevcuttur. Web 3.0 döneminde internetteki içeriklere yalnızca insanlar değil aynı zamanda bazı bilgisayar yazılımları da erişebilmiştir. Bu dönemde bilgisayar yazılımları, mevcut bilgileri hafızasına kaydederek kullanıcılara en uygun olan bilgiyi iletecek şekilde programlanmıştır. Böylece Web 3.0 döneminde yapay zekanın etkili olacağı öngörülmektedir (Kutup, 2010, s. 13-14, http-18).

Türkiye'ye 1960 yılında gelmiş ilk bilgisayar IBM 650 modelidir. Ancak ülkemizde internetin gelişim tarihi incelendiğinde, ilk bilgisayarın gelmesinden yaklaşık otuz yıl sonra ilk internet bağlantısının gerçekleştiği görülmektedir. Buna göre; 1991 yılında Orta Doğu Teknik Üniversitesi (ODTÜ) ve Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'nun (TÜBİTAK) birlikte yürüttüğü çalışmayla ilk internet bağlantısı gerçekleştirilmiştir. 1993 yılında ise ODTÜ ve Washington arasında internet bağlantısı kurulmuştur (Canbey – Özgüler, 2015, s. 211). Bu ağ bağlantısıyla amaçlanan, bilimsel bilgi alışverişinin sağlanmasıyla akademik hayatın gelişimine yardımcı olmaktır (Yılmaz, 2015, s. 10).

ODTÜ'deki internet bağlantısının sonrasında 1994 yılında Ege Üniversitesi'nde, 1995 yılında Bilkent Üniversitesi ve Boğaziçi Üniversitesi'nde ve 1996 yılında İstanbul Teknik Üniversitesi'nde internet bağlantısı gerçekleştirilmiştir (Parlak, 2005, s. 30). Ancak internetin halkın kişisel kullanımına sunulması 1996 yılında olmuştur. Bu yıl içerisinde Türk Telekom ülkemizdeki ilk internet servis sağlayıcısı olan TR-NET projesiyle interneti hem halkın hem de ticari kuruluşların erişimine açmıştır (Saka, 2019, s. 9).

1996 yılında TÜBİTAK kapsamında Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) kurulmuştur. ULAKBİM'in amacı, teknolojik gelişmeler ışığında Türkiye'de yer alan eğitim ve araştırma kuruluşları arasında hızlı bir iletişim ağı oluşturmak ve bu ağ üzerinden bilgi hizmeti sağlamaktır. ULAKBİM'in iletişim ağı

Ulusal Akademik Ağ (ULAKNET) adıyla bilinmektedir. ULAKBİM, ülkemizde internet ağının yayılmasına yardımcı olmuştur (Parlak, 2005, s. 30).

1996 yılında toplamda beş tane internet servis sağlayıcısına sahip olan Türk Telekom, 1997 yılında bu sayıyı seksene yükseltmiştir. Böylece Superonline gibi internet hizmetini sağlayan şirketler kurulmuş ve internet hizmeti satılmaya başlanmıştır (Saka, 2019, s. 9).

1998 yılı itibarıyla Ulaştırma Bakanlığı tarafından *İnternet Üst Kurulu* kurulmuştur. Bu kurulun amacı; internetin tüm boyutlarıyla ilgili kısa, orta ve uzun vadeli planlar yaparak hedefler belirlemek, bu hedeflerin gerçekleştirilmesi için birtakım kararlar almak, kararların uygulanmasında ortaya çıkan ya da çıkabilecek problemleri tespit ederek çözmek, ağ sistemlerinin geliştirilmesi ve yaygın hale getirilmesi için çalışmalar yürütmektir (Canbey – Özgüler, 2015, s. 213). İlerleyen yıllarda isim değişikliğiyle birlikte *İnternet Kurulu* olarak görevlerine devam etmiştir (Saka, 2019, s. 9).

2002 yılına gelindiğinde ülkemizde E-Devlet sistemine dair çalışmalar başlamıştır. Ancak çalışmaların tamamen bitirilerek E-Devlet'in kullanıma açılması 2008 yılında meydana gelmiştir (http-19). 2003-2004 yılları arasında ise bir internet bağlantısı tekniği olan Asimetrik Sayısal Abone Hattı (Asymmetric Digital Subscriber Line – ADSL) bağlantıları yapılmıştır (Saka, 2019, s. 11). ADSL bağlantısına geçilmesiyle internete bağlanma hızı artmıştır (http-20). 2000'li yılların başlarında *Ekşi Sözlük (eksisozluk.com)* kurulmuştur.

2000'li yıllardan günümüze uzanan dönemde internette meydana gelen teknolojik ilerlemeler sonucunda *Youtube (youtube.com)* gibi video paylaşım sitesi, haber içerikli siteler, *Facebook (facebook.com)* gibi sosyal paylaşım ve iletişim siteleri, kişisel bilgi paylaşımına olanak tanıyan bloglar ve tartışma forumları gibi birçok internet sitesi kurulmuştur ve günümüzde de halen yenileri kurulmaktadır (Başaran, 2010, s. 260).

Günümüzde insanlara ait bilgilerin elde edilmesi ve kullanılmasında bir araç olan bilgisayarların yanı sıra internet ağ sistemiyle kişisel verilere ulaşım yaygınlaşmıştır (Akgül, 2013, s. 32). Teknolojik gelişmeler doğrultusunda artık, yalnızca bilgisayarlar üzerinden değil cep telefonu ve tabletler gibi elektronik cihazlardan da internete erişmek oldukça kolaylaşmıştır. Zira, internet ağıyla yapılan her türlü işlem sonucunda bilgi üretimi ve bu bilgilerin depolanması söz konusudur (Lessig, 2006, s. 216). E-posta ve anlık mesajlaşma hizmetlerinin geliştirilmesiyle internet, sadece belirli kurumlarda

kullanılabilen bir ağ sistemi olmaktan çıkarak günlük hayatın bir parçası halini almaya başlamıştır (Güven, 2014, s.102-103; Castells, 2010, s. 52-53; Staples, 2007, s. 297-298).

30 Ocak 2019 tarihinde yayımlanan Küresel Dijital 2019 Raporu'na bakıldığında, dünya çapında 4,39 milyar kişinin internet kullandığı verisine ulaşmak mümkündür (http-21). Dünya çapında internet kullanımının yaygınlaşmasıyla birlikte internet üzerinden yapılan her türlü işlem gözetlenebilmektedir. Günümüzde bilgisayar, tablet ve cep telefonu gibi siber gözetimde kullanılan araçlar internet bağlantısına sahip olduğundan, işçilerinin internet kullanarak yaptığı tüm hareketlerin gözetlenebilmesi mümkündür. İnternete bağlı bir bilgisayara yüklenen birtakım programlar yardımıyla işçilerin gönderdiği ya da aldığı e-postaların içeriğine işverenler tarafından ulaşılabilmektedir. Bununla birlikte internete erişim sağlanan bilgisayar ya da telefon gibi cihazlara birtakım programlar yüklenmesiyle işçilerin hangi internet sitelerine hangi saatler içerisinde giriş yaptığı bilgisi de işverenler tarafından bilinebilmektedir (Savaş, 2009, s. 97-99).

1.3.3. Elektronik Posta (E-Posta)

Electronic Mail (e-mail) kavramının dilimizdeki karşılığı olan e-posta; "İnternet veya herhangi bir ağa sahip bilgisayar ve cep telefonu gibi elektronik cihazlar aracılığıyla kişilerin bir sunucu üzerinden diğer kişilerle iletişim kurmasına olanak tanıyan dijital mesajlaşma sistemi" olarak tanımlanmaktadır (Soysal, 2005, s. 321; Staples, 2007, s. 198). Günümüzde e-postaların sadece yazıdan oluşması şartı bulunmamaktadır. Yazı içeriğine ek olarak fotoğraf, ses kaydı, müzik dosyası ve video gibi çeşitli dosyalar da e-postalara eklenerek gönderilebilmektedir (Kalaman, 2013, s. 171).

Ray Tomlinson tarafından 1972 yılında bir program yazılmıştır. Bu yazılımın amacı, bir bilgisayardan diğerine elektronik bir mesajın iletilmesini sağlamaktır. ARPANET üzerinden ve Tomlinson tarafından gönderilen ilk e-posta rastgele harflerden oluşmuş bir test mesajını içermektedir (Varol ve Baştürk, 2015, s. 273; http-22). Sonrasında, e-postayı gönderen kullanıcının adı ile e-postayı gönderirken kullandığı bilgisayarın adının birbirine karışmaması amacıyla bir sembole ihtiyaç duyulmuştur. Bunun üzerine Tomlinson "@" sembolünü seçmiştir (Soysal, 2007, s. 146; Kutup, 2010, s. 12).

1972 yılının mart ayında, Tomlinson basit bir e-posta yazma ve okuma sisteminin geliştirilmesi üzerinde çalışmalar yapmıştır. Bundan dört ay sonra, temmuz ayı itibarıyla, e-posta sisteminde iletilerin listelenmesi, dosyalanması, başka bir kullanıcıya iletilmesi ve cevaplanması gibi birtakım geliştirmeler yapılmıştır (Leiner vd., 2009, s. 24).

1983 yılı itibarıyla Domain Name System (DNS) sunucuları geliştirilmiştir. Ağ üzerinden veri göndermek ya da veri almak için kullanılan Internet Protocol (IP) adresi yerine alan isimleri kullanılmıştır ve e-posta adreslerinin önüne "@" simgesi yerleştirilmiştir. O dönemde gönderilen ilk e-postaların içeriğini yazılar oluşturmaktadır ve başlık ile gövde şeklinde iki ana bölümden meydana gelmektedir. Başlık ve gövde bölümlerini boş bir satır birbirinden ayırmıştır (Varol ve Baştürk, 2015, s. 273).

Teknolojik gelişmelerle birlikte bugün gönderilen *e-postalarda çok amaçlı internet posta eklentileri (multipurpose internet mail extensions – MIME)* kullanılmaktadır. Günümüzde sadece metinlerden oluşan e-posta yerine içerisinde fotoğraf, müzik ya da video dosyaları bulunan e-posta alışverişinde bulunmak mümkün olmaktadır. Buna ek olarak; sadece başlık ve gövdeden oluşan e-postaların yerini daha detaylı bilgiler içeren e-postalar almıştır. Gelişmeler doğrultusunda e-postalara konu, alıcı ve gönderen kişiye ait bilgiler eklenebilmektedir (Varol ve Baştürk, 2015, s. 273-274).

Günümüzde e-posta kullanımı kişilerin hem özel hem de çalışma hayatında önemli bir yer edinmiştir. Özellikle hızlı bir şekilde iletişim kurmayı kolaylaştırdığı ve maliyetsiz olduğu için e-posta kullanımı yaygın hale gelmiştir (Keser, 2005, s. 60). E-posta kullanımının yaygınlaşmasıyla zaman ve yer fark etmeksizin kolay bir biçimde kişilerarası yazılı iletişim gerçekleştirilebilmektedir. Bugün, yurtdışında ikamet eden herhangi bir kişiye e-posta göndererek kendisiyle iletişime geçmek bir hayli basit ve ucuzdur (Özger, 2017, s. 31).

Günlük hayatta ve çalışma hayatında kişilerin e-posta alışverişlerinin gözetlenebilmesi mümkündür. Kişinin e-posta kullanımlarının gözetlenmesinde *Echelon* adı verilen sistem kullanılmaktadır. İşverenler, birtakım anahtar kelimeler belirledikten sonra Echelon sistemi yardımıyla işçilerin e-postalarında bu kelimeleri filtreleyebilmektedir. Böylece, gözetim faaliyetini gerçekleştirmek isteyen kişilerce e-posta konuşmalarının içeriğine basitçe ulaşılabilmektedir. (Bölükbaş, 2014, s. 37; Lyon, 2006, s. 15).

1.3.4. Kamera

TDK tarafından kamera; "Hareketsiz olan görüntülerin film haline getirilmesini gerçekleştiren optik bir alet" olarak tanımlanmaktadır (http-23). Gözetim faaliyetlerinde kullanılan en önemli aracı kamera sistemleri oluşturmaktadır (Koskela, 2000, s. 243). Bu nedenle kameranın tarihsel gelişimini ele almak yararlı olacaktır.

Tüm fotoğraf makineleri ve kameraların atası olarak bilinen alet *Camera Obscura*'dır. Latince iki kelimeden oluştan Camera Obscura, karanlık oda anlamına gelmektedir. M.Ö. 5. yüzyılda Çinli bir filozof olan Mo Ti tarafından ortaya atılan Camera Obscura tasarımı karanlık bir odayı ya da bir kutuyu betimlemektedir. Bu odanın duvarlarından birinin ortasına, yalnızca küçük bir ışık hüzmesinin girebileceği bir delik açılmaktadır. Bu delik haricinde oda tamamen karanlık durumdadır. Delikten odanın içerisine sızan ışık, deliğin hemen karşısındaki duvara yansımaktadır. Dolayısıyla deliğin önünde bulunan nesneye ait görüntü karşıdaki duvara ters dönmüş bir biçimde iletilmektedir (Turan, 2011, s. 20; Uçar vd., 2015, s. 189).

Camera Obscura sisteminin geliştirilmesindeki en önemli rol İbn-i Heysem'e aittir. 10. yüzyılda yaşamış olan İbn-i Heysem, Camera Obscura tasarımını mum ışığı kullanarak gerçeğe döndürmüştür. Mum ışığının odanın deliğinden geçerek kırılmasını ve ters bir biçimde yansımasını açıklamıştır. İbn-i Heysem'in açıkladığı bu sistem, 19. yüzyıla kadar kullanılmıştır (Göktepe, 2015, s. 7).

16. yüzyıla gelindiğinde Camera Obscura resim yapma amacıyla kullanılmaya başlanmıştır. 1550 yılında Girolama Cardano tarafından Camera Obscura'ya bir optik takılmıştır (MEB, 2012, s. 4). 1568 yılında ise Daniello Barbero tarafından Camera Obscura sistemine farklı merceklerin eklenmesi sayesinde alınan görüntü daha net ve daha parlak hale gelmiştir. Camera Obscura orijinal haliyle bir oda olarak düşünülmüştür. 17. yüzyıla kadar uzanan dönemde de oda büyüklüğünde kalmıştır. Ancak hem daha küçük bir kamera ihtiyacından hem de kullanımında kolaylık sağlaması açısından ilerleyen yıllarda geliştirilerek boyutu küçültülmüştür. 1776 yılında Johann Zahn tarafından taşınabilir bir kutu haline getirilen Camera Obscura'ya, günümüzdekine benzer bir objektif düzeneği ilave edilmiştir (Göktepe, 2015, s. 6-9).

Camera Obscura'nın hem daha kullanışlı bir hale getirilmesi hem de çektiği görüntüleri kaydetmesi amacıyla yapılan çalışmalar 19. yüzyıla dek devam etmiştir. 1827 yılında ilk fotoğraf Jacques Louis Daguerre ve Joseph Nicéphore Niépce'nin gerçekleştirdiği çalışmalarla Fransa'da çekilmiştir (Göktepe, 2015, s. 18; Şan-Aslan,

2019, s. 53). Niépce'nin ilk fotoğrafı, günümüzdeki anlamıyla bir elektronik fotoğraf makinesi aracılığıyla çekilen fotoğraftan farklıdır. Helyografi adı verilen bu fotoğraf karanlık bir kutuda, ışığa duyarlı bir yüzey yardımıyla kaydedilmiştir (Kılıç, 2015, s. 115).

1833 yılında Niépce'nin ölümü üzerine Daguerre çalışmalarını tek başına yürütmek zorunda kalmıştır. 1835 yılı itibarıyla Daguerre, sodyum klorür bileşiğini kullanarak görüntüyü kaydetme üzerinde çalışmıştır. 1839 yılında ise *Daguerrotype* isimli bir buluş gerçekleştirmiştir. Helyografiden sonra en önemli icat kabul edilen Daguerrotype sayesinde önceleri yaklaşık yedi ila sekiz saat süren fotoğraf çekme süresi yarım saate kadar düşmüştür (Algan, 1999'dan aktaran Göktepe, 2015, s. 18; http-24).

1850'lerden itibaren fotoğraf çekme eylemi giderek yaygınlaşmıştır, dolayısıyla fotoğraf makineleri ve kameralar da gün geçtikçe geliştirilmiştir. 1852 yılında Kodak şirketinin kurucusu olan George Eastman tarafından ilk Kodak fotoğraf makinesi piyasaya sürülmüştür. On adet poz çekebilme imkânı sağlayan bu makinenin taşınabilir ebatta olması sebebiyle fotoğrafçılara büyük bir kolaylık sağlanmıştır. 1877-1878 yılları arasında Eadward Muybridge tarafından *Zoo-praxiscope* isimli alet üretilmiştir. Tek tek çekilmiş olan fotoğraflar Zoo-praxiscope isimli aynalar ve film bandından oluşan düzeneğe yerleştirilmiştir ve düzenek çevrildiğinde, sanki kamerayla çekilmiş bir görüntü gibi hareket ediyor olarak görülmektedir. İlerleyen zamanlarda Muybridge'nin Zoo-praxiscope düzeneği sinemanın gelişmesine öncülük etmiştir (http-25).

1887 yılı itibarıyla Hannibal Goodwin fotoğraf çekmek için selüloit film şeridi kullanmıştır. Bu gelişmeden bir yıl sonra 1888 yılında ise, Eastman tarafından selüloit film şeritlerinin seri üretimi yapılarak sinema filmlerinin çekilmesinde ve dolayısıyla kameranın geliştirilmesinde büyük bir adım atılmıştır (Göktepe, 2015, s. 26).

1890 ve 1891 yıllarına gelindiğinde Thomas Alva Edison, *Kinetograf* ve *Kinetoskop* adlı iki alet üretmiştir. "Hareket eden görüntüleri kayıt altına alan alet" *kinetograf* olarak tanımlanmıştır. Tek tek çekilmiş olan fotoğrafları seri şeklinde kaydetmesi amaçlanan bu alet, günümüzdeki kameraların üretilmesinde önemli bir adım olarak görülmektedir. "Kaydedilmiş olan hareketli görüntüleri göstermeye yarayan alet" ise *kinetoskop* adıyla bilinmektedir. Edison, Kinetoskop'u tasarlarken, Muybridge'nin Zoo-praxiscope'sinden ilham almıştır (Ekinci, 2017, s. 829).

Edison'un tasarladığı Kinetoskop aletiyle kaydedilen görüntüler, yalnızca tek bir kişi tarafından izlenebildiği için Lumière Kardeşler tarafından *Sinematograf* icat

edilmiştir. Sinematograf sadece görüntüleri kaydetmekle kalmayıp, çekilen bu görüntülerin başkaları tarafından izlenebilmesine ve bu negatif filmin pozitif baskının yapılabilmesine olanak tanımaktadır. On altı kareye kadar görüntüleri kaydedebilen sinematograf, kaydettiği bu on altı kareyi de on altı saniye boyunca kesintisiz olarak göstermektedir. Sinematograf; yedi kilogram ağırlığında, yirmi santimetre uzunluğunda ve ok iki santimetre genişliğinde olacak şekilde üretilmiştir (Kılıç, 2015, s. 121).

1923 yılında Film Kamerası adında bir kamera üretilmiştir. Bu kamerayla birlikte artık amatör kullanıcıların da film çekebilmesi olanaklı hale gelmiştir. 1959 yılına gelindiğinde ise tek mercekli (Single-Lens Reflex – SLR) ilk fotoğraf makinesi olan Nikon F modeli piyasaya sürülmüştür (Kılıç, 2015, s. 126-128; Kayabaş, 2016, s. 118; http-26).

Kamera sistemlerinin yaygınlaştığı 1980'li yıllarda, kameraların en temel özelliği görüntüleri kayıt altına alabiliyor olmalarıdır. Bu anlamda; günümüzde kullanılan kamera sistemleri, daha eski dönemlere ait olan sistemden farklı olarak birbirine bağlı bir biçimde çalışma prensibi olan, görüntüleri kaydedip saklayan, kaydetme sırasında izleme olanağı sunan ve isteğe bağlı olarak farklı açılardan görüntü alınması sağlanabilen bir sistem haline gelmiştir (Güven, 2012, s. 42-43). Aynı zamanda elektronik fotoğraf makinelerinin üretimine de 1980 yılında başlanmıştır. 1988 yılında FujiFilm tarafından üretilmiş olan FUJIX DS-1P model fotoğraf makinesinin tanıtımı yapılmıştır. Bu makinenin en önemli özelliği tamamıyla dijital olan ilk makine olmasıdır. Özellikle 1990'lı yıllardan günümüze uzanan dönemde teknolojide meydana gelen ilerlemeler doğrultusunda fotoğraf makineleri ve kameralar giderek küçülmüştür. Günümüzde fotoğraf makineleri ve kameraların satılması dışında akıllı cep telefonları, tabletler ya da bilgisayarlara entegre edilmiş halde insanların ceplerinde ve çantalarında taşıyabildikleri ve hatta kalemlerin içine sığdırılabilen boyutlara gelmiştir (Kılıç, 2015, s. 126-128; Kayabaş, 2016, s. 118; http-26).

Günümüzde taşınabilir kameraların yanı sıra gözetim faaliyetinde kullanılan bir diğer kamera türü de Kapalı Devre Kamera Sistemi'dir (Closed Circuit Television – CCTV). Bu sistem işyeri, banka, havaalanı, üniversite gibi kurum ve kuruluşlarda yer alan bir sistem olarak bilinmektedir. CCTV sistemi; "Gözetimi yapmakla görevlendirilen kişinin, kameranın kaydettiği görüntüleri televizyon aracılığıyla izleyebildiği bir teknolojiyi" nitelendirmektedir (Walby, 2005, s. 658).

CCTV sisteminin ilk defa kullanılması 1942 yılına dayanmaktadır. Almanlar tarafından Nazi ordusuna ait roketlerin izlenerek kontrol edilmesi amacıyla kamera sisteminin kullanıldığı bilinmektedir. İngiltere'de kamerayla yapılan ilk gözetim faaliyeti ise, 1956 yılı itibarıyla halkın, trafik ışıklarına uyup uymadığının denetlenmesini sağlamak için polis tarafından gerçekleştirilmiştir. Londra ve New York'taki tren istasyonları ve meydanlar gibi kamuya açık alanlarda kameralarla gözetleme, ilk kez 1960'lı yıllarda yapılmıştır (Güven, 2012, s. 42-43; Norris, McCahill ve Wood, 2004, s. 110). Londra'nın yeraltı metrosunda kullanılan *Cromatica* adlı sistem; "Kayıt yapan kameranın bir bilgisayara bağlanması sonucunda, metro istasyonundaki halkın izlenebilmesini ve yoğunluktan oluşabilecek herhangi bir izdihamın engellenebilmesini sağlamak" için tasarlanmıştır (Lyon, 2006, s. 120).

Özellikle Kuzey Amerika, Avrupa ve Asya kıtasında yer alan ülkelerde CCTV sistemi yaygın olarak kullanılmaktadır. İngiltere ve Amerika Birleşik Devletleri gibi gelişmiş ülkelerde güvenliğin sağlanması, şehir içi trafiğin yönetilmesi ve işyerlerinin denetlenmesi amacıyla CCTV sistemiyle gözetime sıklıkla rastlanmaktadır (http-27). Böylece şehirlerde yer alan kamera sayısının ve dolayısıyla gözetim faaliyetinin giderek artmasıyla şehirler modern bir Panoptik mekân halini almıştır (Koskela, 2000, s. 243).

Gözetim faaliyetlerinde kullanılan kamera sistemleri yalnızca günlük hayatın izlenmesinde değil, aynı zamanda işyerlerindeki işçilerin gözetiminde de kullanılmaktadır (Koskela, 2000, s. 243). Teknolojik gelişmelerle birlikte kameraların boyutları giderek küçülmüştür. Gözle görülebilir boyuttaki kameraların yanı sıra; gözlük, yangın detektörü, ışıklandırma sistemleri, duvara asılmış saatler ve masaların üzerinde duran dekoratif heykelcikler gibi nesnelerin üzerine konulmuş veya içerisine gizlenmiş boyutlarda kameralar da üretilmektedir (Aydemir, 2012, s. 46). Dolayısıyla günlük hayat ya da çalışma hayatı içerisinde kameralarla siber gözetim faaliyetinin yapılabilmesi giderek kolaylaşmaktadır.

1.3.5. Telefon

Dilimize Fransızcadan geçen *telefon* kelimesinin TDK tarafından verilmiş karşılığı; "Birbirinden uzakta bulunan kişilerin konuşmasını sağlayan aygıt" şeklindedir (http-28).

Alexander Graham Bell'in 1878'de telefonun patentini alarak halka tanıtmasından kısa bir süre sonra, 1900'lü yılların başında, telefon sistemleri ilk kez Amerika Birleşik Devletleri'ndeki polis karakollarında kullanılmaya başlanmıştır (Petersen, 2001, s. 125).

1975 yılına gelindiğinde, Martin Cooper tarafından ilk cep telefonunun patenti alınmıştır. 1980'li yıllara geçilmesiyle beraber dünya genelinde hem cep telefonları hem de iletişim kurmak için gerekli olan altyapı sistemleri hızlı bir biçimde gelişmeye başlamıştır (Staples, 2007, s. 29-88).

ABD'de 1952 yılında kurulan Ulusal Güvenlik Ajansı (National Security Agency – NSA), diplomatlar ile askerlerin yaptığı şifrelenmiş telsiz konuşmalarını dinleme yöntemine başvurarak, dinleme yoluyla gözetim faaliyetini başlatan ilk kuruluştur. İlerleyen yıllarda ise NSA, dünya genelinin konuşmalarını dinleme faaliyetini üstlenmiştir. Günümüzde NSA, hem gelişmiş teknolojilere sahip olması bakımından hem de uydu sistemlerinin ilerlemesi bakımından tüm dünyanın izlenmesini gerçekleştiren en üst kuruluş olarak bilinmektedir (Dolgun, 2005b, s. 123).

Hootsuite ve We Are Social tarafından toplanan verilere göre Digital 2019 raporunda dünya genelinde 5,11 milyar kişi cep telefonu kullanmaktadır. Bununla birlikte, 2018 yılından bu yana cep telefonu kullananların sayısı 100 milyon artmıştır. 2019 yılı itibarıyla dünya nüfusunun 7,53 milyar olduğu göz önüne alındığında cep telefonu kullanan kişi sayısının bir hayli yüksek olduğu görülmektedir (http-29). Cep telefonu kullanımının giderek artmasıyla birlikte siber gözetim faaliyetinin uygulanması da giderek kolaylaşmaktadır. Gerek sabit telefonların gerekse cep telefonlarının fatura dökümleri sayesinde hangi numaralarla ve ne kadar süre konuşulduğu bilgisine rahatça erişilebilmektedir (Mitchell, 1996, s. 158). Cep telefonlarına yüklenebilen çeşitli uygulamalar ve programlar aracılığıyla kişinin faaliyetlerinin izlenebilmesinin yanı sıra, cep telefonu tamamen kapalı konumdayken dahi dinleme yapılabilmesi mümkün olmaktadır. Aynı şekilde, yüklenen bazı uygulamalar üzerinden telefonu kullanan kişinin konum bilgilerine de ulaşılabilmektedir (Akyürek, 2011, s. 69). Sonuç olarak, cep telefonlarının bu fonksiyonları göz önüne alındığında siber gözetim faaliyetinin çok önemli bir parçasını oluşturduğu söylenebilmektedir (Çetin ve Asıl, 2017, s. 193).

1.4. İşyerinde Yapılan Siber Gözetim Faaliyeti

Çalışma ortamında işverenler, kimi zaman işçileri kimi zaman ise işyerini korumak amacıyla çeşitli araçları kullanarak gözetim faaliyetini gerçekleştirmektedir (Rosenblum, 1990, s. 80). İşyeri ortamında işçilerin gözetlenmesi faaliyeti günümüzde popüler bir hal almış gibi görünse de aslında geçmişte de işverenler tarafından tercih edilen bir yöntem olmuştur. 1913 yılında; "İşyerinde kullanılan daktilolardaki tuş

vuruşlarını sayarak kayıt altına alan" *cyclometer* adındaki cihazlar yardımıyla işçiler gözetime tabi tutulmaktaydı (Botan, 1996, s. 294).

Teknolojik gelişmelerin ışığında işverenlerin, işçilerini gözetlemesi bilgisayar, kamera ve telefon gibi birçok elektronik cihazın yaygınlaşmasıyla giderek kolaylaşmıştır (Cozzetto ve Pedeliski, 1996, s. 22). İşçilerin, teknolojinin gelişmesiyle işyerlerinde siber gözetim araçları yardımıyla gözetlenmesi *Elektronik Performans İzleme Sistemi* (EPİS) adıyla bilinmektedir. Bu sistem çoğunlukla hizmet sektöründe ve imalat sanayisinde kullanılmaktadır. EPİS; "Bilgisayarlar kullanılarak fabrikalardaki işçilerden yaptıkları işlerle ilgili bilgilerin elde edilmesi, biriktirilmesi ve analiz edilerek raporlar haline getirilmesi" şeklindeki sistemi tanımlamaktadır (Carayon, 1994, s. 177-178). Bilgisayarlarla yapılan gözetim faaliyeti, işçilerin çalışma performansının değerlendirilmesiyle onlara zam yapılması ya da prim almalarının sağlanmasının yanı sıra, çalışma saatleri içerisinde işten kaytaran işçileri denetim altına almak için de kullanılan bir sistemdir (George, 1996, s. 461).

Bilgisayarların kullanımıyla yapılan gözetim faaliyeti iletişim takibi olarak da bilinmektedir. İletişim takibi işlemi; bilgisayarlar aracılığıyla internette yapılan araştırmaların, gönderilen ya da alınan e-postaların takip edilmesi şeklinde gerçekleştirilmektedir. İşyerinde bilgisayar kullanan işçilerin hangi sitelerde gezindiği, ne kadar süre boyunca bir sitede vakit harcadığı, kimlerle e-posta alışverişinde bulunduğu ve kimlerle anlık görüşmeler yaptığı bilgisayarlara yüklenen birtakım yazılımlar sayesinde tespit edilerek kayıt altında tutulabilmektedir. Bunun yanı sıra bilgisayar klavyelerindeki tuş vuruşlarının ölçülmesi ve işçiye ait verilerin kayıt altına alınmasıyla gözetimin gerçekleştirilmesi mümkündür. Bu yöntemle her fare hareketi, e-posta trafiği ve yazılıp silinmiş olan cümleler gibi veriler toplanabilmektedir. İşverenler, işçilerinin bilgisayarlarda yaptığı işlemleri rahatlıkla izleyebilmektedir. Bu gözetimin yapılmasında casus olarak tanımlanan klavyeler, hafıza kartları ya da çeşitli bağlantı kabloları kullanılabilmektedir (TMMOB Elektrik Mühendisleri Odası, 2009, s. 10; Weckert, 2005, s. 27).

İlk bilgisayarın üretildiği ve geliştirildiği yıllarda bilgisayarlar hem yüksek maliyetli hem de bu teknolojiye ulaşmak zor olduğundan her işyerinde bulunmamaktaydı. Teknolojide meydana gelen gelişmeler sonucunda günümüzde bilgisayarlara ulaşmak giderek kolaylaşmıştır. İşyerlerinin birçoğunda kullanılan bilgisayarlar aracılığıyla siber gözetim yapılması mümkün olmaktadır. Üç temel özelliği

bakımından bilgisayarlar, siber gözetim faaliyetinde kullanılmaktadır. Bilgisayarların birinci özelliği; sistematik bir biçimde çalışmakta olduğu için gözetimi sürekli ve kolay bir biçimde gerçekleştirebilmesidir. İkinci özellik, günümüz teknolojisinde bilgisayarların çok hızlı bir biçimde işlem yapabilmesi sebebiyle kişilere ait verileri de kısa sürede toplayabilmesidir. Siber gözetim faaliyetinde kullanılan bilgisayarların sonuncu özelliği ise; toplanan verilerin birçok bilgisayar arasında aktarılabilir olmasıdır. Bu üç temel işlevi açısından bilgisayarlar, gözetim aracı olarak ele alınabilme anlamında önemli bir konumdadır (Petersen, 2001, s. 893).

Shoshana Zuboff'un gözetim hakkında yaptığı araştırmalara göre, özellikle üretim bandında ve büro bölümünde çalışan işçilerinin daha yüksek oranda gözetlendiği ortaya çıkmıştır. Zuboff'un bu araştırması, üretim bandında ve büro bölümünde çalışan işçilerin diğer departmanlarda çalışan işçilere kıyasla siber gözetim faaliyetinden daha fazla şikayetçi olduğunu göstermiştir. Zuboff, bu işçilere ait bilgilerin işverenler tarafından bilgisayarlarla denetlenerek elde edildiğini ve diğer işçilere göre bu işçilerden daha fazla bilgi toplandığını vurgulamıştır. Bu nedenle işçilerin siber gözetim faaliyetinden diğer işçilere göre daha fazla şikayetçi olduğu düşünülmektedir. (Zuboff, 1988'den aktaran Lyon, 1994, s. 131-132).

Amerikan Yönetim Örgütü (American Management Association – AMA) ve E-Politika Enstitüsü (The ePolicy Instutite) 2007 yılında *Elektronik İzleme ve Gözetim Araştırması* adıyla bir çalışma yapmıştır. Bu çalışma göstermektedir ki, işverenlerin %45'i işçilerinin klavye üzerinden gerçekleştirdiği tuş vuruşlarını ve klavyeyi kullandıkları sürenin ne kadar olduğunu takip etmektedir. Bunun dışında, işverenlerin %43'ü bilgisayardaki dosyaları depolayıp incelemektedir (http-30). Dokuz yüz işyerinde yapılan bu araştırmanın sonucuna göre; bu işyerlerinin üçte ikisinde çalışan işçiler siber gözetim faaliyetiyle denetlenmektedir. ABD'de olduğu gibi Fransa'da da benzer durum geçerlidir. Ulusal Bilgi İşlem ve Özgürlükler Komisyonu (Commission Nationale de L'informatique et des Libertés – CNIL) verilerine bakıldığında, elektronik gözetimin 1998 yılı itibarıyla yirmi sekiz bin şirket tarafından uygulandığı bilinmektedir. İşverenler, işçilerinin gözetimini bilgisayar üzerinden yaparken "Pc Anywhere" isimli programdan yardım almaktadır. Buna ek olarak, Microsoft'un ürettiği "Intellimouse" isimli programla bilgisayar kullanan işçiler denetlenebilmektedir. Bu program; bilgisayar kullanıcılarının fare (mouse) hareketleri üzerinden işçilerin işbaşı

yaptığı saati göstermenin yanı sıra, bu hareketlerinin ölçülmesi yardımıyla işçilerin ne kadar süre çalışmış olduklarının bilgisini de vermektedir (Dolgun, 2005a, s. 510).

Hootsuite ve We Are Social tarafından toplanan verilere göre Digital 2019 raporunda dünya genelinde 4,388 milyar kişinin interneti kullandığı açıklanmıştır. 7,676 milyardan oluşan dünya nüfusunun yarısından fazlasının internet kullanıcısı olduğu düşünüldüğünde internet kullanımının çok yaygın olduğu söylenebilmektedir (http-29).

İşyerinde işçilerin internet kullanımına yönelik 2014 yılında Salary.com web sitesi için Cheryl Conner tarafından bir araştırma yapılmıştır. 750 işçiden veri toplanarak yapılan bu araştırmaya göre; işçilerin %69'u çalışma esnasında internette vakit geçirdiğini belirtmiştir. İşçilerin %31'i çalışma saatleri içerisinde internette otuz dakika harcarken, yine %31'lik diğer kesim ise bir saat harcamaktadır (http-31).

İşyerinde internet kullanımının tespit edilmesi amacıyla Harris şirketi tarafından CareerBuilder için bir araştırma yapılmıştır. Birçok farklı sektör ve şirkette çalışan 2,138 üst düzey çalışan ile 3,022 tam zamanlı çalışan üzerinde yapılan bu araştırmaya göre; işçilerin %24'ü gün içerisinde internette en az bir saat harcamaktadır. Bu işçilerin %50'si cep telefonundan görüşme yapmakta ya da mesaj atmaktayken, %39'u ise internet sitelerinde vakit geçirmektedir (http-31).

AMA'nın internet kullanımına ilişkin diğer verilerine bakıldığında; işverenlerin, işçilerinin internette uygunsuz aramalar yapmasından kaygılanmakta olduğu sonucuna ulaşılmaktadır. Bu nedenle işverenlerin %60'ı işçilerinin internet bağlantısını izlerken, %65'i ise bir yazılım programı kullanarak işçilerinin uygunsuz sitelere girişini önlemeye çalışmaktadır (http-30).

Weckert (2005, s. 24) ve Aydemir'in (2012, s. 39-40) işyerinde işçilerin internet kullanımına dair düşünceleri ise şu şekildedir: "Çalışma saatlerinin belli bir kısmını internette harcayan bazı işçiler; tatil rezervasyonu ya da internet alışverişi yapma, eğitici web sitelerinden bilgi edinme faaliyetinde bulunmakta, bilgisayarları oyun oynama amacıyla kullanmakta, uygunsuz içeriğe sahip bazı siteleri ziyaret etmekte ve çalışma süresini çalışma performansını arttırmak adına verimli kullanmak yerine diğer iş arkadaşlarıyla sohbet ederek harcamaktadırlar". İşverenler ise işçilerinin çalışma saatleri içerisinde sorumlu olduğu işi yapmasını ve iş dışında başka herhangi bir faaliyet aracılığıyla dikkatini dağıtmamasını talep ettiği için işçilerini gözetleme ihtiyacı duymaktadır. Temel olarak bu sebeple işverenler, işçilerinin bilgisayar ve internet ağı üzerinden yaptıkları kullanımlarla gözetleme yoluna başvurmaktadır.

Gerek günlük hayatta gerekse çalışma hayatında bilgisayar ve internet teknolojisinin etkisiyle e-postanın sıklıkla tercih edilen bir iletişim biçimi olduğu bilinmektedir. Günümüzde yalnızca bilgisayardan değil aynı zamanda cep telefonları ve tabletler gibi yanımızda taşıyabildiğimiz elektronik cihazlardan da internete bağlanmak mümkün hale gelmiş ve böylece şirketlerde internet kullanımı oranı da giderek artmıştır. İş hayatında e-postayla iletişim kurulması hem maddi açıdan hem de hızlı ve kolay kullanım imkânı sunması nedeniyle tercih edilmektedir (Yiğit, 2013, s. 45; Aydemir, 2012, s. 37).

Fernandez'in (2004'den aktaran Kierkegaard, 2005, s. 235) işçilerin e-posta kullanımına yönelik yapmış olduğu bir çalışmanın sonuçlarına göre; işçilerin çalışma sırasında gönderdiği ya da aldığı e-postaların %50-60'ı işçinin özel hayatıyla ilgili içeriğe sahiptir. Bu e-postalarla yapılan iletişim ise, işçilerin verimliliğini %30-40 oranında düşürmektedir. İşverenler; işletmenin ve işçinin verimliliğinin artması, çalışma ortamında güvenliğin sağlanması ve işçilerin çalışma sırasında sorumlu oldukları iş haricinde e-posta gönderme ya da alma gibi faaliyetlerle dikkatini dağıtmasını ve zamanını boşa harcamasını önlemek amacıyla e-posta kullanımını gözetlemektedir.

İşverenler, işçilerinin ve işletmenin çalışma performansının artması için e-postaları gözetlemenin yanı sıra, işçiler ile müşteriler arasındaki iletişimin içeriğini de bilmeye ihtiyaç duymaktadır. İşçilerin; işyeri, işin kendisi ve işveren hakkındaki bazı paylaşılması sakıncalı olacak bilgileri müşterilere iletebileceği ihtimaline karşı işverenler e-posta gözetimi yapmaktadır. Burada işverenin temel amacı; işletmenin meşru menfaatlerinin korunması ve güvenliğinin sağlanmasıdır. Bunun dışında verilen mal ve hizmet kalitesinin artırılması için de işverenler, işçilerin e-posta kullanımını gözetlemektedir. İşçilerin e-posta üzerinden müşterilerle yaptığı konuşmaların işverenlerce gözetlenmesi sonucunda müşteri ile işçi arasındaki iletişimin daha iyi bir şekilde yönetilmesi ve mal ve hizmet kalitesini arttırılması amaçlanmaktadır (Everett, Wong ve Paynter, 2004, s. 295; Aydemir, 2012, s. 37).

AMA'nın işyerindeki e-postaların gözetlenmesine dair verilerine göre; işçilerinin e-postalarını denetleyen şirketlerin oranı %43 olarak saptanmıştır. Bu şirketlerin %73'ü e-postaların denetlenmesini bir program aracılığıyla gerçekleştirirken, %40'ı ise e-postaların gözetlenmesi için başka bir işçiye görev vermektedir (http-30).

E-postanın kim tarafından gönderilip kim tarafından alındığı, yazılı metnin kaç kelimeden oluştuğu, işçilerin gönderdiği e-postayı yazarken ya da aldığı e-postayı

incelerken harcadığı sürenin ne kadar olduğu ve bu e-postanın ekinde ne tür belgelerin olduğu gibi ayrıntılar işverenlerin e-postayla ilgili gözetim faaliyetinde dikkate aldığı noktaları oluşturmaktadır (İbiş ve Batman, 2014, s. 8).

İşyerlerindeki kamera ile yapılan gözetim faaliyeti hem ortaya çıkabilecek suçların önlenmesi hem de işçilerin çalışma performansının kontrol edilebilmesi için önem taşımaktadır. Cinsel taciz, hırsızlık ve işi aksatma gibi birtakım olumsuz davranışların önüne geçmek, işyerinde güvenliği sağlamak ve işçilerin verimliliğini denetlemek amacıyla işverenler tarafından kamerayla gözetim faaliyeti tercih edilmektedir. İşverenlerce gözetlendiğinin farkına varan işçiler, bu yanlış davranışları yapmaktan sakınmaktadır. Çalışma sırasında kameralarla gerçekleştirilen gözetim faaliyetiyle böylece hem suçun önüne geçilmekte hem de işçi performansı arttırılmaktadır (Aydemir, 2012, s. 46).

AMA tarafından yürütülen araştırmanın kamerayla gözetim faaliyetine ilişkin sonuçlarına göre; araştırma yapılan işyerlerinin %48'inde hırsızlık, şiddet ya da sabotaj riskine karşı gözetim yapılmaktadır. Buna ek olarak işverenlerin %7'si işçilerin çalışma performansını ölçmek amacıyla kamerayla gözetim faaliyetine başvurmaktadır (http-30).

Son olarak, işverenlerin gözetim faaliyetini en kolay biçimde gerçekleştirebildiği cihazın telefon olduğu bilinmektedir. Çalışma ortamında işverenler, işçiler ile müşteriler arasındaki görüşmelerde herhangi bir problem yaşanmaması adına telefonlar üzerinden gözetim yapma yoluna başvurmaktadır. Özellikle turizm ve seyahat sektöründe faaliyet gösteren şirketlerin işverenlerinin, telefonla gözetim yöntemini kullandığı bilinmektedir. Zira bu sektörlerde çalışan işçilerin, müşterileri yanlış anlaması ya da herhangi bir aksilik olması durumunda ortaya çıkan maliyet çok yüksek olmaktadır. Bu nedenle işverenler, işçilerini türlü yöntemlerle gözetlemektedir (İbiş ve Batman, 2014, s. 10).

Telefonla yapılan gözetim faaliyetinin bir diğer amacı, işçilerin telefon görüşmelerinde harcadıkları sürenin tespit edilmesidir. Bununla beraber, işçilerin cep telefonlarına yüklenmiş uygulamalar yardımıyla onların konum bilgilerine erişilebilmesi de mümkün olmaktadır. İşverenlerin, işçilerini bu uygulamalarla gözetliyor olmasındaki en önemli amaç; işyerinin kârının ve işçilerin verimliliğinin arttırılmasını sağlamaktır. Ancak gözetim faaliyeti, işçilerin mahremiyetinin korunması açısından birtakım problemler yaratabilmektedir (Büyük ve Keskin, 2012, s. 57-58).

ABD'de yapılan araştırmalar göstermiştir ki, şirketlerde çalışan işçilerin telefon görüşmelerinin %20'sini işle alakalı olmayan konular oluşturmaktadır. Bu araştırmanın sonucuna göre işverenler, işçilerinin çalışma performansını ve verimliliğini artırmak amacıyla telefon görüşmelerinin gözetimini yapmaktadır. Verimlilik kaybına dair endişelerin yanı sıra; işyeri ve işle ilgili özel bilgilerin diğer şirketlerin ve müşterilerin eline geçmesini önlemek, müşterilerle yapılan görüşmelerin daha kaliteli olmasını sağlamak ve telefon görüşmelerinin yarattığı maddi külfetin önüne geçmek gibi nedenlerle de işverenlerin gözetim faaliyetine başvurduğu bilinmektedir (Aydemir, 2012, s. 43). Benzer şekilde, AMA'nın araştırma sonuçları, telefon kullanılarak yapılan gözetimin yaygınlığı ve işverenlerin kaygıları konusunda fikir vermektedir. İşyerinde yapılan telefon görüşmeleriyle ilgili gözetim verilerine bakıldığında işverenlerin %45'i, işçilerin telefon konuşmalarının sürelerini tespit etmekte ve kimi aradıklarını gözetlemektedir. %16'lık işveren kesimi ise, işçilerinin telefon konuşmalarını kayıt altına almaktadır (http-30).

İşyerinde işverenlerce uygulanan gözetim faaliyetinin amacının üç ana başlık çerçevesinde özetlenebilmesi mümkündür. Bunlardan birincisi; işçinin iş saatlerinde ne kadar çalıştığının ölçülmesiyle ilgilidir. Çağrı merkezinde çalışanların gün içinde kaç kişiyi arayarak görüşme yaptığı, bilgisayar programcılarının çalışma sırasında kaç adet kod girdiği ya da anketörlerin kaç kişiye anket yaptığı gibi veriler toplanıp sayılmaktadır. Gözetimin bu şekliyle işçilerin çalışma performansına dair istatistikler ortaya çıkmaktadır. Gözetimin ikinci türünde amaç, işçilerin işlerine ve çalıştıkları ortama uyum sağlayıp sağlamadığının belirlenmesidir. İşçilerin işyerinde giydiği kıyafetler ve gün içinde kaç kere tuvalet molası verdiği gibi bilgiler kameralar aracılığıyla takip edilmektedir. Gözetimin son amacı ise; işçilerin fizyolojilerinin ve hayat tarzlarının, yaptıkları işe ve dolayısıyla işteki başarılarına nasıl etki ettiğinin anlaşılması adına gözetim uygulanmasıdır. İşçilerin uyuşturucu, sigara gibi zararlı madde kullanımının tespiti için yapılan testler ile işini etkileyecek herhangi bir sağlık problemi olup olmadığının anlaşılması için kolesterol, tansiyon ve diyabet ölçüm testlerinin yapılması bu kategoride değerlendirilmektedir. İşçilerden toplanan bu sağlık verileri, işverenlerce bilgisayarlarda ya da dosyalar içerisinde saklanmaktadır (Saf, 2016, s. 243-247).

İşverenlerin işçilerini gözetleme oranının giderek artış göstermesinin, gözetim araçlarının ve yöntemlerinin gün geçtikçe gelişmesiyle doğru orantılı olduğu

söylenebilmektedir. Sanayi Devrimi döneminde işçilerin başındaki usta başı ya da işverenler tarafından izleme yöntemiyle yapılan gözetimin yerini siber gözetim araçları almaktadır. Siber gözetim faaliyetinde kullanılan araçlar ise, teknolojik gelişmeler doğrultusunda yaygınlaşmakta ve gelişmektedir. Teknolojinin etkisiyle siber gözetim araçları gün geçtikçe daha az görülebilir, daha minimal boyutlarda üretilen araçlar halini almaktadır. İlk üretildiği yıllarda ağır ve büyük bir kutu boyutundaki kameralar günümüzde bir kalemin içerisine yerleştirilebilir boyutlarda üretilmektedir dolayısıyla işçilerin gözetimi gün geçtikçe kolay bir hal almaktadır. Bununla birlikte bilgisayar, internet ve e-posta gibi siber gözetim araçlarının işverenler tarafından işyerlerinde kullanılması yaygınlaşmıştır. Bu nedenle işverenler, işyerinde güvenliği sağlayabilmekte ve işçilerin çalışma performansını denetleyebilmektedir (Weckert, 2005, s. 23).

Sonuç olarak, siber gözetim faaliyetiyle işyerinin verimliliği ve güvenliği işverenler tarafından sağlanabilmektedir. Teknolojide meydana gelen gelişmelerle birlikte işçiler, bilgisayar ağları üzerinden işyerine gelmelerine gerek kalmadan işlerini yapabilmektedir (Canbey – Özgüler, 2018, s. 381). Bu açıdan işverenlerin, işçinin denetimini yapması hem zorlaşmış hem de işçiye işini yapması için tahsis edilen bilgisayar ve telefon gibi cihazların kötüye kullanması gibi problemler meydana gelmiştir. Dolayısıyla işverenler için siber gözetim faaliyeti işyerinin ve işçinin korunması amacıyla gereklidir. Bunun yanı sıra işçiler açısından bakıldığında ise, özel hayatın gizliliği ve mahremiyet bağlamında bu gözetim faaliyetinin birtakım problemlere yol açabileceği düşünülmektedir. Bu nedenle işçinin, siber gözetime karşı yasalarla korunma altına alınması gerekmektedir (Goldfrey, 2000, s. 19; Weckert, 2005, s. 23).

2. ULUSLARARASI BELGELER İLE KARŞILAŞTIRMALI HUKUKTA İŞYERİNDEKİ SİBER GÖZETİM MEKANİZMALARINA YÖNELİK YASAL DÜZENLEMELER

Siber gözetim faaliyetinin en önemli parçasını işçilere ait veriler oluşturmaktadır. Kimliği belirlenmiş ya da belirlenmesi mümkün olan bireylere ait kişisel verilerin, siber gözetim faaliyeti kapsamında korunması büyük bir gerekliliktir.

Modern hukuk sisteminin ana hattını meydana getiren en önemli kavram, insanın kişiliğinin ve kişiliğine ait haklarının savunulması ve müdafaa edilmesidir. Kişilere ait bilgilerinin korunmasıyla mahremiyet ve özel hayatın gizliliği sağlanmış olmaktadır. Kişisel verilerin korunması bu çerçevede, insanların sahip olduğu en temel hak ve özgürlüklerden biri olarak kabul görmektedir (Bük, 2015, s. 7; Oğuz, 2013, s. 2-3).

Kişisel verilerin korunması ile özel hayatın gizliliğinin sağlanması ve muhafaza edilmesi birbirinden ayrı düşünülemeyecek kadar iç içedir. "Özel hayatın gizliliğinin sağlanması" kişisel bilgi mahremiyeti kavramını karşılamaktadır. Buradan hareketle, özel hayatın gizliliğinin en temel parçasının kişisel verilerin korunması ilkesi olduğu söylenebilmektedir (Bük, 2015, s. 32-33).

24/10/1995 tarihli ve 95/46/EC sayılı "Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Yönelik Bireylerin Korunması Hakkındaki Avrupa Birliği ve Avrupa Parlamentosu Direktifi", "Tespit edilmiş ya da tespit edilebilir durumda olan kişilerin bilgilerini kişisel veriler olarak açıklamaktadır (95/46/EC sayılı Direktif, m.2)". Yalnızca kâğıt üzerindeki yazılardan oluşan bilgiler değil aynı zamanda rakamlar, grafikler, fotoğraflar ya da ses kayıtları gibi elektronik cihazlar aracılığıyla toplanabilen bilgiler de kişisel veri kavramının içerisine dahil edilmektedir (http-32). Nitekim, siber gözetim faaliyetinin gerçekleştirilmesi sırasında işçilere ilişkin verilerin toplanması, işlenmesi ve kullanılması kişilik haklarını esas alan bir uygulamayı nitelendirmektedir. İşçilerin bilgilerinin muhafaza edilmesiyle onların; kişisel değer, onur ve saygınlığı gibi manevi unsurlarını temsil eden haklarının savunulması birbiriyle ilişki içerisindedir (Oğuz, 2013, s. 2; Önok, 2013, s. 1230; Bölükbaş, 2014, s. 48).

Siber gözetim faaliyetiyle kişisel veriler arasında önemli bir bağ vardır. Siber gözetim faaliyetini gerçekleştiren işverenler, belirli bazı amaçlar doğrultusunda işçileri hakkındaki verileri toplamaktadır. İşletmenin ve işçinin verimliliğinin artması, işçilerin cinsel taciz ve hırsızlık gibi istenmeyen olaylara karşı korunması ya da işçilerin çalışma performansının değerlendirilmesi için işverenlerin siber gözetime başvurduğuna önceki

bölümde değinmiştik. İşyerinde kamera sistemleriyle işçilerin görüntülerinin depolanması, bilgisayar üzerinden ziyaret ettiği sitelerin hangileri olduğuna bakılması ve e-posta yazışmalarının okunması işçinin kişisel verilerine erişim olarak kabul edilmektedir (Lyon, 2006'dan aktaran Bölükbaş, 2014, s. 46). Kişisel veriler, kişiyle ilgili her türlü bilgiyi nitelendirdiği ve siber gözetim faaliyeti de kişisel verilerin elde edilmesiyle bağlantılı olduğundan, siber gözetim faaliyetine yönelik özellikle hazırlanmış hukuki düzenlemelerin olmaması durumunda, kişisel verilerle ilgili hukuki düzenlemelere yer verilecektir.

İşverenlerin işçilerini gözetlemesi faaliyeti öncelikle bağlılık, sadakat, güven ve işverenin birtakım haklı çıkarları olarak kabul edilmiş ve böylece siber gözetim faaliyeti meşrulaştırılmıştır. Özellikle günümüzde teknolojik gelişmelerin ilerlemesi sonucunda işverenlerce yürütülen bu siber gözetim faaliyeti, insan haklarının korunmasına yönelik bir tehdit oluşturmuştur. İşçilerin mahremiyet alanının müdafaa edilmesi amacıyla bazı uluslararası ve ulusal belgeler yürürlüğe sokulmuş, buna ek olarak birçok ülke de kendi mevzuatında birtakım düzenlemeler yapmıştır (Tabak ve Konukpay, 2018, s. 118).

Çalışmanın bu bölümünde, ilk olarak uluslararası belgelerde siber gözetim faaliyetine yönelik yasal düzenlemelere yer verilecek, ardından karşılaştırmalı hukukta siber gözetim faaliyetine ilişkin mevcut düzenlemeler anlatılacaktır.

2.1. Uluslararası Belgelerdeki Yasal Düzenlemeler

2.1.1. Ekonomik Kalkınma ve İş Birliği Örgütü (OECD)

İkinci Dünya Savaşı sona erdiğinde Avrupa'nın ekonomisinin canlandırılması amacıyla 1948 yılında Avrupa Ekonomik İş Birliği Örgütü (Organisation for European Economic Cooperation – OEEC) kurulmuştur. OEEC'nin hedefi; Marshall Planı çerçevesinde ABD ve Kanada'nın on iki milyar dolar tutarındaki yardımını Avrupa ülkelerine dağıtmak ve Avrupa ülkeleri arasındaki ödemelerin serbestleştirilmesini ve geliştirilmesini sağlayarak Avrupa'nın ekonomisini düzeltmektir. Ancak 1960'lı yıllara gelindiğinde OEEC, işlevini yitirmiştir (http-33). Bunun üzerine 14 Aralık 1960 tarihinde Paris'te "Convention on the Organisation for Economic Co-operation and Development" adında bir sözleşme imzalanmıştır. İmzalanan bu sözleşme, 30 Eylül 1961 tarihinde kurulan OECD'nin kurucu sözleşmesi olarak bilinmektedir (http-34). OECD'nin amacı ise, kurucu sözleşmesinin birinci maddesinde yer almaktadır. Buna göre "OECD; üye ülkelerin ekonomisinin gelişmesini, bu ülkelerdeki halkların daha yüksek standartlarda refah içinde yaşamasını ve böylece dünya çapında ekonominin

yükselmesini hedeflemektedir". Merkezi, Fransa'nın Paris şehrinde olan OECD'nin günümüzde otuz altı üye ülkesi vardır. Ülkemiz ise, OECD'nin yirmi kurucu ülkesinden biri olma özelliğini taşımaktadır (http-35).

OECD tarafından, 23 Eylül 1980 tarihinde "Özel Hayatın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler" adıyla oluşturulan konsey tavsiyesinde, kişilere ait verilerin muhafaza edilmesinin ekonomik anlamdaki önemi üzerinde durulmuştur. Bu ilkeler altı ana bölümden oluşmuştur. Bu bölümler sırasıyla; kişisel veriler hakkında genel hükümler, ülkelerin ulusal uygulamalarına ilişkin temel prensipler, uygulamaya ilişkin sorumluluklar, bu ilkelerin uygulanmasının ana prensipleri – veri akışı ve birtakım yasal kısıtlamalar, ülkelerin kendi mevzuatına göre uygulanması ve uluslararası çalışma ortaklığıdır (http-36; Şimşek, 2008, s. 13).

Bu tavsiyenin birinci maddesinde; verilerin denetimini yapan kişilerin, kişisel verinin, mahremiyetin korunmasına ilişkin kanun ve düzenlemelerin, mahremiyeti uygulama makamının ve sınır ötesi kişisel veri akışı kavramlarının tanımı yapılmıştır. Kişisel verileri elde eden kişiler; "Bir araç yardımıyla bilgileri elde eden, depolayan, istediğinde bu verilerin işlenmesini sağlayan ve verilerin kullanılmasında yetki sahibi olanlar" şeklinde tanımlanmıştır. "Kişilere ait olan, açıklanmış ya da açıklanabilir durumdaki her türlü bilgi" ise kişisel verinin karşılığı olarak verilmiştir. Mahremiyetin korunmasına ilişkin hazırlanan kanun ve düzenlemeler ile ülkelerin, bu tavsiye ilkeleriyle uyumlu olarak hazırlanmış mevzuat kastedilmektedir. Mahremiyeti uygulama makamı, "Ülkelerin kendi oluşturduğu ve kişisel verilerin gizliliğine ilişkin yasalar ile düzenlemeleri uygulama yetkisini elinde bulunduran kamu organı" olarak tanımlanmaktadır. Son olarak; sınır ötesi kişisel veri akışı kavramı ise; "Kişilere ait bilgilerin ülke sınırları dışındaki bir kişiye ya da kuruma iletilmesi" şeklinde verilmiştir (http-36).

Bu tavsiye metninin 7 ila 14. maddeleri arasında sekiz başlıktan oluşan ilkeler verilmiştir:

1. İlke: Sınırlı Haldeki Verilerin Toplanması İlkesi
2. İlke: Verilerin Kalitesine Yönelik İlke
3. İlke: Verilerin Amaca Uygun Özellik Taşıması İlkesi
4. İlke: Verilerin Kullanımına Yönelik İlke
5. İlke: Güvenlik Tedbirlerine Yönelik İlke
6. İlke: Açıklık İlkesi

7. İlke: Bireyin İştirak Etmesine Yönelik İlke

8. İlke: Hesap Verilebilirlik İlkesi.

Bu ilkelerden birincisi; sınırlı haldeki verilerin toplanmasına ilişkin ilkedir. Kişiden veri toplama sırasında yasal yolların kullanılması ve kişinin rızası alınarak hakkındaki bilgilerin elde edilmesi gerektiğine ilişkin ilke 7. maddede açıklanmaktadır. 8. maddede yer alan ikinci ilke; verilerin kalitesine yöneliktir. İkinci ilkeyle, toplanacak olan kişisel bilgiler amacına uygun olarak seçilmesi; eksiksiz bir biçimde, dürüst ve aktüel içeriğe sahip olması gerektiği belirtilmiştir. Üçüncü ilke, verilerin amaca uygun özellik taşımasıyla ilgili olan 9. maddede yer almaktadır. Veriler hangi amaca hizmet etmek için toplanıyorsa, sadece o amaca uygun nitelikteki bilgilerin alınması önerilmektedir. Burada önemli olan, kişisel bilgileri toplanan bireyin rızasının olması ve bu işlemin yasaların yetkisi çerçevesinde gerçekleştirilmesidir. Verilerin kullanımına yönelik ilke olan dördüncü ilke, 10. madde çerçevesinde açıklanmaktadır. Kişisel bilgiler dördüncü ilkeye göre işlevinin dışında depolanamaz, işlenemez ya da başkalarına iletemez konumdadır. Verilerin sahibinin rızası varsa ya da kanunlar bu yetkiyi vermişse, bu durumda bir istisna meydana gelebilmekte ve verilerin işlenmesi mümkün olabilmektedir. Beşinci ilke olan güvenlik tedbirleri ilkesi, 11. maddede düzenlenmiştir. Beşinci ilkeye göre; bahsi geçen kişisel bilgilerin kaybolması, çalınması ya da başkaları tarafından açığa çıkartılması gibi olumsuzluklara karşı, verileri toplayan kişilerce korunması gerektiği belirtilmiştir. Altıncı ilkeye dair düzenlemeler, bu tavsiye metninin 12. maddesinde yer almaktadır. Açıklık ilkesi olarak bilinen altıncı ilkeye göre verileri toplanan bireyler; istedikleri zaman, verilerini toplayan kişilerin, kurumların ya da kuruluşların kimliğini ve adresine erişebilmelidir. Yedinci ilke, bireyin iştirak etmesine dayanan ilkedir. 13. madde içerisinde açıklanan bu ilke uyarınca; bireyin izin vermediği durumlarda, kendine ait bilgilerin hiç kimseyle paylaşılmadan saklanması gerekmektedir. 14. maddede verilmiş olan sekizinci ilke ise; hesap verilebilirlik ilkesidir. Sekizinci ilkeyle birlikte verilerin sahiplerinin, kişisel bilgilerini toplayıp depolayan kişilere hesap sorabilmesi mümkün kılınmıştır. Bu ilkelerin tamamıyla işyerinde çeşitli araçlar yardımıyla gözetim faaliyetine maruz kalan işçilerin kişisel verilerinin ve özel hayatlarının gizliliği hakkı koruma altına alınabilmektedir (http-36; Bölükbaş, 2014, s. 49-51).

OECD'nin sözü edilen bu ilkeleri, üye devletlerin uygulamasını zorunlu kılan bağlayıcılığa sahip olmamakla birlikte, tavsiye kararı niteliğindedir. Bu tavsiye

kararıyla amaçlanan, öncelikli olarak kişisel bilgilerin korunmasının sağlanmasıdır. Bunun yanı sıra ülkelerin, veri korumasına dair hazırlayacakları kendi ulusal düzenlemelerinde bu tavsiye kararını benimseyerek hareket etmeleri amaçlanmaktadır. Bu anlamda OECD yayınladığı bu tavsiye kararıyla minimum düzeydeki ilkeleri belirlemiş, ayrıntıların düzenlenmesi için hem uluslararası alanda hem de ülkelerin mevzuatlarının düzenlenmesinde öncü olmuştur (Uncular, 2012, s. 15).

Bu tavsiye kararının hemen sonrasında, 1985 yılı itibarıyla, OECD ülke bakanları "Sınır Ötesi Veri Akışı" hakkında bir bildiriyi onaylamıştır (http-37). 1997 yılında gelindiğinde "Şifreleme Politikasına İlişkin Kılavuz İlkeler" kabul edilmiştir (http-38). Bundan bir yıl sonra, 1998'de Kanada'nın Ottawa kentinde gerçekleştirilen bir konferansta "Küresel Ağlarda Gizliliğin Korunması" hakkında bir başka bildiri kabul edilmiştir (http-39). 2000 yılında kişisel bilgilerin taranmasıyla, mahremiyet politikasına ilişkin bir bildiri geliştirilmesine yönelik çevrimiçi kullanılan bir cihaz tasarlanmıştır. Teknolojik gelişmelerle birlikte bu cihaz yetersiz kaldığı için on yıl sonra kullanımına son verilmiştir (http-40; Şimşek, 2008, s. 14-15).

Son olarak, 2002 yılında "Bilgi Sistemlerinin Güvenliğine İlişkin OECD Rehber İlkeleri: Güvenlik Kültürüne Doğru" isimli tavsiye kararı yayınlanmıştır. Bu yönergeyle; bilgi sistemi ve bilgi ağının kullanım oranının günden güne artmakta olduğu, ağ sisteminin ve verilerin korunmasına önem verilmesi gerektiği ve dolayısıyla emniyetin sağlanması açısından ne tür bir yöntem geliştirilebileceği hakkında bir tavsiye kararı sunulmuştur. Bu tavsiye kararı, dokuz temel ilkeyi içermektedir (Önok, 2013, s. 1240; http-41).

1. İlke: Bilinç
2. İlke: Mesuliyet
3. İlke: Reaksiyon
4. İlke: Etik
5. İlke: Demokrasi
6. İlke: Risk Değerlendirmesi
7. İlke: Emniyetin Tasarlanması ve Uygulanması
8. İlke: Emniyet Yönetimi
9. İlke: Değerlendirmenin Tekrarlanması

Bu dokuz ilke sırasıyla açıklanmıştır. Birinci ilke ele alındığında, veri sistemi ve ağlarının emniyetini sağlayabilmek için, bu sistemi kullananların ortak bir bilinçle

hareket etmesi gerektiği belirtilmektedir. İkinci ilkeyle, sistemi kullananların güvenli bir ortamı oluşturma açısından sorumlu oldukları dile getirilmektedir. Üçüncü ilke incelendiğinde görülmektedir ki; veri ağı ve sistemini kullananların, olası bir risk durumuna karşın birlikte hareket ederek geç kalmadan tepki vermeleri gerekmektedir. Bunlar uygulandığı sırada kullanıcılar, diğer kişilere ve onların menfaatlerine saygı göstermelidir. Dördüncü ilke gereğince kişisel verileri işleyen kişi ile kişisel veri sahibi olan kişi birbirinin çıkarlarını koruyarak saygı çerçevesinde hareket etmekle yükümlüdür. Veri ağı ve sistemlerinin emniyeti sağlanırken, ülkelerin kendi demokrasilerine uygun bir biçimde hareket etmelerinin gerekliliği beşinci ilkenin içeriğini oluşturmaktadır. Böylece, bahsi geçen bu ağ sistemlerin ne türde riskleri olabileceğinin değerlendirmesinin de yapılması önerilmektedir. Altıncı ilke uyarınca, sistemi kullananlar tarafından sebebiyet verilebilecek ya da sistemi kullananları etkileyebilecek risklerin kolaylıkla tespit edilebileceği ifade edilmektedir. Yedinci ilkeye göre, emniyetin sağlanması; veri sistemleri ve ağlarını kullanan kişilerce en önemli öge olarak ele alınmalıdır. Sekizinci ilke bağlamında; veri ağı ve sisteminde oluşabilecek herhangi bir tehdit, problem, aksama ya da bozulma gibi olumsuz durumlara karşı bir tutum oluşturulmasının gerekliliği belirtilmiştir. Sonuncu ilke ise; veri sistemi ve ver ağını kullananların aralıksız bir biçimde güncelleme yapmalarını önermektedir. Değişen koşullara uyum sağlayarak risklere karşı durulabilmesi için sistemin incelenerek güncelleştirilmesi ihtiyacı doğmaktadır (http-41).

OECD'nin ilgili bu tavsiye kararı, kişisel verilerin korunması konusunda düzenlenmiş ve tavsiye niteliği taşıyan ilk uluslararası belge olmakla birlikte, beklenenden daha az derece rağbet görmesi sonucunda, oluşturulan başka uluslararası metinlerle desteklenmiştir (Uncular, 2014, s. 29-30).

2.1.2. Birleşmiş Milletler (BM)

1945 yılında İkinci Dünya Savaşı'nın sona ermesiyle birlikte 24 Ekim 1945 tarihinde, savaşın yarattığı olumsuz ve kötü atmosferin tekrarlanmasını önlemek amacıyla BM Şartı'nın imzalanarak kabul edilmesiyle BM kurulmuştur (http-42). 2019 yılı itibarıyla yüz doksan üç üyesi olan BM'nin misyonu insanların temel hak ve özgürlüklerini her daim korumak ve geliştirmektir (Uncular, 2014, s. 35).

10 Aralık 1948 tarihine gelindiğinde, "BM Evrensel İnsan Hakları Bildirisi" kabul edilmiştir. Bu bildirinin en önemli özelliği, temel insan hak ve özgürlüklerinin dünya çapında uygulanıp korunmasını sağlayacak standartları belirlemiş olmasıdır. Otuz

maddeden oluşan bu Bildiri'nin 12. maddesi bağlamında özel hayatın gizliliği hakkı ele alınmıştır. Bu maddeye göre; "Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı kanunlar tarafından korunmaya hakkı vardır (BM Evrensel İnsan Hakları Bildirisi, m. 12)". Ancak bu Bildiri, üye ülkeleri hukuki anlamda bağlayıcı bir özelliğe sahip olmamakla birlikte, kılavuz niteliğindedir (Sevimli, 2006, s. 36; Küzeci, 2010, s. 132).

BM Evrensel İnsan Hakları Bildirisi'nin bir sözleşme haline getirilebilmesi için yapılan çalışmalar sonucunda; "Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşmenin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu", 19 Haziran 1966 tarihinde kabul edilerek 23 Mart 1976'da uygulamaya konmuştur (Sevimli, 2006, s. 37). Türkiye tarafından 15 Ağustos 2000 tarihinde imzalanan bu sözleşme elli üç maddeden oluşmaktadır (http-43).

Kişilerin özel hayatına ilişkin düzenleme, sözleşmenin 17. maddesinde iki fıkra halinde yer almaktadır. Bu maddenin birinci fıkrası uyarınca; "Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz (Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme, m. 17/1)". İlgili maddenin ikinci fıkrasına göre ise; "Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir (Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme, m. 17)". Bu sözleşmeyi kabul ederek imzalayan bütün ülkelerin, ulusal yasalarını bu sözleşmeye uygun olarak düzenlemesi gerekmektedir (Sevimli, 2006, s. 37; Korkmaz, 2017, s. 141).

1985 yılına gelindiğinde BM tarafından, kişilere ait verilerin korunmasına yönelik bir belge hazırlanmasına karar verilmiştir. 14 Aralık 1990 tarihi itibarıyla, "Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler" isimli tavsiye özelliğini taşıyan yönerge yürürlüğe girmiştir. Toplam on ilkeden oluşan Rehber İlkeler'in imzalanmasındaki temel amaç; üye ülkeleri mevzuatında kişisel verilerin korunmasına yönelik düzenlemeler yapması için teşvik etmek ve böylece kişilerin haklarının korunmasını sağlamaktır (http-44).

Bu ilkelerden birincisi uyarınca; kişilere ait verilerin meşru ve adil bir yöntem izlenerek elde edilmesi ve BM Şartı'nda bulunan ilkeler dışındaki amaçlara hizmet etmemesi gerektiği belirtilmiştir (http-44; Şimşek, 2008, s. 16; Küzeci, 2010, s. 135).

İkinci ilkede, bilgisayarlar aracılığıyla kişilere ait bilgileri toplayıp depolayanlara birtakım sorumluluklar yüklenmiştir. Buna göre verileri toplayanların verilerin doğru olup olmadığını kontrol etmesi, var olan eksiklikleri gidermesi ve düzenli ve güncel bir biçimde depolaması tavsiye edilmiştir (Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler, m. 2).

Üçüncü ilkeye göre, kişisel verilerin toplanması yalnızca belli bir amaç çerçevesinde mümkün olabilmektedir. Belirlenmiş meşru bir amaç dışında kişisel verilerin toplanması yasaktır. Bu amacın geçerli olduğu süre sona erdiğinde ise kişisel verilerin toplanması, kullanılması ya da başkalarına dağıtılması üçüncü ilkeyle engellenmiştir. Aynı zamanda verilerin sahibinin onayı ve rızası doğrultusunda veri işleme yapılabilmektedir. Veri sahibinin izni olmadığı durumda verilerin kullanılması mümkün değildir (Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler, m. 3).

Dördüncü ilke gereğince, hangi milletin vatandaşı veya hangi ülkede yaşıyor olursa olsun kimliğiyle verilerin sahibi olduğunu kanıtlayan bireyler, kendilerine ait olan bilgilerin toplanıp kaydedildiğini öğrenme hakkına sahiptir. Kişiler, bu bilgilerin yanlış ya da yasalara aykırı olduğunu düşünüyorsa böyle bir durumda verilerin silinmesini ya da değiştirilmesini talep edebilmektedir (Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler, m. 4).

Beşinci ilke, kişiler arasında yapılan ayrımcılığı önlemek adına düzenlenmiştir. Altıncı ilkedeki istisnai durumlar dışında kişinin; milliyeti, konuştuğu dili, mensup olduğu dini, siyasi görüşleri, değerleri, inançları ve hangi sendikaya üye olduğu gibi ayrımcılık yaratacak verileri toplanamaz ve işlenemez (Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler, m. 5).

Altıncı ilke uyarınca, ilk dört ilkenin uygulamasında bazı istisnai durumlar meydana gelebilmektedir. "Halkın düzeni ile refahının, sağlığının, ahlakının, güvenliğinin ve bireylerin kişisel hak ve özgürlüklerinin korunması amacıyla oluşan birtakım istisnai durumlarda ülkeler, mevzuatlarında uygun düzenlemeleri yapmakla ve vatandaşlarını korumakla yükümlüdür (Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler, m. 6)".

Yedinci ilkede; kişilere ait bilgilerin kaybolması, başkaları tarafından bu bilgilere erişim sağlanması, bilgilerin kötüye kullanılması ve depolandığı bilgisayarlara virüs bulaşması gibi olumsuzluklara karşı tedbirlerin alınması tavsiye edilmektedir

(Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler, m. 7).

Sekizinci ilke uyarınca, bu Rehber İlkelere uyulup uyulmadığını denetleyecek bir kurulun oluşturulması gerekmektedir. Bu kurul, tarafsız bir biçimde hareket etmek koşuluyla kişisel verilerin korunmasında rol oynayacak ve ülkelerin bu konudaki düzenlemelerinin ihlal edilmesi durumunda gerekli cezaların verilmesini sağlayacaktır (Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler, m. 8).

Kişisel verilerin korunması ve özel hayatın gizliliğine dair düzenlemelere sahip olan ülkeler arasında kişisel veri aktarımı yapılabilmesi mümkündür. Veri aktarımı dokuzuncu ilkede belirtilmiştir. Kişisel verilerin korunması konusunda yeterli derecede düzenlemenin bulunmadığı ülkelerde ise kişinin özel hayatının gizliliğinin korunması esastır (Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler, m. 9).

Sonuncu ilkeye göre ise, yapılan düzenlemeler özel ve kamu sektörü ayrımı olmaksızın tüm alanlarda hem bilgisayarlarla yapılan hem de elle yapılan veri kaydetme işlemi bağlamında geçerliliğe sahiptir. Bunun yanı sıra, onuncu ilkede belirtildiği üzere bilgisayarla işlenen verilerin korunması gereklidir (Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler, m. 10).

Rehber İlkeler'in sekizinci ilkesi uyarınca, yapılan bu düzenlemelere uyulup uyulmadığının denetlenmesi için ülkelerin bağımsız bir kurul kurmasının gerekliliği üzerinde durulmuştur (Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler, m. 8). Kişisel verilerin ve özel hayatın gizliliği hakkının korunmasını denetlemek amacıyla bağımsız ve yetkili bir kurul oluşturulması anlamında bu Rehber İlkeler, ilk uluslararası belge olma özelliğine sahiptir (Küzeci, 2010, s. 136).

BM'nin bu Rehber İlkeleri'nde özellikle işyerindeki siber gözetim faaliyetine yönelik düzenleme bulunmamaktadır. Onuncu ilkede de belirtildiği üzere, bilgisayarlarla toplanan ve işlenen kişisel verilerin korunması bu Rehber İlkeler kapsamında değerlendirilmektedir. Böylece işyerinde işverenler tarafından bilgisayarla uygulanan gözetim faaliyetinin de bu düzenlemelerle korunma altında olduğu sonucu çıkmaktadır.

Bu Rehber İlkeler; OECD'nin Rehber İlkeleri ve AK Sözleşmesi gibi diğer uluslararası belgelerle kıyaslandığında, üye ülkeler için tavsiye kararı niteliğinde olması

sebebiyle kişisel verilerin korunmasında daha az etkili olmuştur. Nitekim OECD'nin Rehber İlkeleri de tavsiye kararı olma özelliğine sahiptir. Ancak kişisel verilerin ve özel hayatın gizliliğinin korunması bağlamında düzenlenmiş ve tavsiye niteliği taşıyan ilk uluslararası belge olması açısından önemli bir yere sahiptir (Korkmaz, 2017, s. 142; Küzeci, 2010, s. 136).

2.1.3. Uluslararası Çalışma Örgütü (ILO)

ILO, Birinci Dünya Savaşı'nın sona ermesinin hemen ardından 1919 yılında Versailles Barış Anlaşması'yla kurulmuştur. 1946 yılı itibarıyla ise ILO, BM'nin ilk uzman kuruluşu olmuştur. Kuruluş amacı, dünya çapında sürekli olarak barış ortamının kalıcılığının sağlanması olmuştur. ILO'nun görevleri arasında; çalışma hayatına dair belirli standartların oluşturulmasıyla kişinin temel hak ve özgürlüklerinin korunması ve kişilerin insan onuruna yaraşır bir biçimde çalışmasının sağlanması bulunmaktadır (http-45 ve http-46).

Yüz seksen yedi üye ülkeden oluşan ILO'nun merkezi İsviçre'nin Cenevre şehridir. ILO, çalışma hayatına ilişkin standartları belirlerken sözleşmelerden ve tavsiye kararlarından yararlanmaktadır. 2019 yılının temmuz ayı itibarıyla ILO'nun düzenlediği yüz doksan sözleşmesi ve iki yüz altı tavsiye kararı bulunmaktadır. Üye ülkelerin kabul ettiği ILO sözleşmeleri, o ülke için bağlayıcı bir nitelik taşımaktadır. Ancak tavsiye kararları, üye ülkeler açısından herhangi bir bağlayıcı niteliğe sahip değildir. Üye ülkeler için tavsiye kararları, o ülkenin çalışma alanında yer alan düzenlemeleri tamamlayıcı özellikte kabul edilmektedir (Nurdoğan, 2018, s. 84). 18 Temmuz 1932 tarihinde ILO'ya üye olan Türkiye tarafından, bugüne kadar elli dokuz sözleşme onaylanmıştır. Ancak bu sözleşmelerden elli beş tanesi yürürlüğe girmiştir (http-47).

OECD ve BM gibi uluslararası kuruluşların kişilere ait bilgilerin ve özel hayatın gizliliğinin korunması bağlamında yapmış olduğu düzenlemeler önceki bölümlerde tarafımızca incelenmişti. Bu anlamda ILO'nun, işverenler tarafından işyerinde uygulanan siber gözetim faaliyetine yönelik herhangi bir sözleşmesi mevcut değildir (Tekergül, 2010, s. 25). Kişisel verilerin gizliliğinin korunması ve çalışma esnasında siber gözetim faaliyetiyle elde edilen işçilere ait bilgilerin güvenliğinin sağlanması amacıyla 1996 yılının Kasım ayında ILO tarafından, "Çalışanların Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu" imzalanmıştır. On üç maddeden oluşan bu kodun amacı, işçilere ait kişisel bilgilerin korunmasını sağlamak olarak 2. maddede açıklanmıştır (http-48).

ILO'nun bu Uygulama Kodu'nun 3. maddesinde kişisel veri, kişisel verilerin işlenmesi, gözetim ve işçi kavramlarının tanımlarına yer verilmiştir. Buna göre kişisel veri; "Kimliği belirlenmiş ya da belirlenebilir olan işçiler hakkındaki bilgi" anlamını taşımaktadır. "İşçilere ait bilgilerin çeşitli araçlar yardımıyla elde edilmesi, kayıt altına alınması, başka kaynaklara aktarılması ve kullanılması" kişisel verilerin işlenmesi olarak tanımlanmıştır. Gözetim kavramı; "Bilgisayar, internet, telefon, kamera, ses kayıt cihazı ve diğer iletişim araçlarının kullanılmasıyla kişinin kimliğinin ve konumunun belirlenmesi ya da kişinin kendisinin izlenmesi faaliyetidir" şeklinde verilmiştir. 3. maddede yer alan son tanıma göre; "Eskiden işyerinde çalışmış, gelecekte işyerinde çalışacak veya şu anda çalışıyor olan kişilere işçi denmektedir (Çalışanların Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu, m. 3)".

4. maddede Uygulama Kodu'nun kapsamı ele alınmıştır. Bu belgede yer alan hükümler özel ya da kamu sektörü ayırt edilmeksizin tüm kurum ve kuruluşlarda geçerli olacaktır. Aynı zamanda toplanan verilerin yalnızca elektronik araçlar yardımıyla toplanması şartı da aranmamaktadır. İşçilerin verileri bir kişi tarafından elde yazılarak dosyalanmış olsa bile bu belgedeki düzenlemeler kapsamında korunmak durumundadır (Çalışanların Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu, m. 3).

Uygulama Kodu'nun 5. maddesinde genel ilkeler başlığı altında on üç fıkraya yer verilmiştir. Söz konusu fıkralardaki düzenlemelerin kısaca özetlenmesi yerinde olacaktır. Birinci fıkraya göre, işçilere ait veriler yalnızca işle ilgili sebeplerle toplanmalı ve kullanılmalıdır. 2. fıkra uyarınca işle ilgili hangi amaç doğrultusunda işçinin verileri toplanmışsa, o amaca uygun bir biçimde bu veriler kullanılmalıdır. 3. fıkraya göre işçiye ait veriler eğer işin kendisiyle ilgili bir amaç için kullanılmayacaksa işveren, bu verilerin yanlış kullanılmasını önlemek amacıyla tedbirler almalıdır. 4. fıkrada, kişisel verilerin toplanmasını sağlayan otomatik veri sistemlerinin güvenliğinin sağlanması ve hata yapmadan çalışması için elde edilen kişisel verilerin, işçi davranışlarını kontrol altında tutma amacıyla kullanımı yasaklanmıştır. İşverenin işçi hakkında bir karar vermesi esnasında, sadece gözetim faaliyetiyle elde ettiği bilgileri baz almaması gerektiği ve aynı zamanda işçilerin performanslarının yalnızca gözetim faaliyeti sonucunda ortaya çıkan veriler üzerinden değerlendirilmemesi ise 5. ile 6. fıkralar uyarınca belirtilmiştir. 7. fıkra bağlamında işverenler, işçilerden mümkün olduğunca az miktarda veri toplamalı ve işçilerin özel hayatının gizliliğinin korunması adına özen göstermelidir. İşçilerin ise, kendilerine ait bilgilerin toplandığını bilme hakkı

olduğu 8. fıkrada belirtilmiştir. Buna göre, işverenler işçilerinden veri topluyor olduklarında işçilerini bilgilendirmek durumundadır. İşverenler 9. fıkra uyarınca, veri toplama görevini bir başka işçiye vermişse bu durumda, veri toplama işlemini yürüten kişiye sistematik olarak eğitim verme yükümlülüğü altındadır. 10. fıkraya göre işverenler, işçilerine ait bilgileri çalışma esnasında ayrımcılık yapma amacıyla kullanmaktan kaçınmak durumundadır. İşverenlerin, işçilerinin mahremiyet hakkını korumak için bu Uygulama Kodu'na uygun bir politika geliştirmesi gerekliliği ve işverenler, işçiler, İş Bulma Kurumu ve işçi temsilcilerinin ortak çalışmasıyla işçilerin mahremiyeti hakkını koruması 11. ve 12. fıkralarda ele alınmıştır. Sonuncu fıkra uyarınca ise, işçilerin sahip olduğu bu mahremiyet hakkından vazgeçmesi söz konusu olamayacaktır (Çalışanların Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu, m. 5).

ILO'ya ait Uygulama Kodu'nun 6. maddesinde, işçilere ait verilerin toplanmasına ilişkin düzenlemeler on dört fıkrayla verilmiştir. Bu fıkralardan işyerinde siber gözetim faaliyetiyle ilgili olanların incelenmesi, işçilerin verilerinin toplanmasına dair düzenlenmelerin anlaşılması açısından faydalı olacaktır. Birinci fıkra uyarınca, toplanacak olan kişisel verilerin yalnızca işçilerden toplanması gerektiği belirtilmiştir. 2. fıkraya göre, herhangi bir üçüncü kişiden işçiye ait kişisel veri toplanması gerekiyorsa, bu durumda hem işçinin bilgilendirilmesi hem de rızasının alınması gerekmektedir. Bahsedilen bu üçüncü kişi; bir işçi, başka bir kişi ya da bir kurum olabilmektedir. 3. fıkra uyarınca eğer işveren, üçüncü kişilerin veri toplaması için işçinin onay verdiğine dair bir belge imzalamasını talep ederse, bu belgede verileri kimin toplayacağını, veri toplamadaki amacın ne olduğunu ve ne kadar süre boyunca verilerin toplanacağını açıkça bu belgede belirtmek durumundadır. 4. fıkraya göre kişisel verilerin toplanması amacıyla işçisinden onay almış olan işveren, bu verileri toplayacak üçüncü kişilerin daima açık ve net bir biçimde veri toplama işlemini gerçekleştirmesini sağlamakla yükümlüdür. 5. fıkrada işçilere ait hangi bilgilerin işverenler tarafından toplanmasının uygun olmadığı açıklanmıştır. Buna göre; işçinin cinsel hayatına, siyasi görüşüne ve dini ya da diğer inançlarına dair bilgiler işverenlerce toplanamayacak bilgiler kapsamında yer almaktadır. İşveren, işçiyi işe alırken, eğer ülkenin ulusal düzenlemelerinde buna karşı bir hüküm bulunmuyorsa, yukarıda belirtilen bilgileri de toplama hakkını elde etmektedir. 6. fıkra uyarınca, işçilerin sendika üyelikleri ya da sendikal faaliyetlere katılmalarına dair verileri de işverenler tarafından toplanmaması

gereken bilgiler arasında yer almaktadır. İşçilerin sağlığıyla ilgili bilgilerin toplanması hususuna 7. fıkrada değinilmiştir. Buna göre; işçinin sağlığının çalışacağı işe uygun olup olmadığının belirlenmesi, iş sağlığı ve güvenliğinin sağlanması ve işçiye sosyal yardım yapma amacıyla işverenler, işçilerinin tıbbi bilgilerine erişebilme hakkına sahiptir. Son olarak 14. fıkrada işverenlerin işçilerini gözetleme faaliyetine değinilmektedir. Buna göre; işverenler işçilerini gözetliyorsa neden bu faaliyeti gerçekleştirdiğini, hangi zamanlarda gözetimi yaptığını, hangi yöntemi kullanarak izlediğini ve elde edeceği verilerin hangi veriler olacağını işçilerine bildirmek ve onlardan açık onay almakla yükümlüdür. Burada açık onay kavramıyla, işçiye ait verilerin toplanması için işçinin yazılı izninin alınması şartı kastedilmektedir. İşçinin okuma-yazma bilmiyor olması ya da işverenle aynı dili konuşamıyor olması durumunda onayın sözlü olarak verilmesi yeterli görülmüştür. Buna ek olarak işverenlerin, işçilerinin haberi olmaksızın gözetim yapabilmesi için ülkenin kendi mevzuatında buna yönelik bir düzenlemenin olması ve işçinin şüpheli davranışlarda bulunması ya da suç işlemiş olması koşulu aranmaktadır. İşveren tarafından kesintisiz gözetim yapılabilmesi için işyerinde güvenliğin, sağlığın ya da işyerinin korunmasını gerektirecek bir durumun olması gerekmektedir. Gözetim hakkında yapılan araştırmalar, aralıksız olarak gözetime maruz kalan kişilerin gerek psikolojik gerekse fizyolojik anlamda problemler yaşadığını göstermiştir. Bu nedenle bahsi geçen bu Uygulama Kodu, kesintisiz gözetim faaliyetini kısıtlayıcı düzenlemelerin gerekliliğini savunmaktadır (Çalışanların Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu, m. 6).

İşyerinde gözetim faaliyetini gerçekleştiren işverenlerin, işçilere ait verilerin güvenliği sağlaması oldukça önemlidir. Bu bağlamda ILO Uygulama Kodu'nun 7. maddesi uyarınca işverenler, çeşitli güvenlik önlemlerini alarak bu kişisel verilerin başkaları tarafından kullanılmasını, üzerinde değişiklik yapılmasını ve verilere erişilmesini engellemekle yükümlüdür (Çalışanların Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu, m. 7).

ILO tarafından 1996 yılında imzalanan "Çalışanların Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu", üye ülkeler açısından hukuki bağlayıcılığı bulunmayan bir uluslararası belgedir. Dolayısıyla bu uluslararası belgenin; ülkelerin yasalarının, toplu sözleşmelerinin, çalışma hayatına dair kuralların, düzenlemelerinin ve politikalarının geliştirilmesi amacıyla kullanılması tavsiye edilmektedir (http-48; Abrahamse, 2014, s. 6).

2.1.4. Avrupa Konseyi (AK)

AK, İkinci Dünya Savaşı'nın bitmesinden sonra 1949 yılı içerisinde, Londra'da imzalanan bir anlaşmayla birlikte kurulmuştur. Kurulduktan birkaç ay sonra, ülkemiz, 5456 sayılı Onay Kanununa 7382 sayılı Resmî Gazete'de yer verilmesiyle AK'ye üye olmuştur (Aydın, 2002, s. 42; Akgül, 2013, s. 119). Konsey, savaş sonrasında Avrupa'da huzurlu bir ortam sağlama amacını güderek oluşturulmuştur. AK'nin temel misyonu; demokrasi, insan hakları ve hukuk devleti gibi en temel prensipleri savunarak sahip çıkmaktır (Akgül, 2013, s.119-120). Nitekim AK, 4 Kasım 1950 tarihinde Avrupa İnsan Hakları Sözleşmesi'ni (AİHS) onaylamıştır (Korkmaz, 2017, s. 143; Şimşek, 2008, s. 19).

AK tarafından hazırlanmış olan üç uluslararası belge, siber gözetim faaliyetine yönelik düzenlemeler içermektedir. Bunlar; AİHS, 108 Sayılı AK Sözleşmesi ve 185 Sayılı Siber Suçlar Sözleşmesi'dir. Bu belgelerde yer alan siber gözetime ilişkin düzenlemelerin neler olduğu anlatılacaktır.

2.1.4.1. Avrupa İnsan Hakları Sözleşmesi (AİHS)

İkinci Dünya Savaşı'nın sona ermesinin ardından, Avrupa'da insan haklarının savunulması bağlamında herhangi bir sözleşme oluşturulmamıştır. Bunun üzerine, 4 Kasım 1950 tarihinde AİHS adıyla bilinen, "İnsan Haklarının ve Temel Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi", İtalya'nın başkenti Roma'da imzalanmıştır. İmzalanmasından üç yıl sonra, 3 Ekim 1953 yılı itibarıyla uygulamaya konmuştur (Schermer, 2007, s. 80; Türkel, 2010, s. 19).

Ülkemiz tarafından 6366 sayılı "İnsan Haklarını ve Ana Hürriyetleri Koruma Sözleşmesi" ve bu sözleşmenin ek protokolü, 18/5/1954 tarihli ve 8662 sayılı Resmî Gazete'de yayımlanarak yürürlüğe konmuştur (Türkel, 2010, s. 19).

AİHS'nin 19. maddesi uyarınca, Avrupa İnsan Hakları Mahkemesi (AİHM) kurulmuştur. AİHS'deki maddelerden herhangi birine uyulmadığı durumda ve aynı zamanda birey, ülkesindeki hukuksal yollara başvurup sonuç alamadığında AİHM'ye başvurabilme hakkına sahiptir. AİHM'nin verdiği kararlar mutlaktır (Aydın, 2002, s. 43).

AİHS'de bireylere ait kişisel bilgilerin korunmasını hedef alan doğrudan bir kanun maddesi yer almamaktadır. Ancak sözleşmenin 8. maddesi, özel ve aile hayatının müdafaa edilmesiyle ilgilidir. Söz konusu madde toplamda iki fıkradan oluşmaktadır. Birinci fıkra uyarınca; "Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı

gösterilmesi hakkına sahiptir (AİHS, m. 8)". Görüldüğü üzere ilgili maddenin birinci fıkrası uyarınca, "Bireylerin özel ve aile yaşamının, oturduğu evinin ve kurduğu iletişiminin kendisine ait bir hak olduğu ve bu haklara saygı duyulması gerektiği belirtilmiştir (Şimşek, 2008, s. 30-31)".

İlgili maddenin ikinci fıkrasında ise; kişinin sahip olduğu bu hakkı kullanmasını kamusal kurum, kuruluş ya da kişilerin engelleyemeyeceği; yalnızca birtakım istisnai durumların meydana gelmesi sonucunda bu hakka müdahale edilebileceği belirtilmektedir (Şimşek, 2008, s. 30-31). Maddenin ilgili fıkrası şu şekildedir:

> MADDE 8 – (2) Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir (AİHM, m.8/2).

AİHS'nin 8. maddesinde kişisel verilerin korunması hakkında açıkça bir hüküm bulunmamakla beraber, ilgili maddenin birinci fıkrası uyarınca bireyin özel ve aile hayatının korunmasıyla, kişisel verilerin korunması arasında bir bağlantı olduğu savunulmaktadır. Böylece kişisel veriler, bireylerin özel hayatının bir parçası kapsamında değerlendirilmektedir (Şimşek, 2008, s. 31). Özellikle 1980'li yıllardan itibaren AİHM, kişisel verilerin korunması hakkına önem atfederek AİHS bağlamında değerlendirmeye almıştır. Ancak buradaki en önemli nokta, devlet kurumları ile kişiler arasındaki ayrımdır. AİHS'nin 8. maddesiyle kişisel verilerin korunması hükmü, bu sözleşmeyi kabul eden devletlerin kurum ve kuruluşlarını bağlayıcı bir çerçevede değerlendirilmektedir. Kişiler tarafından veya özel sektörde siber gözetim faaliyetini gerçekleştirerek kişisel verilerin korunmasını ihlal eden işverenler açısından bahsi geçen sözleşme maddesinin geçerliliği bulunup bulunmadığı konusunda net bir kanun hükmü bulunmamaktadır (Uncular, 2014, s. 34).

Sözleşmenin 8. maddesinin birinci fıkrasındaki özel hayat ve aile hayatı olgularının düzgün bir biçimde açıklanması bu sözleşme bağlamında önem taşımaktadır. Mahkeme, bu olguları kesin bir şekilde tanımlamaktan kaçınmıştır. Teknolojik gelişmelerin hızla artması, kanunların bu teknolojik ve toplumsal gelişmeler ışığında revize edilmesi gibi nedenlerle özel ve aile hayatı gibi kavramların kesin tanımları yapılmamıştır. Bu nedenle AİHM, incelediği her dava dosyasındaki olaya uygun biçimde karar verilmesini daha uygun görmektedir (Güntürk, 2012, s. 106).

2.1.4.2. 108 Sayılı Avrupa Konseyi Sözleşmesi

AK, 108 sayılı Sözleşme imzalanmadan yirmi yıl önce, 1960'lı yılların sonlarına doğru, kişinin kişisel verilerinin ve özel hayatının korunması hakkı üzerinde düzenlemeler yapılmasını gerekli görmüştür. Söz konusu yıllarda kişilere ait verilerin korunmasına yönelik herhangi bir hukuki düzenlemenin olmayışı birtakım kaygıların su yüzüne çıkmasına sebep olmuştur. AK'nin karar organı olan Bakanlar Komitesi, kişisel verilerin korunmasına yönelik gerek mevzuatta gerekse insan haklarıyla ilgili sözleşmelerde yer alan düzenlemelerin konuşulması ve incelenmesi amacıyla 1968 yılında ilk kez bir toplantı gerçekleştirmiştir (Atak, 2010, s. 91; Grupe, Kuechler ve Sweeney, 2003, s. 4-5).

Bakanlar Komitesi daha sonra, Konsey üyesi devletlerin sahip olduğu özel hayatın gizliliği ve kişisel verilerin korunması hakkındaki kanunları araştırmıştır (Pearce ve Platten, 1998, s. 531). 1968 yılında AK, 509 sayılı "İnsan Hakları ile Modern, Bilimsel ve Teknolojik Gelişmeler" isimli tavsiye kararını onaylamıştır. Bu kararla Konsey, üyesi olan ülkelerde modern, teknolojik ve bilimsel cihazların kullanımı sırasında kişisel verilerin korunmasına ve özel hayatın gizliliğinin sağlanmasına ilişkin ulusal düzenlemelerin yapılmasını talep etmiştir. Yeterli ulusal düzenlemenin bulunmadığı durumlarda ise ülkelerin, AİHS maddeleri uyarınca hareket etmesini talep etmiştir. Konsey, elektronik araçlarla yapılan gözetleme faaliyetinde toplanan kişisel verilerin yasadışı bir biçimde kullanılmasıyla kişisel verilerin ve özel hayatın korunmasının ihlal edildiğini kabul etmiştir (Akgül, 2013, s. 126-127). Konsey tarafından daha sonra *Uzmanlar Komitesi* adıyla bir kurul oluşturulmuştur. Uzmanlar Komitesi kurulu; teknolojiyle beraber gelişen bilgisayar ve telefon gibi araçların kullanımının özel hayat ile kişisel verilerin korunması hakkını ihlal etmemesi adına önerilerde bulunmuştur. Bu komite gerek kişisel verilerin korunması gerekse özel hayata saygı duyulması anlamında büyük bir misyon üstlenmiştir (Bennett ve Raab, 2004, s. 72).

108 sayılı Sözleşme'den kısa bir süre önce, kişisel verilerin korunması amacıyla hazırlanmış olan iki karar metni Bakanlar Komitesi tarafından kabul edilmiştir. Bunlar; "Özel Sektördeki Elektronik Veri Bankaları Karşısında Bireylerin Özel Hayatlarının Korunmasına İlişkin Karar" ve "Kamu Sektöründeki Elektronik Veri Bankaları Karşısında Bireylerin Özel Hayatlarının Korunmasına İlişkin Karar"dır. Bu iki karar sırasıyla, 1973 ve 1974 yıllarında onaylanmıştır. 108 sayılı Sözleşme'nin

oluşturulmasında ise, bu kararların önemli bir zemin oluşturduğu bilinmektedir (Atak, 2010, s. 92).

AK tarafından 28 Ocak 1981 tarihinde kabul edilmiş olan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunması Sözleşmesi", kişisel verilerin korunmasını temel alan ve bağlayıcı niteliğe sahip ilk ve tek sözleşme olma özelliğini taşımaktadır. Buna ek olarak hem Konsey üyesi ülkelerin hem de üye konumunda olmayan ülkelerin imzalayabileceği bir sözleşme olması açısından da önem arz etmektedir. Bu sözleşme, kişisel verilerin korunması anlamında minimum düzeydeki standartları içeren bir metindir. Konsey üyesi devletler, ulusal düzenlemeler yapmak suretiyle kişisel verilerin korunmasını sağlamakta özgürdür (Küzeci, 2010, s. 142-144). 108 sayılı Sözleşme ile, AİHS'deki kişisel verilerle ilgili boşluk giderilmeye çalışılmıştır (Akgül, 2013, s. 126; Uncular, 2012, s. 16). Mayıs 2019 tarihi itibarıyla 44 ülke tarafından bu sözleşme kabul edilmiştir. Ülkemiz ilgili sözleşmeyi 28 Ocak 1981 tarihinde imzalamış, 17/3/2016 tarihli ve 29656 sayılı Resmî Gazete'de yayımlamış ve 1 Eylül 2016 itibarıyla da yürürlüğe koymuştur (http-49).

Birinci madde uyarınca bu sözleşmenin amacının, kişilere ait bilgilerin otomatik bir biçimde toplanıp depolanmasına karşılık kişinin özel hayatına saygı gösterilmesi hakkının korunması olduğu belirtilmiştir. Sözleşmenin 2. maddesinde ise kişisel veri, otomatik veri dosyası, otomatik işlem ve dosya yöneticisi kavramlarının tanımlaması yapılmıştır. Bu maddeye göre; "Kimliği belirlenebilir ya da belirlenmiş olan gerçek kişiye ait her türlü bilgi kişisel veriyi" oluşturmaktadır. "Otomatik bir şekilde işlenen tüm veriler" otomatik veri dosyası tanımını karşılamaktadır. Otomatik işlem olarak ifade edilen kavram ise; "Tamamen ya da belli bir bölümünde otomatik bir sistem kullanılarak elde edilen kişisel verilerin toplanması, saklanması, üzerinde oynanarak değişiklik yapılması, başka kaynaklara iletilmesi" olarak verilmiştir. Son olarak; "Otomatik bir sistem yardımıyla kişilere ait bilgileri kaydeden ve bu bilgilerin işlenmesinde söz sahibi olan gerçek kişi, tüzel kişi, kamu kurum ve kuruluşu ve yetkili diğer kuruluşlar" dosya yöneticisi olarak bu maddede tanımlanmıştır. 3. maddede; "Bu sözleşmenin, kamu sektörü ve özel sektörde elde edilen kişisel verilerin otomatik olarak işlenmesi bağlamında geçerli olduğu belirtilmiştir (108 sayılı Sözleşme, m. 1-3)".

Sözleşmenin 5. maddesi, kişisel verilerin özelliklerinin açıklandığı maddedir. Otomatik bir sistem aracılığıyla işlenen veriler, meşru ve adil olarak toplanmalı ve düzenlenmelidir. Verilerin, belli bir amaç doğrultusunda toplanması ve belirlenmiş bir

süre içerisinde saklanması çok önemlidir. Bu amacın ve sürenin dışına çıkılması yasaktır. Elde edilen kişisel bilgilerin akla, mantığa ve gerçeğe uygun nitelikte olması gerekmektedir. Bu nedenle içerikte herhangi bir değişiklik olması durumunda verilerin güncellenmesi şarttır (108 sayılı Sözleşme, m. 5).

6. ve 7. madde uyarınca; bazı kişisel verilerin, ulusal düzenlemeler yapılmadığı sürece otomatik işleme tabi tutulamayacağı açıklanmıştır. Bu çerçevede; kişinin ırkı, siyasi düşünceleri, mensup olduğu din ile diğer inançları, sağlığı ve cinsel hayatına dair bilgileri otomatik bir sistem aracılığıyla toplanamamaktadır. Bununla birlikte, kişisel verilerin kaydedilmesini sağlayan kişi veya kurumlar, herhangi olumsuz bir durumda verilerin başkaları tarafından ele geçirilmesi, değiştirilmesi veya başka kaynaklara iletilmesi ihtimaline karşı verileri korumakla yükümlüdür (108 sayılı Sözleşme, m. 6 ve m. 7).

Madde 8'e göre, kendisine ait bilgileri toplanan ve işlenen herkesin birtakım hakları olduğu belirtilmiştir. Bu kapsamda kişiler, verilerini elde edip saklayan yetkililerin adresini öğrenebilecek, verilerle ilgili dosyaların var olup olmadığını sorgulayabileceklerdir. Herhangi bir gerekliliğin vuku bulması sonucunda kişiler, bu verilerin düzeltilmesini veya silinmesine talep etme hakkına sahiptir. Verileri kaydedenlerin, talep doğrultusunda düzeltme ya da silme işlemini gerçekleştirmemesi sonucunda bireylerin hukuki yollara başvurma hakkı saklıdır (108 sayılı Sözleşme, m. 8). Bunlara ek olarak, ilgili sözleşmenin 5, 6 ve 8. maddeleri istisnai durumlara tabi değildir. İstisnai koşulların oluşması yalnızca devletin ve halkın emniyeti, devletin mali çıkarları, suç işlenmesinin önüne geçilmesi ile verileri toplanan kişinin ya da diğer kişilerin hak ve özgürlüklerinin muhafaza edilmesi durumlarında geçerlidir. 108 sayılı Sözleşme'de yer alan hükümlerin uygulanabilmesi için sözleşmeyi kabul eden ülkelerin kendi ulusal düzenlemelerini yürürlüğe koyması şartı da 10. maddede belirtilmiştir (108 sayılı Sözleşme, m. 9 ve m. 10).

Sözleşmenin tüm maddelerinin daha kolay bir biçimde uygulanmaya koyulması ve eksikliklerin giderilmesi amacıyla çeşitli tavsiyelerde bulunacak bir Danışma Komitesi kurulmuştur (108 sayılı Sözleşme, m. 18 ve m. 19). Komite, gerçekleştirilen her toplantının sonrasında AK Bakanlar Komitesi'ni bilgilendirmek amacıyla bir rapor hazırlamaktadır. Bu raporu daha sonra AK Bakanlar Komitesi'ne takdim etmektedir. Bu bağlamda Danışma Komitesi, 2002 yılında; "Kişisel Veriler Açısından Yeterli Düzeyde Koruma Sağlamayan Üçüncü Ülkelere Veri Transferini Sağlayacak Sözleşme

Şartlarının Hazırlanmasına İlişkin Rehber" ve 2005 yılında "Biyometrik Verilerin Toplanması ve İşlenmesinde 108 sayılı Sözleşme İlkelerinin Uygulanmasına İlişkin İlerleme Raporu" hazırlamıştır (Atak, 2010, s. 99).

Komite tarafından 2001 yılında 108 sayılı Sözleşme'ye ek bir Protokol yayımlanmış ve bu protokol 2004 yılı itibarıyla uygulanmaya başlanmıştır. Protokol gereğince, kişilere ait bilgilerin işlenmesi faaliyetini gerçekleştirmesi amacıyla bağımsız bir makama ihtiyaç doğmuştur. Bu makamın görevi; kişisel verilerin muhafaza edilmesi bağlamında birey hak ve özgürlüklerini korumak, çeşitli araştırmalar yapmak ve gerektiğinde duruma müdahale ederek kişilerin yaptığı şikâyetleri değerlendirmektir. Bu makam, bağımsız bir biçimde hareket etme hakkına sahiptir. Ancak makamın verdiği kararlara karşılık kişilerin diğer hukuki yollara başvurma hakkı mevcuttur. 108 sayılı Sözleşme'nin Ek Protokol'ü, ileriki bölümlerde incelenecek olan; "95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Yönelik Bireylerin Korunması Hakkındaki Avrupa Birliği ve Avrupa Parlamentosu Direktifi" ile paralellik göstermektedir. Aralarındaki en temel farklılık ise şudur; bahsi geçen bu Ek Protokol yalnızca kişisel verilerin otomatik bir sistem aracılığıyla elde edilmesini içerirken, 95/46/EC sayılı Direktif kişisel verilerin korunmasına ilişkin her türlü faaliyeti kapsamaktadır (Küzeci, 2010, s. 146-147; Atak, 2010, s. 99-100; Korkmaz, 2017, s. 145).

Ülkemiz tarafından bu Ek Protokol, 20 Nisan 2016 tarihi itibarıyla 6705 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokolün Onaylanmasının Uygun Bulunduğuna İlişkin Kanun" uyarınca kabul edilerek 5/5/2016 tarihli ve 29703 sayılı Resmî Gazete'de yayımlanarak yürürlüğe konmuştur (Korkmaz, 2017, s. 151).

BM'nin, "Evrensel İnsan Hakları Bildirisi" içindeki 12. maddenin önemini daha önce belirtmiştik. Bu maddeye göre; "Hiçbir bireyin özel hayatına, ailesine, ikamet ettiği yere, iletişim kurma hakkına, kişiliğine ve şerefine karşı saldırıda bulunulamaz. Bu şekilde müdahalelere maruz kalan kişilerin, kanunlarla korunması hakkı mevcuttur (BM Evrensel İnsan Hakları Bildirisi, m. 12)". Avrupa Konseyi Danışma Komitesi, 23 Ocak 1970 tarihinde özel hayatın gizliliği hakkının tanımını yaparken BM'nin sözü edilen bu bildirisinin 12. maddesinden yararlanmıştır. Danışma Komitesi, kişilerin özel hayatına saygı gösterilmesi gerektiğini ve herkesin hayatlarını devam ettirirken

tercihleri doğrultusunda hareket edebilme hakkının olduğunu belirtmiştir. Bu bağlamda, kişinin hayatına bir başkası tarafından karışılmasının olabildiğince sınırlı tutulmasının gerektiği savunulmaktadır. Danışma Komitesi tıpkı BM Evrensel İnsan Hakları Bildirisi'nin 12. maddesinde olduğu gibi; "Bireylerin özel ve aile yaşamına, yaşadığı yere, kişiliğine ve şerefine karşı saygılı olunması gerektiğini belirterek özel hayatın mahremiyetinin korunması" hakkına atıf yapmıştır. Aynı zamanda Komite; kişilere ait fotoğrafların, bilgi ve belgelerin onların rızası dışında yayınlanması ve kişilerin hukuk kurallarının dışında bir gözetim faaliyetine maruz kalması durumlarının da özel hayatın gizliliği hakkı çerçevesinde ele alınması gerektiğini belirtmiştir (Korkmaz, 2017, s. 141).

2.1.4.3. 185 Sayılı Siber Suçlar Sözleşmesi

1 Temmuz 2004 tarihi itibarıyla 185 sayılı "Siber Suçlar Sözleşmesi" AK tarafınca uygulamaya konmuştur. Bu sözleşmenin en temel özelliği, siber suçlar hakkında hazırlanmış ilk ve tek sözleşme olmasıdır. Gerek bilgisayar tabanlı teknolojiler gerekse ceza hukuku bağlamında ilk uluslararası sözleşme olması açısından da önemlidir (Turhan, 2010, s. 72). 185 sayılı Sözleşme ile amaçlanan; sözleşmenin tarafı olan ülkelerin birlikte hareket etmesiyle siber suçlar bağlamında düzenlemeler yapılması ve böylece suçun ve suçlunun niteliği belirlenerek devletlerin ortaklaşa bir çalışma yürütmesidir (Civelek, 2011, s. 67-68). Ülkemiz tarafından 10 Kasım 2010 tarihinde imzalanan bu sözleşme, 1 Ocak 2015 yılında yürürlüğe konmuştur (http-50).

Bilgisayarların ağ sistemlerinin giderek yaygın bir biçimde insan hayatında yer almasıyla ağ sistemleri üzerinden işlenebilecek siber suçlar da her geçen gün artmaktadır. 185 sayılı Sözleşme yardımıyla siber suçların işlenmesinin önüne geçilmesi için hem ülkelerin hem de ülkelerdeki özel sektör kuruluşlarının birlikte hareket ederek bilgi teknolojisiyle ilgili hakları koruması beklenmektedir (http-51).

185 sayılı Siber Suçlar Sözleşmesi dört ana bölümden oluşmaktadır. Birinci bölüm siber suçlarla ilgili bilgisayar sistemi, bilgisayar verisi gibi bazı terimlerin açıklandığı bölümdür. İkinci bölümde ulusal boyutta alınması gereken tedbirler ne olduğu açıklanmıştır. Üçüncü bölümde uluslararası boyutta iş birliğine dair hükümler yer alırken son bölümü ise sonuç hükümleri olarak verilmiş bazı düzenlemeler oluşturmaktadır (http-51).

Sözleşmenin 1. maddesinde yer alan bilgisayar sistemi ve bilgisayar verisi kavramlarının ne anlama geldiğinin ifade edilmesi yerinde olacaktır. Bilgisayar sistemi;

"Belirli programlar kullanılarak birbirine bağlanmış ve aynı zamanda otomatik bir sistem içerisinde kişisel bilgileri işleyebilen birden fazla elektronik cihazdır". Bilgisayar verisi ise; "Bilgisayar sistemleri içerisinde mevcut olan işlenebilir her türlü bilgidir (185 sayılı Siber Suçlar Sözleşmesi, m.1)".

185 sayılı Siber Suçlar Sözleşmesi'nin ikinci kısmı da kendi içerisinde iki bölüme ayrılmaktadır. Buna göre birinci bölümde *maddi ceza hukuku* ve ikinci bölümde *usul hukuku* hükümleri yer almaktadır. 2. maddede bu sözleşmeyi kabul eden ülkelerin, bilgisayar ve veri sistemlerine illegal ve kasıtlı bir biçimde erişim sağlanmasıyla ilgili cezai ulusal düzenlemeler yapması gerektiği belirtilmektedir. Benzer biçimde illegal ve kasıtlı olarak, özel bilgisayarlardaki verilerin birtakım yöntem ve araçlar kullanılarak başka bilgisayarlara aktarılması da cezai bir suç olarak kabul edilmektedir. Madde 4, kişisel verilerin müdahaleye maruz kalmasıyla ilgili bir düzenlemeyi içermektedir. Buna göre, bilgisayar verileri ortada herhangi bir gerekçe bulunmadığı halde zarara uğratılıyor, siliniyor, bozuluyor veya üzerinde oynama yapılıyorsa bu durum ulusal hukukta cezai işleme tabi olmak durumundadır. Bilgisayar veri sistemlerine de hukuk dışında müdahale edilmesi durumunda, aynı şekilde cezai yaptırım uygulanması gerekmekte olduğu hükmü 5. maddede verilmektedir (185 sayılı Siber Suçlar Sözleşmesi, m. 2-5). Özetle bu maddelerde, bilgisayarlardaki verilerin ve bilgisayar sistemlerinin mahremiyeti ve kullanımı sırasında işlenen suçlar açıklanmaktadır.

185 sayılı Sözleşme'yi kabul ederek taraf devlet statüsünü kazanmış ülkelerin, kendi mevzuatlarında gerekli düzenlemeleri yapması ve bu suçları yasal hale getirmesi Konsey tarafından talep edilmektedir. Ülkelerin ulusal ceza hukuku düzenlemeleriyle, bu sözleşmenin paralel olması, Konsey için yeterli sayılmaktadır (Özbek, 2015, s. 78-79).

2.1.5. Avrupa Birliği (AB)

Avrupa Kıtası'ndaki devletler, geçirdikleri savaş dönemlerinden sonra barış sözleşmeleri imzalamıştır. Bu barış sözleşmeleriyle birlikte Avrupa'da bir *birlik* kurulması fikri ortaya çıkmıştır. 1945 yılında İkinci Dünya Savaşı'nın sona ermesinin ardından, savaşın yarattığı olumsuzlukların giderilmesi adına dünya genelinde birçok kuruluş oluşmuştur. Bunlardan birincisi 1951 yılında; "Avrupa Kömür ve Çelik Topluluğu (AKÇT)"dur. 1957 yılında ise; "Avrupa Ekonomik Topluluğu (AET)" ve "Avrupa Atom Enerjisi Topluluğu (AAET)" bir araya gelmiştir (Akgül, 2013, s. 135).

8 Nisan 1965 tarihinde imzalanan Brüksel Antlaşması'yla birlikte AKÇT, AET ve AAET birleşerek "Avrupa Topluluğu (AT)" isminde tek bir topluluğa dönüşmüştür. Ardından 7 Şubat 1992 tarihinde, "Maastricht Antlaşması"nın imzalanması sonucunda ilk kez AB adı kullanılmaya başlanmıştır. AB'nin temel amacı, üyesi olan yirmi sekiz ülkenin ve bu ülkelerin vatandaşlarının huzurlu, adil, güvenli ve özgür bir ortamda yaşamasına olanak tanımaktır (http-52; http-53).

AB'nin kuruluşunda rol oynayan antlaşmalar, diğer bir deyişle AB hukukunun kaynakları birinci ve ikinci düzey olmak üzere ikiye ayrılmaktadır. AB'nin birinci düzeydeki hukukunu Kurucu Antlaşmalar ve AB Temel Haklar Şartı oluşturmaktadır. Kurucu Antlaşmalar; 1951 yılında kabul edilen Paris Antlaşması ve 1957 yılında kabul edilen Roma Antlaşması olarak bilinen AKÇT, AET ve AAET Antlaşmaları'ndan başlayarak 2009 yılında yürürlüğe girmiş olan Lizbon Antlaşması'na kadar uzanan dönemde AB üyesi ülkelerin imzaladığı antlaşmaları ifade etmektedir (Bilgin, 2016, s. 40; http-54).

AB'nin birinci düzeydeki hukukunu oluşturan antlaşmalar, AB üyesi olan ülkelerin görüş birliği sonucunda oluşturulup yürürlüğe konmuştur (Korkmaz, 2017, s. 179-180). AB'nin ikinci düzeydeki hukuku ise şunlardan oluşmaktadır: "Tüzükler, Direktifler, Kararlar ve Tavsiye Kararları". Bunlar arasından *Tüzükler*, AB üyesi konumundaki ülkeleri bağlayıcı özelliğe sahiptir. *AB Direktifleri*, üye ülkelerin mevzuatlarıyla uyumlu halde olmak durumundadır. *AB Kararları*, kararın muhatabı olan kişileri bağlayıcı niteliktedir. Bu kararların muhatabı hem gerçek hem de tüzel kişiler olabilmektedir. Son olarak *Tavsiye Kararları* ise, tavsiye niteliğinde olup herhangi bir bağlayıcılığa sahip değildir (Akgül, 2013, s. 135-136).

Uluslararası düzeyde kurulmuş olan diğer kuruluşlara bakıldığında AB'nin en önemli niteliği, uluslar üstü bir yapıya sahip olmasıdır. Bu nedenle AB, kendisine üye olan ülkelerin mevzuatlarında gerekli olduğu durumlarda birtakım düzenlemeler yapabilme hakkına sahiptir (http-42; Korkmaz, 2017, s. 180).

2.1.5.1. Avrupa Birliği Temel Haklar Şartı

AB Temel Haklar Şartı, 7 Aralık 2000 tarihinde imzalanmıştır. AB Temel Haklar Şartı'yla birlikte ilk defa, AB üyesi devletlerin vatandaşların ve Avrupa'da yaşayan halkın ekonomik, siyasal ve bireysel hak ve özgürlükleri tek bir belgede bir araya getirilmiştir. Temel Haklar Şartı, yapılan birtakım düzenlemelerin ardından 2004 yılı itibarıyla AB Anayasası'na *temel haklar kataloğu* adı altında eklenmiştir. 1 Aralık 2009

tarihinde kabul edilen Lizbon Antlaşması'yla birlikte AB Temel Haklar Şartı, üye ülkeleri bağlayıcı bir nitelik kazanmıştır (Küzeci, 2010, s. 173).

AB Temel Haklar Şartı, yedi ana bölüm ve elli dört maddeden oluşmaktadır. Bu bölümler sırasıyla; itibar, özgürlükler, eşitlik, dayanışma, vatandaş hakları, adalet ve genel hükümler şeklindedir. Özgürlükler kategorisini kapsayan ikinci bölümdeki 7. ve 8. madde siber gözetim faaliyeti bağlamında önemlidir. Buna göre 7. maddede; "Kişinin özel hayatına ve aile hayatına saygı gösterilmesi gerektiği" hükmü yer almaktadır. Bu hüküm bağlamında; "Kişinin özel hayatı, aile hayatı, yaşadığı konutu ve iletişim kurma hakkına herkes tarafından saygı gösterilmesi" gerekmektedir. 7. maddenin AİHS'nin 8. maddesiyle eşdeğer olduğu da kabul edilmektedir. AİHS'nin 8. maddesinde *haberleşme* olarak geçen kavram, AB Temel Haklar Şartı'nın 7. maddesinde *iletişim* olarak değiştirilmiştir. Bunun temel sebebi, iletişim bağlamında meydana gelen teknolojik gelişmelere karşı özel hayatın ve kişisel verilerin korunmasına yönelik daha geniş kapsamlı düzenlemeler yapılmasını sağlamaktır (AB Temel Haklar Şartı, m. 7; Şimşek, 2008, s. 69).

8. maddede ise, kişisel verilerin korunması hakkında üç fıkradan oluşan bir düzenleme yer almaktadır. İlgili madde, AİHS'nin 52. maddesinin üçüncü fıkrasıyla eşdeğer konumdadır (Şimşek, 2008, s. 69). 8. maddenin birinci fıkrasına göre; "Her birey, kendisiyle ilgili kişisel verilerin korunmasını talep edebilir". İkinci fıkrada; "Kişilere ait verilerin belli bir amaç doğrultusunda, yasal ve adil bir biçimde kullanılması gerektiği" belirtilmiştir. Kişisel verilerin sahipleri ise bu verilere istediği zaman ulaşabilmeli ve gerektiğinde bilgilerin değiştirilmesini, düzeltilmesini talep edebilmelidir. Sonuncu fıkrada ise, ilk iki fıkradaki düzenlemelere uyulup uyulmadığını bağımsız bir makamın denetlemesi gerektiği belirtilmiştir (AB Temel Haklar Şartı, m. 8).

2.1.5.2. 95/46/EC Sayılı Direktif

Kişisel verilerin korunması amacıyla hazırlanmış en önemli belgelerden bir tanesi "Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Yönelik Bireylerin Korunması Hakkındaki 24/10/1995 tarihli ve 95/46/EC sayılı Avrupa Birliği ve Avrupa Parlamentosu Direktifi"dir. Teknolojinin her geçen gün hızla gelişmesiyle birlikte kişilere ait verilerin işlenmesi de giderek kolaylaşmaktadır. Bu nedenle kişisel verilerin korunabilmesi amacıyla 95/46/EC sayılı Direktif, AB tarafından hazırlanmıştır. Bu direktif ile, AB üyesi ülkelerde kişisel verilerin korunması bağlamında minimum

düzeydeki standartların belirlenmesi sağlanmaya çalışılmaktadır (Küzeci, 2010, s. 176-178). AB üyesi olan tüm ülkelerde bu direktifin kişisel verilerin korunması bakımından eşit derecede koruma sağlaması amaçlanmıştır. Böylece tüm AB üyesi devletlerin, ulusal düzenlemelerini bu direktife uygun bir biçimde yapması gerekmektedir (Uncular, 2014, s. 39).

95/46/EC sayılı Direktif; "Yalnızca kimliği belirlenmiş ya da belirlenebilir durumdaki gerçek kişilere ait verilerin korunmasını sağlamaktadır (95/46/EC sayılı Direktif, m. 1)". AB üyesi olan devletler, eğer isterlerse yapacakları düzenlemelerle tüzel kişileri de kapsama alabilecektir (Şimşek, 2008, s. 42). Bu direktif ile yapılan düzenlemeler hem kısmen otomatik olarak hem de tamamen otomatik olarak işlenen kişilerin verilerin korunmasını kapsamına almaktadır (95/46/EC sayılı Direktif, m. 3). Burada verilerin otomatik olarak işlenmesiyle kastedilen; "Bilgisayar gibi teknolojik gözetim araçları yardımıyla kişilere ait bilgilerin toplanması" faaliyetidir. Elle ya da bir kısmı elle bir kısmı da teknolojik araçlarla toplanan veriler de yine bu direktif kapsamındadır.

Toplanan bu kişisel verilerin dürüstlük kuralı çerçevesinde ve kanun dışı bir durum oluşturmayacak biçimde toplanması önemlidir. Buna ek olarak, toplanan verilerin belirlenmiş açık bir amaç için ve kanun dışı olmayacak biçimde işlenmesi gerekmektedir. Kişisel verilerin, veri sahiplerinin onayı dahilinde ve belirlenmiş bir amaç doğrultusunda işlenebilmesi mümkündür. İşçinin işe alınırken imzaladığı sözleşmede kişisel verilerinin işleneceğine dair herhangi bir maddenin yer alması durumunda ise işçi, kişisel verilerinin işlenmesi onaylamış kabul edilecektir. Böylece işverenin, işçinin kişisel verilerini işleyebilme hakkı doğacaktır (95/46/EC sayılı Direktif, m. 6-7).

İşlenecek veriler konusundaki istisna 95/46/EC sayılı Direktif'in 8. maddesinde verilmiştir. AK'nin 108 sayılı Sözleşmesi'nin 6. ve 7. maddelerinde de hangi verilerin işlenemeyeceğine dair düzenleme yer almaktadır. 95/46/EC sayılı Direktif'e göre işlenemeyecek veriler, AK'nin 108 sayılı Sözleşmesi'ndekine nazaran daha ayrıntılı bir biçimde düzenlemiştir (Korkmaz, 2017, s. 193). Buna göre kişilerin; sağlık durumuyla ya da cinsel hayatıyla ilgili bilgilerinin, sendika üyeliğine, dini inancına, siyasi görüşüne ya da etnik kökenine yönelik verilerinin işlenmesi yasaklanmıştır. Bireyin bu verilerinin toplanabilmesi için bazı istisnai durumlar söz konusudur. Kişinin onayı varsa, herhangi bir suçla mücadele etme durumu ortaya çıkmışsa, kişi fiziksel ya da yasal anlamda onay

veremeyecek bir durumdaysa veya başka bir kişinin hayati çıkarlarının korunması gereken bir durum varsa bu koşullar altında kişinin verileri işlenebilecektir (95/46/EC sayılı Direktif, m. 8).

Daha önce incelediğimiz bazı uluslararası belgelerde olduğu gibi 95/46/EC sayılı Direktif'te de kişisel verileri toplayan kişiler, veri sahiplerine bu konuda bilgi vermek durumundadır. Kendisine ait verileri kimin topladığını, bu verilerin toplanma amacının ne olduğunu ve kendi talebi doğrultusunda bu verilerin değiştirilebileceğini verilerin sahibinin bilme hakkı vardır (95/46/EC sayılı Direktif, m. 10-11).

95/46/EC sayılı Direktif'in 22. maddesi uyarınca, kişisel verileri işlenen kişilerin mevzuatta yer alan düzenlemeler çerçevesinde yargıya başvurma hakkı bulunmaktadır. Verilerin işlenmesi esnasında kişiler herhangi bir mağduriyet yaşarsa bu durumda, verilerini işleyen kişilerden tazminat talep etme hakkı mevcuttur. Verileri işleyen kişiler, bu mağduriyetin yaşandığı olayda herhangi bir sorumluluğunun bulunmadığını kanıtlarsa bu durumda tazminat ödeme yükümlülüğünden kısmen ya da tamamen muaf olabilmektedir (95/46/EC sayılı Direktif, m. 22-23).

Son olarak 95/46/EC sayılı Direktif'in 29. maddesi uyarınca bir *çalışma grubu* oluşturulması gerekli görülmüştür. Bu çalışma grubu 95/46/EC sayılı Direktif'in uygulanması esnasında görüşlerini bildirmek ve gerekli düzenlemeleri yapmakla yükümlüdür (Savaş, 2009, s. 104). Çalışma grubu aynı zamanda; işçilere ait kişisel verilerin toplanmasını, işlenmesini ve saklanmasını sağlayacak, işçilerin siber gözetim araçları yardımıyla gözetlenmesinden sorumlu olacak ve tüm bu faaliyetlerin, işçilerin kişisel verilerinin korunması hakkını ihlal edip etmediğini denetleyerek bu konuda rapor hazırlayacaktır (Özdemir, 2010, s. 251).

2.1.5.3. 97/66/EC ve 2002/58/EC Sayılı Direktifler

97/46/EC sayılı Direktif ile kişisel verilerin korunması daha geniş bir çerçevede sağlanmaya çalışılmıştır. Bu genel çerçeve daraltılarak özellikle telekomünikasyon sektöründe birtakım düzenlemeler yapılması gereksiniminin doğmasıyla 95/46/EC sayılı Direktif'i tamamlayıcı özellikte olan; "Telekomünikasyon Sektöründe Kişisel Verilerin İncelenmesi ve Özel Hayatın Gizliliğinin Korunması Hakkındaki 15/12/1997 tarihli ve 97/66/EC sayılı Avrupa Birliği ve Avrupa Parlamentosu Direktifi" kabul edilmiştir. Bu Direktif ile telefon, kamera ve cep telefonu gibi ağ sistemleri üzerinden işlenen verilerin korunmasına yönelik düzenlemeler yapılmıştır (Küzeci, 2010, s. 201-202; Akgül, 2013, s. 151).

12/7/2002 tarihli ve 2002/58/EC sayılı "Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunması Hakkındaki Avrupa Birliği ve Avrupa Parlamentosu Direktifi", 97/66/EC sayılı Direktif'in yerini almıştır (Aksoy, 2008, s. 11). Yirmi bir maddeden oluşan 2002/58/EC sayılı Direktif'in amacı 1. maddesinde de belirtildiği üzere; "Elektronik iletişim sektöründe kişisel verilerin ve özel hayatın gizliliğinin korunması bağlamında 95/46/EC sayılı Direktif'i tamamlayacak biçimde düzenlemeler getirmektir (2002/58/EC sayılı Direktif, m. 1)".

2002/58/EC sayılı Direktif, 95/46/EC sayılı Direktif'ten farklı bir biçimde "Kimliği belirlenmiş ya da belirlenebilir gerçek kişilere ek olarak tüzel kişilerin de kişisel verilerini ve özel hayatının gizliliği hakkını koruma altına almaktadır (2002/58/EC sayılı Direktif, m. 1; Küzeci, 2010, s. 203)". 2002/58/EC sayılı Direktif'in 4. maddesi uyarınca, AB üyesi ülkelerin elektronik iletişim sektöründe çalışan işçilerin kişisel verilerin işlenmesi ve özel hayatının gizliliğinin korunması konusundaki risklere karşı düzenlemeler yapması gerektiği belirtilmiştir (2002/58/EC sayılı Direktif, m. 4).

Önceki bölümde internet üzerinden yapılan gözetim faaliyetinde çerezlerin (cookie) kullanıldığını ifade etmiştik. Çerezler, interneti kullanan kişilerin hangi sitelerde ne kadar süre gezindiği bilgisine erişilmesini sağlamaktadır. 2002/58/EC sayılı Direktif'te; "Çerezlerin gözetim faaliyetinde kullanılabileceği" ibaresi yer almaktadır. Bu çerezlerin kullanıldığının bilgisi ise gözetim faaliyetine maruz kalan kişiye, 95/46/EC sayılı Direktif'e uygun bir biçimde, açık ve net olarak verilmelidir (2002/58/EC sayılı Direktif; Küzeci, 2010, s. 206).

2002/58/EC sayılı Direktif'in 15. maddesi uyarınca; "Elektronik iletişim sektöründe kişilerin birbiriyle iletişim kurmak için gönderdiği ve aldığı mesajların ve trafik verilerinin başkaları tarafından gözetlenmesi ve kayıt altına alınması hususunda ülkelerin düzenlemeler yapması" gerekmektedir. Veri sahibine; "Verilerinin işlendiği, veri işlemenin amacı, veri işlemeyi kimin gerçekleştirdiği ve veri sahibinin istediği durumda bu siber gözetim faaliyetini kabul etmeme hakkının olduğuna dair açıkça bilgi verildiği koşulda bu iletişim gözetlenebilecektir ya da kayıt altına alınabilecektir (2002/58/EC sayılı Direktif, m. 15; Şimşek, 2008, s. 59)".

2.1.5.4. 95/46/EC Sayılı Direktif'in Çalışma Grubu Kararları

AB'nin 95/46/EC sayılı Direktif'inin 29. maddesi uyarınca; "Bağımsız bir biçimde çalışma yapacak olan çalışma grubu oluşturulması" gerekmektedir. Bu çalışma grubunun amacı, 95/46/EC sayılı Direktif'e ait düzenlemelerin AB üyesi olan tüm

devletlerde eşit şekilde uygulanmasını sağlamaktır. Aynı zamanda bu çalışma grubu, 95/46/EC sayılı Direktif'teki düzenlemelerin çalışma hayatında uygulanmasına yönelik görüş ve öneriler sunmuştur (Okur, 2013, s. 45).

AB'nin önceki bölümlerde bahsettiğimiz Temel Haklar Şartı ile 95/46/EC, 97/66/EC ve 2002/58/EC Direktifleri işçilerin kişisel verileri ile özel hayatının korunması hakkı bağlamında düzenlemeler yapmıştır. Bu belgelere ek olarak çalışma grubunun yaptığı çalışmalar sonucunda iş hukukuna yönelik birtakım raporlar oluşturulmuştur (Yiğit, 2013, s. 7-8).

Çalışmanın bu bölümünde çalışma grubuna ait dört karar incelenecektir. Bu kararlar şu şekildedir:

- 13/9/2001 tarihli ve 5062/01/EN/Final WP 48 sayılı "İşyerinde Kişisel Verilerin İşlenmesi Kararı",
- 29/5/2002 tarihli ve 5401/01/EN/Final WP 55 sayılı "İşyerindeki Elektronik İletişimin Gözetlenmesi Kararı",
- 11/2/2004 tarihli ve 11750/02/EN WP 89 sayılı "Video Sistemleri Kullanılarak Yapılan Gözetim Faaliyetiyle Kişisel Verilerin İşlenmesi Kararı",
- 8/6/2017 tarihli ve 17/EN WP 249 sayılı "İşyerinde Verilerin İşlenmesi Kararı".

Çalışma esnasında, işverenler tarafından işçilere ait kişisel verilerin işlenmesinin gerekliliği ortaya çıkmaktadır. İşçilerin kişisel verilerinin çeşitli siber gözetim araçları yardımıyla toplanması, işlenmesi ya da kayıt altına alınması faaliyetlerinde işçinin verilerinin ulusal düzenlemeler ışığında korunması önemlidir. 5062/01/EN/Final WP 89 sayılı Karar'ın uygulama alanı; işçilerin internet ve e-posta kullanımının gözetlenmesi, çalışma esnasında kameralarla gözetlenmesi ya da konumlarının çeşitli araçlar yardımıyla tespit edilerek gözetlenmesini içermektedir. Bu gözetim faaliyeti sırasında elde edilen kişisel verilerin, geçerli bir amaç için ve gerekli olduğu kadarının toplanması gerekmektedir. İşçinin kişisel verileri, özel hayatına mümkün olduğu kadar az müdahale edilecek biçimde toplanmalı ve işlenmelidir. İşçilere ait kişisel verilerin yalnızca işyerinde çalıştıkları sırada toplanması yeterli değildir. İşçinin çalışırken ortaya koyduğu çalışma performansının değerlendirilmesi için işe girmeden önceki verilerinin de kayıt altına alınması önemlidir. Ancak işveren, işçisi işten çıktıktan sonra da bu kişisel verileri korumakla yükümlüdür (5062/01/EN/Final WP 89 sayılı Karar, s. 2-5).

İşçilere ait kişisel verileri işleyen işverenlerin, dikkat etmesi gereken yedi tane ilkeden bu belgede söz edilmiştir. Öncelikle işçilere ait bilgiler açık ve yasal bir şekilde toplanarak belirlenen amaç doğrultusunda işlenmelidir. İkinci ilke uyarınca işçiler, işverenlerin bu bilgileri ne amaçla kullanacağını bilmelidir. İşçilerin, kendilerine ait verilerin toplanması için açık ve kesin olarak onay vermiş olması ve verilerin yasal bir amaç için kullanılması gerektiği üçüncü ilkede düzenlenmiştir. Dördüncü ilkede işverenlerin topladığı verilerin orantılı olması, gereksiz bilgilerin toplanmaması gerektiği vurgulanmıştır. Beşinci ilkede, işverenlerin bu verileri daima güncel tutması gerektiği hakkındaki düzenleme yer almaktadır. İşverenler, işçilere ait bu bilgilerin, başka kişilerin eline geçmemesi için önlemler almakla yükümlüdür. Sonuncu ilkede ise; işçilere ait veriler eğer işveren tarafından değil de işverenin görevlendirdiği başka bir personel tarafından toplanıyorsa, bu personele veri toplama ve saklama alanında gerekli eğitimlerin verilmesi gerekmektedir (5062/01/EN/Final WP 89 sayılı Karar, s. 3).

Çalışma grubu, 5062/01/EN/Final WP 89 sayılı Karar'ın, 95/46/EC sayılı Direktif kapsamında ele alınması gerektiğini belirtmiştir. Daha önce bahsettiğimiz gibi, 95/46/EC sayılı Direktif; kişilerin verilerinin toplanması, gerektiğinde işlenmesi ya da dosyalar halinde saklanması bağlamında kişilere ait kişisel verilerin ve kişilerin özel hayatın gizliliğinin korunmasına yönelik bir belgedir. Bu Karar metnindeki işçilere ait bilgilerin çeşitli siber gözetim araçları yardımıyla işverenlerce toplanması, işlenmesi ya da depolanması faaliyeti 95/46/EC sayılı Direktif ile paralellik göstermektedir (5062/01/EN/Final WP 89 sayılı Karar, s. 6-7; Savaş, 2009, s. 104). Sonuç olarak 5062/01/EN/Final WP 89 sayılı Karar; 95/46/EC sayılı Direktif'te yer alan düzenlemelerin, işçilere karşı işverenler tarafından gerçekleştirilen siber gözetim faaliyetinin çalışma hayatında uygulanmasına karşılık gelmektedir (Tekergül, 2010, s. 36).

Çalışma grubuna ait bir diğer karar ise, 29/5/2002 tarihli ve 5401/01/EN/Final WP 55 sayılı "İşyerindeki Elektronik İletişimin Gözetlenmesi Kararı"dır. Bu Karar metni 95/46/EC ve 97/66/EC sayılı Direktif kapsamında kabul edilmiştir (5401/01/EN/Final WP 55 sayılı Karar, s. 3).

5401/01/EN/Final WP 55 sayılı Karar; işyerlerindeki internet ve e-posta kullanımı üzerinden gerçekleştirilen siber gözetim faaliyetine yönelik minimum düzeyde düzenlemelerin yapılmasına rehberlik etmektedir. Çalışma hayatında işverenler; hangi siber gözetim aracını kullanarak hangi amaçla gözetim yaptığını işçisine bildirmekle

yükümlüdür. 5401/01/EN/Final WP 55 sayılı Karar uyarınca; gizli siber gözetim faaliyetini haklı çıkaracak sebepler olmadığı müddetçe işverenler, gözetimi gerçekleştirdiklerini işçilerine açıklamak durumundadır (5401/01/EN/Final WP 55 sayılı Karar, s. 4-5).

Çalışma grubu, hazırlamış olduğu 5401/01/EN/Final WP 55 sayılı Karar metninde, e-posta üzerinden siber gözetime yönelik bir çözüm önermiştir. Buna göre; işverenler, işçilerine iki farklı e-posta hesabı vermelidir. Bunlardan birincisi, bu Karar'da yer alan düzenlemeler çerçevesinde siber gözetim uygulamasının yapılabileceği bir e-posta adresi olarak kullanılmalıdır. Diğer e-posta adresi ise; yalnızca özel durumlar söz konusu olduğunda kötüye kullanım olup olmadığının tespit edilebilmesi için işverenler tarafından kontrol edilecektir (5401/01/EN/Final WP 55 sayılı Karar, s. 5).

5401/01/EN/Final WP 55 sayılı Karar, AİHS'nin 8. maddesini temel almıştır. Bu madde uyarınca; "Bireylerin özel ve aile hayatının, oturduğu evinin ve kurduğu iletişiminin kendisine ait bir hak olduğu ve bu hakka saygı duyulması gerektiği" belirtilmiştir. Kişinin sahip olduğu bu hakkı kullanmasını kamusal kurum, kuruluş ya da kişilerin engelleyemeyeceği; yalnızca birtakım istisnai durumların meydana gelmesi sonucunda bu hakka müdahale edilebileceği 5401/01/EN/Final WP 55 sayılı Karar uyarınca belirtilmektedir (Şimşek, 2008, s. 30-31).

5401/01/EN/Final WP 55 sayılı Karar metni, yedi temel ilkeden oluşmaktadır. Birinci ilke gereğince işverenler, uygulayacakları siber gözetimin gerekliliğini tespit etmek durumundadır. Siber gözetim faaliyeti eğer çok gerekli değilse, uygulanmaması tavsiye edilmektedir. İşverenler aynı zamanda, işçilerinin mahremiyet hakkının korunması için daha az oranda müdahaleci olan siber gözetim yöntemini tercih etmelidir. İkinci ilke, siber gözetimin amacının kesin olarak belirlenmesidir. İşverenler, belli bir amaç çerçevesinde ve yasal bir biçimde siber gözetimi gerçekleştirmek zorundadır. Üçüncü ilke şeffaflığı temel almaktadır. Bu ilke uyarınca işverenler, işçilerinin e-postalarını gizli bir şekilde gözetleyemezler. İşverenler, yaptığı siber gözetim faaliyetini hakkında işçiyi mutlaka bilgilendirmek zorundadır. İşçiler aynı zamanda, kendilerine ait bilgileri inceleyerek eksiklik ya da yanlışlık olması durumunda bu bilgilerin değiştirilmesini talep etme hakkına sahip olacaktır. Dördüncü ilke doğrultusunda işverenler, işyerinin korunması gibi belirli bir amaç kapsamında kişisel verileri işlemeyebilecektir. Benzer bir biçimde işçinin, iş ve işyeri hakkındaki bilgileri

rakip şirketlere verme riskine karşılık işverenler, gözetim faaliyetini gerçekleştirebilecektir. Beşinci ilkeye göre, işverenlerin gözetim faaliyetini gerçekleştirirken işçinin özel hayatına en az derecede müdahale edecek biçimde hareket etmesi gerekmektedir. Buradan hareketle işverenler, işyerinin güvenliği söz konusu olmadığı müddetçe işçileri sürekli olarak gözetleme hakkına sahip olamamaktadır. Bu nedenle işçilerin çalışma esnasında ziyaret ettiği her web sitenin gözetlenmesi yerine sakıncalı içeriğe sahip sitelerin belirlenmesiyle sadece o sitelerin ziyaret edilmesine yönelik bir siber gözetim faaliyeti gerçekleştirilmelidir. İşverenler, işçinin bu sitelere erişiminin engellenmesi yoluna da başvurulabilecektir. Altıncı ilkeye göre; işçilerin e-postalarında yer alan verilerin işverenler tarafından saklanırken güncel tutulmasına dikkat edilmesi gerekmektedir. Aynı zamanda e-postada yer alan bu veriler işverenler tarafından belli bir süre sistemde depolanmalı, sürenin dolmasıyla imha edilmelidir. Sonuncu ilkede ise, güvenlik konusuna değinilmektedir. Buna göre işverenler, toplayıp depoladıkları kişisel verilerin korunmasını sağlamalıdır. İşverenler, herhangi birinin bu bilgilere erişememesi adına gerekli önlemleri almakla yükümlüdür (5401/01/EN/Final WP 55 sayılı Karar, s. 13-19; Okur, 2013, s. 46-49).

Bir diğer çalışma grubu kararı, 11 Şubat 2004 tarihinde alınmıştır. 11750/02/EN WP 89 sayılı "Video Sistemleri Kullanılarak Yapılan Gözetim Faaliyetiyle Kişisel Verilerin İşlenmesi Kararı" ile son yıllarda kullanımı giderek yaygınlaşan kamera sistemleri ve ses kaydı, parmak izi alma gibi tekniklerle yapılan siber gözetim faaliyetine yönelik düzenlemeler yapılmıştır. Daha önce bahsettiğimiz kararlarda olduğu gibi bu karar da 95/46/EC sayılı Direktif kapsamında değerlendirilmektedir (11750/02/EN WP 89 sayılı Karar, s. 1-4).

İşverenlerin kameralar yardımıyla yaptığı siber gözetim faaliyetinin amacı üretimin arttırılması ya da iş güvenliğinin sağlanmasıysa bu durumda yapılan gözetimle işçilerin verilerinin toplanması meşru sayılabilmektedir. Bunun yanı sıra işverenler, işçilerin performansının incelenmesi ve verimliliklerinin saptanması açısından siber gözetim faaliyetine başvuruyorsa, gözetimin bu türü 11750/02/EN WP 89 sayılı Karar uyarınca meşru değildir (11750/02/EN WP 89 sayılı Karar, s. 25).

11750/02/EN WP 89 sayılı Karar metni uyarınca; işyerinde işçilerin özel amaçla kullanılması için ayrılmış olan alanlarda, tuvaletlerde, varsa duş alma yerlerinde, işçilere tahsis edilmiş kilitli dolaplarda ve işçilerin dinlenmesi için ayrılmış alanlarda işverenlerin kameralarla gözetim yapmasına yönelik izin bulunmamaktadır. Buna ek

olarak; işyerinin korunması ve işyerinde işlenecek ağır suçlara engel olmak, bu suçları tespit ve takip etmek için kamerayla siber gözetim faaliyeti yapılıyorsa, elde edilen bu kamera görüntülerindeki basit suçlar üzerinden işçilere ceza verilmesi mümkün olmamaktadır. İşverenler, kameralarla işçileri izliyorsa, bu siber gözetim faaliyetinin yapıldığını işçilerine bildirmek durumundadır. Bilgilendirme işlemi, işyerinin çeşitli yerlerine levhalar konmak suretiyle yapılabilecektir. Siber gözetimin kim tarafından gerçekleştirildiği, neden gözetim faaliyeti yapıldığı ve ne kadar zaman boyunca kayıt işleminin devam ettiği gibi bilgilerin işçilere açık ve net bir biçimde verilmesi gerekmektedir (11750/02/EN WP 89 sayılı Karar, s. 25; Okur, 2013, s. 50).

Son olarak, 8 Haziran 2017 tarihinde çalışma grubu tarafından bir başka karar metni kabul edilmiştir. 17/EN WP 249 sayılı "İşyerinde Verilerin İşlenmesi Kararı" yukarıda bahsettiğimiz 5062/01/EN/Final WP 48 ve 5401/01/EN/Final WP 55 sayılı Kararları tamamlayıcı özelliktedir. Bu belge yardımıyla işçilerin, çalışma hayatında toplanan kişisel verilerinin daha sistemli bir biçimde işlenmesi sağlanmaktadır. 95/46/EC sayılı Direktif ile bu belgedeki düzenlemeler paralellik göstermektedir (17/EN WP 249 sayılı Karar, s. 3-5).

17/EN WP 249 sayılı bu Karar uyarınca; işyerindeki elektronik iletişim araçlarının yanı sıra analog iletişim araçları da bu belgedeki düzenlemeler kapsamında yer almaktadır. Dolayısıyla sadece bilgisayarlar üzerinden yapılan iletişimdeki değil, tuşlu ofis telefonlarıyla yapılan iletişimdeki kişisel verilerin korunması da aynı derecede önem taşımaktadır. Buna ek olarak, evden çalışan işçilerin kişisel verilerinin korunması da bu belge kapsamına alınmıştır. Teknolojideki gelişmelerle birlikte artık işçiler, sadece işyerinde değil aynı zamanda evden de işini yapabilmektedir. Bu anlamda işverenlerin hem işini koruması hem de işçilerinin kişisel verilerini ve özel hayatının gizliliğini muhafaza etmesi gerekmektedir (17/EN WP 249 sayılı Karar, s. 4).

Çalışma grubu tarafından düzenlenmiş 17/EN WP 249 sayılı bu Karar uyarınca, işverenler işçilerinin verilerini gerekli olduğu ölçüde ve yasal bir biçimde işleme hakkına sahiptir. İşveren tarafından kararlaştırılan bir amaç doğrultusunda ve belli bir süre boyunca işçilere ait veriler toplanabilmektedir. Bu sürenin aşılmamasına işverenlerin dikkat etmesi gerekmektedir. İşverenler, işçileri verilerinin toplandığı konusunda bilgilendirmekle yükümlüdür. Dolayısıyla işçiler, kendilerine ait bu bilgilerde bir eksiklik ya da hata fark ettiklerinde, verilerin değiştirilmesini ya da silinmesini talep edebilme hakkına sahiptir. Son olarak işverenler, verilerin başkaları

tarafından kötüye kullanılmasına karşı önlem almak durumundadır (17/EN WP 249 sayılı Karar, s. 5).

2.1.5.5. 2016/679 Sayılı Genel Veri Koruma Yönetmeliği

25 Mayıs 2016 tarihinde yürürlüğe giren; "Genel Veri Koruma Yönetmeliği", AB'nin 95/46/EC sayılı Direktif'inin yerine geçmiştir. Bu yönetmeliğin 5. maddesi uyarınca kişisel veriler; "Yasalara uygun, adil ve şeffaf bir biçimde işlenmek durumundadır". Kişisel verilerin toplanabilmesi için yasal ve açık bir amaç olması gereklidir. Belirlenen amaca uygun şekilde verilerin toplanması ve işlenmesi mümkün olabilecektir. Bu bağlamda verilerin minimize edilmesi gerekmektedir. Diğer bir ifadeyle veriler, amaca uygun oranda toplanmalıdır. Amaç dışındaki verilerin toplanmaması gerekmektedir. İşlenen bu veriler, her daim güncel tutulmalı ve gerçek bilgilerden oluşmalıdır. Bilgilerde herhangi bir eksiklik ya da yanlışlık bulunması durumunda, silinmesi ya da düzeltilmesi işlemi yapılmalıdır. Kişisel verilerin işlenme amacı sona erdiğinde, veriler depolanmaya ya da işlenmeye devam edilmemelidir. Son olarak verileri işleyen kişiler, verilerin güvenliğini sağlamakla yükümlüdür (2016/679 sayılı Yönetmelik, m. 5).

Genel anlamda kişisel verilerin korunmasını içeren düzenlemelere yer veren 2016/679 Sayılı Yönetmeliğin 88. maddesinde işçilere ait kişisel verilerin işlenmesine yönelik düzenleme yer almaktadır. Bu maddenin birinci fıkrasına göre; "AB üyesi devletler; kişilerin işe alınması, işveren tarafınca işin planlanması ve yönetilmesi, işçinin çalışma esnasındaki performansının değerlendirilmesi ve işçinin sağlığı ile güvenliğinin korunması gibi hak ve menfaatler için işçilerin kişisel verilerinin işlenebilmesine yönelik düzenlemeler yapmalıdır. Bu düzenlemelere ülkeler, ulusal yasalarında ya da toplu iş sözleşmelerinde yer vermekle yükümlüdür (2016/679 sayılı Yönetmelik, m. 88)".

2016/679 Sayılı Yönetmeliğin devletlere, işçilerin kişisel verilerini korunması anlamında görev yüklediği görülmektedir. İşverenin ya da işçinin hak ve menfaatlerinin gözetildiği durumlarda işyerinde siber gözetim faaliyeti yapılması mümkün olacaktır. İşverenin, siber gözetim faaliyetini kötüye kullanmasının önüne ulusal düzenlemelerle geçilmesi üye devletlerin sorumluluğunda olacaktır.

2.2. Karşılaştırmalı Hukuktaki Yasal Düzenlemeler

Siber gözetim faaliyeti ve kişisel veriler arasında önemli bir bağ olduğunu önceki bölümde belirtmiştik. Siber gözetim faaliyetini gerçekleştiren işverenler, belirli bazı amaçlar doğrultusunda işçileri hakkındaki kişisel verileri toplamaktadır (Lyon, 2006'dan aktaran Bölükbaş, 2014, s. 46). İşyerinde uygulanan siber gözetim faaliyetine ilişkin her ülkenin mevzuatında farklı düzenlemeler mevcuttur. Bu düzenlemelerin bir bölümü siber gözetim faaliyetini esas alarak hazırlanmıştır. Diğer bölümü ise, kişisel verilerin ve özel hayatın korunması hakkı çerçevesinde oluşturulmuştur.

Çalışmamızın bu bölümünde seçilmiş beş ülkenin siber gözetim faaliyetine ilişkin düzenlemeleri incelenecektir. Bu ülkelerden birincisi olan Fransa'da, on altıncı yüzyıl ile on yedinci yüzyıl arasında uygulanan ve Fransız sosyolog Foucault tarafından *Büyük Kapatılma* adı verilen gözetim faaliyeti, günümüzdeki siber gözetim faaliyetinin gelişmesinde etkili olmuştur. Gözetimin faaliyetinin doğduğu ve geliştiği ülkelerden biri olarak adlandırabileceğimiz Fransa'da günümüzde uygulanan siber gözetim faaliyetine ilişkin koruyucu düzenlemelerin incelenmesi önem arz etmektedir.

"İnsan onurunun, hiç kimse tarafından dokunulamayacak kadar değerli bir hak" olduğunu savunan Almanya ise, kişisel verilerin korunmasına yönelik düzenleme yapan ilk ülke olarak bilinmektedir. Dünya genelinde kişisel verilerin korunması kapsamında ilk olma özelliğini taşıyan Almanya'nın, işyerinde siber gözetim faaliyetine ilişkin yaptığı düzenlemeler de tarafımızca incelenecektir.

1996 yılına kadar kanunlarında kişisel verilerin korunmasına yönelik düzenleme bulunmayan İtalya ise, 2015 yılında İş Kanunu'unda yapılan değişiklikle işyerinde siber gözetim faaliyetinin sürekli olarak uygulanmasını engellemiştir. Mevzuatta yakın zamanda yapılan bu değişiklik ile işçinin gözetime karşı korunması sağlanmıştır. Bu bağlamda İtalya'daki mevzuatın incelenmesi önemlidir.

2018 yılında İngiltere Enformasyon Komisyonu tarafından yapılan bir araştırmanın sonucuna göre, ülke genelinde dört buçuk milyona yakın kapalı devre kamera sistemi tarafından gözetim faaliyeti gerçekleştirilmektedir. İngiltere'nin nüfusuyla orantılandığında her on dört kişiye bir kamera düştüğü belirtilmektedir. Bu araştırma sonucu göz önüne alındığında, İngiltere'de çalışma hayatının yanı sıra günlük hayatta da gözetim faaliyetine başvurulduğu görülmektedir (http-76). Gözetimin bu kadar yoğun olduğu İngiltere'de, kişileri gözetim faaliyetine karşı korumak için yapılan düzenlenmelerin incelenmesi tarafımızca gerekli görülmüştür. Bütün bunlara ek olarak,

Fransa'yla benzer biçimde İngiltere de gözetim faaliyetinin geçmişten günümüze gelmesinde önemli bir rol oynamıştır. İngiliz filozof Bentham'ın bu gözetim faaliyetinden etkilenerek İngiltere'de tasarladığı Panoptikon gözetim kulesi yıllar içerisinde siber gözetim faaliyetinin artmasını sağlamıştır. Gözetimin ortaya çıktığı ülkelerden biri olarak düşünülen İngiltere'de, siber gözetim faaliyetine ilişkin düzenlemelerin olup olmadığının incelenmesi yerinde olacaktır.

Son olarak, ABD'nin hukuk sistemi Anayasa, eyalet kanunları ve mahkeme kararlarının oluşturduğu üçlü bir yapıdadır. ABD, siber gözetim ve kişisel verilerin korunmasına yönelik düzenlemelere sahiptir. Ancak çoğu zaman işçiler, kişisel verilerinin ve özel hayatlarının gizliliğinin ihlal edildiği gerekçesiyle mahkemeye başvurmaktadır. Bu bağlamda ABD'de, siber gözetim faaliyetine ilişkin birçok mahkeme kararı yer almaktadır. Dolayısıyla ABD'deki üçlü hukuksal yapıda siber gözetim faaliyetine ilişkin düzenlemelerin incelenmesi tarafımızca gerekli görülmüştür.

2.2.1. Fransa

Siber gözetim faaliyetine ve işçilerin kişisel verileri ile özel hayatının korunmasına yönelik düzenlemeler açısından Fransa, diğer AB üyesi ülkelere kıyasla yetersiz kalmaktadır (Dabosville, 2013, s. 31).

4 Ekim 1958 tarihinde kabul edilen Fransız Anayasası'nda özel hayatın gizliliği ve kişisel verilerin korunmasına yönelik özel bir hüküm yer almamaktadır (Korkmaz, 2017, s. 217). Kişisel verilerin korunmasına yönelik Fransa'nın mevzuatında yer alan ilk düzenleme 1978 tarihinde yapılmıştır. 6/1/1978 tarihli ve 78-17 sayılı "Bilgi Teknolojisi, Veri Dosyaları ve Temel İnsan Hakları" adıyla bilinen bu Kanun, kişisel verilerin korunması bağlamında önemli bir rol üstlenmiştir (Korkmaz, 2017, s. 218). On üç temel bölüm ve yetmiş iki maddeden oluşan bu Kanun gereğince; "Bilgi teknolojileri her insanın hayatına hizmet etmelidir. Ancak bu teknolojiler kişilerin temel hak ve özgürlüklerini ihlal etmeyecek bir biçimde kullanılmalıdır (http-55)".

Bu Kanun; "Sadece otomatik olarak değil elle işlenen verilerin de korunmasını öngörmektedir (78-17 sayılı Kanun, m. 2)". Bu bağlamda Kanunun birinci bölümünde veri işlemeye yönelik ilkeler ile bu Kanun çerçevesinde bilinmesi gereken kişisel veri, veri denetleyicisi gibi birtakım kavramların tanımları verilmiştir (http-55).

İkinci bölümde kişisel verilerin işlenmesinin hukuki boyutu ele alınmıştır. Kanun'un 6. maddesinde yer alan bu hükümler, daha önce bahsettiğimiz uluslararası belgelerde geçen hükümlerle paralellik göstermektedir. İlgili madde uyarınca; "Kişisel

verilerin adil ve yasal biçimde işlenmesi gerekmektedir. Bununla birlikte veriler, belirlenmiş yasal ve açık bir amaç doğrultusunda işlenmelidir. Toplanacak veriler aşırıya kaçmamak kaydıyla, amaca uygunluk gösterecek miktarda toplanmalıdır. Aynı zamanda bahsi edilen kişisel verilerin her daim eksiksiz, doğru ve güncel bir biçimde tutulması şartı bulunmaktadır. Son olarak, belirlenen amaca uygun olan süre boyunca verilerin işlenmesi gerekmektedir. Bu süre dolduğunda, veri işleme faaliyeti durdurulmalıdır. Kanun uyarınca, veri sahibinin onayı doğrultusunda verilerin işlenmesi gerektiği düzenlenmesi yapılmıştır (78-17 sayılı Kanun, m. 6 ve m. 7)".

İşlenecek verilerin neler olamayacağına ilişkin düzenleme, madde 8'de yer bulmuştur. Buna göre; "Kişilerin ırkına ya da etnik kökenine, dini ve felsefi inancına, siyasi görüşüne, sendika üyeliğine ve cinsel hayatı ile sağlığına yönelik bilgilerin elde edilmesi, işlenmesi ya da depolanması yasaklanmıştır (78-17 sayılı Kanun, m. 8)".

Bu Kanun'un 11. maddesi uyarınca, Fransız Veri Koruma Komisyonu (Commission Nationale de l'Informatique et des Libertés – CNIL) kurulmuştur. Komisyon, Fransız devletinden bağımsız idari bir makam olarak var olmaktadır. Bu Komisyon'un amacı 11. maddede açıklanmıştır. Buna göre Komisyon; verileri işleyen kişilere sahip oldukları hak ve görevleri anlatmakla yükümlüdür. Aynı zamanda bu Komisyon, kişisel verilerin işlenmesi faaliyetinde 78-17 sayılı "Bilgi Teknolojisi, Veri Dosyaları ve Temel İnsan Hakları Kanunu" hükümlerine uygun davranmakla yükümlü olacaktır (78-17 sayılı Kanun, m. 11).

1978 tarihinde kabul edilen bu Kanun, ilerleyen yıllarda yapılan düzenlemelerle AB'nin 95/46/EC sayılı Direktif'ine uyumlu hale getirilmiştir. 78-17 sayılı Kanun üzerinde yapılan son değişiklik 2/8/2015 tarihli ve 2015-948 sayılı Kanunla tarafından gerçekleştirilmiştir. Bu bağlamda, 78-17 sayılı Kanun tüzel kişileri kapsam dışı bırakmıştır (Korkmaz, 2017, s. 218). Buna ek olarak, verileri işleyen kişilerin sorumlulukları 32. maddede yer bulmuştur. "Verileri toplamakla yükümlü olanlar, veri sahiplerini bilgilendirmek durumundadır". 32. madde uyarınca; "Verilerin kim tarafından toplanacağı, veri toplayan kişinin adresi ve hangi amaçla verileri işleyeceği gibi bilgiler veri sahibine verilmelidir". Buna ek olarak; verileri işleyen kişiler, bu durumu CNIL'ye bildirmekle yükümlüdür (78-17 sayılı Kanun, m. 32).

78-17 sayılı Kanun'un 8. maddesinde ise; "Kişinin ırkına, etnik kökenine, dini ve siyasi görüşüne, hangi sendikaya üye olduğuna ve cinsel hayatına ilişkin verileri özel

veri kategorisinde sayılmaktadır ve bu verilerin işlenmesi yasaklanmıştır (Korkmaz, 2017, s. 219)".

78-17 sayılı Kanun'un yanı sıra, 17/7/1970 tarihli ve 70-643 sayılı Fransız Medeni Kanunu'nun 9. maddesinde; "Her vatandaşın özel hayatına saygı gösterilmesi hakkına sahip olduğu düzenlenmiştir (Abrahamse, 2014, s. 27)". Ancak ne 78-17 sayılı Kanun'da ne de 70-643 sayılı Fransız Medeni Kanunu'nda özellikle işçilerin kişisel verilerinin işlenmesi hakkını koruyan herhangi bir düzenlemeye yer verilmemiştir.

1992 yılı itibarıyla Fransız İş Kanunu'nda yapılan bazı değişiklik doğrultusunda işyerinde siber gözetim faaliyetine karşı işçilerin kişisel verilerinin ve özel hayatının gizliliğinin korunması sağlanmaya çalışılmıştır (Savaş, 2009, s. 109).

Fransız İş Kanunu'nun L121 – 8 maddesine göre; "İşçilere, kişisel verilerinin toplandığı bilgisi verilmeksizin, işverenler tarafından herhangi bir veri toplama faaliyetinin gerçekleştirilmesi mümkün olmamaktadır. Veri toplama faaliyetini yürüten işverenler, bu durumu CNIL'ye bildirmekle yükümlüdür (Abrahamse, 2014, s. 28)". İlgili Kanun'daki L722 – 35 maddesi gereğince; "İşverenler, siber gözetim faaliyetini *iyi niyet* unsuruna uygun bir biçimde gerçekleştirmelidir. İşçinin aleyhine sonuç doğuracak bir gözetim faaliyeti yerine, iyi niyetli bir tutum çerçevesinde, örneğin işçiyi tacizden koruma gibi amaçlarla işyerinde gözetim yapmalıdır (Abrahamse, 2014, s. 28)".

Fransız İş Kanunu'nda üç temel ilke bulunmaktadır. *Şeffaf olma, kolektif halde katılım* ve *ölçülü olma* şeklindeki bu üç temel ilke ile işçilerin işyerinde izlenmesi faaliyeti düzenlenmek istenmiştir (Tekergül, 2010, s. 46). L120 – 2 maddesindeki *ölçülü olma* ilkesi uyarınca; "Hiç kimse, bireysel veya kolektif özgürlüklere gözetim faaliyetinin amacıyla örtüşmeyecek biçimde sınırlama getiremeyecektir. Bu ilkeyle işverenlerin, gözetim faaliyeti uygulamaları doğrultusunda işçilerini kısıtlamasının önüne geçilmek istenmiştir (Okur, 2013, s. 54)".

L121 – 8 maddesindeki *şeffaflık* ilkesine göre; "İşverenler, işçi ya da işçi adaylarına haber vermeksizin hiçbir kişisel veriyi toplama hakkına sahip olamayacaktır". Bu ilkede önemli olan iki unsur yer almaktadır. Birinci unsur, ilkenin sadece işçiler için değil aynı zamanda işe alınma evresindeki işçi adayları açısından da geçerli olmasıdır. İkinci unsur ise, işçi ve işçi adaylarına kişisel bilgilerinin işleneceğinin bilgisinin verilmesidir. İşveren bu iki unsura uymak zorundadır. Kişisel verilerde yanlışlık ve eksiklik olması durumunda işçilerin, ilgili verileri düzelttirme

talebinde bulunabileceğini de yine işverenler, işçilere bildirmekle görevlidir (Okur, 2013, s. 54; Abrahamse, 2014, s. 27).

Son olarak L432 – 2 ve 432 – 2 – 1 maddelerinde düzenlenmiş olan *kolektif halde katılım* ilkesi gereğince; "İşverenler, işçileri gözetleyecekleri araçları seçmeden önce bu konuyla ilgili olarak işyeri komitesine ile diğer temsilcilere haber vermek ve danışmak zorundadır". Bu düzenlemeyle birlikte, kullanılacak olan siber gözetim araçlarını işverenlerin kendi isteği doğrultusuna seçmesinin önüne geçilmeye çalışılmıştır (Okur, 2013, s. 54; Abrahamse, 2014, s. 27).

Fransız ulusal hukuk sisteminde kişisel verilerin gizliliği hakkının ihlal edilmesine yönelik yaptırımlar 1/3/1994 tarihli ve 80-538 sayılı Fransa Ceza Kanunu'nda düzenlenmiştir. Ceza Kanunu'nun 226 – 16 numaralı maddesi, 2016 yılı itibarıyla değişikliğe uğramıştır. 2016 – 731 sayılı "Organize Suç, Terörizm ve Finansmanı ile Mücadeleyi Güçlendirmek ve Ceza Muhakemesi Prosedürünün Etkinliğini ve Güvencelerini Arttırmak" isimli Kanun'daki 117. maddeyle değiştirilmiştir. 2016 – 731 sayılı Kanun'un 117. maddesine göre; "Kanuna aykırı bir biçimde kişisel verilerin işlenmesi durumunda, verileri işleyen kişiye beş yıl hapis cezasına ek olarak üç yüz bin Euro para cezası kesilecektir". 78 – 17 sayılı Bilgi Teknolojisi, Veri Dosyaları ve Temel İnsan Hakları Kanunu'nda yer alan 45. maddeye aykırı davrananlar da aynı cezaya hükmedilecektir. İlgili Kanun'un 45. maddesine göre; "CNIL, 78 – 17 sayılı Kanun'a uymayanları uyarmakla görevlendirilmiştir". CNIL'nin yaptığı uyarıya uymayan işverenler, 78 – 17 sayılı Kanun'un 22. maddesi gereğince "CNIL, ilgili kişinin veri işleme faaliyetini durduracak ya da 25. madde gereğince kişiye verilen veri işleme görevi sonlandırılacaktır". Bu iki maddeye uyulmadığı durumda ise Fransız Ceza Kanunu'nun 226 – 16 numaralı maddesindeki ceza verilecektir (Korkmaz, 2017, s. 219).

80-538 sayılı Fransız Ceza Kanunu'nun 226 – 18 numaralı maddesinde; "Kişisel verilerin hileyle, haksız yollarla ya da yasalara aykırı biçimde toplanması sonucunda, verileri toplayan kişilere verilecek cezalar düzenlenmiştir". Bu kişilere, beş yıl hapis cezasına ek olarak üç yüz bin Euro para cezası verilecektir. 226 – 19 numaralı madde uyarınca; "Kişilerin ırkına ya da etnik kökenine, siyasi görüşüne, dini ve felsefi inancına, sendika üyeliğine ve cinsel hayatı ile sağlına ilişkin bilgileri, veri sahibinin rızası olmadan elektronik araçlara kaydedenlere yine beş yıl hapis cezası ve üç yüz bin Euro para cezası verilecektir (Korkmaz, 2017, s. 220)".

Son olarak, Fransız Temyiz Mahkemesi tarafından verilmiş olan bir karara bakmak yerinde olacaktır. 2002 yılında gerçekleşen olayda işçi Frederic Onof, iş saatleri içerisinde interneti kişisel amaçlarına hizmet edecek şekilde kullanarak e-posta göndermiştir. Bu e-postaların gözetimini yapan işvereni ise, Onof'un iş sözleşmesini feshetmiştir. Ancak Temyiz Mahkemesi, işçisinin kişisel e-postalarına gizli ve yasal olmayan şekillerde erişim sağlayan işvereninin, haberleşme gizliliğini ihlal ettiğine karar vermiştir. Mahkemece çalışma saatleri esnasında olsa dahi işverenin, işçinin kişisel yazışmalarına erişimin mahremiyet hakkına ihlal teşkil ettiği belirtilmiştir. Temyiz Mahkemesi ilgili kararı alırken AİHS'nin 8. maddesi ve Fransız Medeni Kanunu'nun 9. maddesi uyarınca hareket etmiştir (Abrahamse, 2014, s. 29; Savaş, 2009, s. 112; Okur, 2013, s. 54).

2.2.2. Almanya

Almanya'nın Anayasası (Grundgesetz für die Bundesrepublik Deutschland) 23 Mayıs 1949 tarihinde kabul edilmiştir. Bu Anayasanın ilk on dokuz maddesinde Alman vatandaşlarının temel hak ve özgürlüklerine ilişkin hükümler yer almaktadır (Can, 2004, s. 1).

Siber gözetim faaliyetiyle toplanan bilgilerin, kişisel veri kapsamında ele alınması gerektiğine daha önce değinmiştik. Özellikle Avrupa ülkelerinde kişisel verilerin korunması, temel insan hak ve özgürlüklerinden ayrı düşünülmemektedir. Bu bağlamda kişisel verilerin korunmasıyla birlikte kişinin hem özel hayatının ve mahremiyet hakkının hem de insan onurunun korunması amaçlanmaktadır (Dülger, 2018, s. 77).

Alman Anayasası'nın birinci maddesi kişilerin onur ve şerefinin korunmasına yönelik bir düzenleme içerdiği için önemlidir. Bu maddenin birinci fıkrasına göre; "Alman vatandaşlarının onuruna ve şerefine dokunulamaz. Alman Devleti, vatandaşlarının onur ve şerefini korumak ve saygı göstermekle yükümlüdür (Alman Anayasası, m. 1/1)". Kişisel verilerin korunması ile kişilerin onur ve şerefinin korunması birbirinden ayrı düşünülemeyecek haklar olduğu için Alman Anayasası'nın birinci maddesi önem arz etmektedir (Gören, 1992, s. 166).

Buna ek olarak, Alman Anayasası'nda ve mevzuatlarında işçilerin kişisel verilerinin gizliliğine dair herhangi bir düzenleme yer almamaktadır. Anayasa'nın 10. maddesi uyarınca kişilerin birbirleriyle gerçekleştirdikleri elektronik haberleşmelerin gizliliğinin ihlal edilemeyeceği düzenleme altına alınmıştır (Korkmaz, 2017, s. 223). Doğu ve Batı bloklarının birleşmesinden sonra Anayasa'ya veri gizliliğine yönelik özel

bir hüküm eklenmesi yönünde toplantılar gerçekleştirilmiştir. Ancak bu öneri muhafazakâr kesimce reddedilmiştir (Rodrigues, Wilson ve Schanz, 2001, s. 76).

Almanya, kişisel verilerin korunmasına ilişkin en kısıtlayıcı kanunlardan birine sahip olan AB ülkesi olarak bilinmektedir. Ancak kişisel verilerin korunmasıyla ilgili dünya çapında ilk ulusal düzenlemeyi yapan ülke de Almanya'dır. 1970 yılında Hessen eyaletinde ilk "Veri Koruma Kanunu (Datenschutzgesetz – DSGVO)" kabul edilmiştir. 1977 yılı itibarıyla ise "Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz – BDSG)" yürürlüğe konmuştur. Seksen beş maddeden oluşan bu Kanun'un amacı; "Tamamı ya da bir kısmı otomatik şekilde işlenen kişisel verilerin korunmasını sağlamaktır". Bu Kanun, 2002 yılında AB'nin 95/46/EC sayılı Direktif'iyle uyumlu hale getirilmiştir (Korkmaz, 2017, s. 224). Ancak bu Kanun'da işçi – işveren ilişkisindeki gözetim faaliyetine yönelik özel bir düzenleme bulunmamaktadır (BDSG, m. 1; Civelek, 2011, s. 9). Bu Kanun'un kabulüyle ilk kez, verilerin korunmasının sağlanması için "Federal Veri Koruma ve Bilgi Özgürlüğü Komisyonu (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)" kurulmuştur. Almanya kabul ettiği bu Kanun'unla dünya çapında kişisel verilerin korunmasına yönelik düzenlemelerin yapılmasına öncülük etmiştir. BDSG Kanunu'na göre; "Kişisel verileri işleyen kişiler bu durumu, Komisyon'a bildirmekle yükümlüdür". Kanun çerçevesinde; "Kişisel verilerin korunması için gereken tüm önlemler alınmak durumundadır (Civelek, 2011, s. 9; Korkmaz, 2017, s. 225)".

BDSG Kanunu uyarınca, işçilerin gözetlenmesi faaliyeti yalnızca sınırlı durumlarda yapılabilmektedir. Bu Kanun'un 26. maddesinde 23 Mayıs 2018 tarihinde yapılan düzenlemeye göre; "İşçinin suç işlemiş olduğuna ya da iş sözleşmesini ihlal ettiğine dair yazılı kanıt bulunuyorsa, suçun ortaya çıkarılması için kişisel verilerin işlenmesi faaliyeti gerekli olabilecektir (Aloisi ve Gramano, 2019, s. 19)". İşverenlerin, kameralar aracılığıyla işyerinde sürekli olarak gözetim faaliyetini gerçekleştirmesi yasaktır. Bunu yapan işverenlere para cezası verilmektedir. Kesintisiz olarak telefon görüşmelerini dinleme ya da kameralarla izleme faaliyeti yalnızca belirli amaçlar çerçevesinde uygulanabilecek yöntemlerdir. Örneğin; işin kalitesinin arttırılması için müşterilerle yapılan konuşmaların kayıt altına alınması bu bağlamda ele alınabilmektedir. İşin kalitesini arttırma amacıyla olsa bile işverenler, gözetim faaliyetini aşırıya kaçmadan ve yasalara uygun bir biçimde gerçekleştirmekle yükümlüdür. 26. madde kapsamında; "İşçinin verilerini işleyen işverenler, işçiden onay

almak zorundadır". Buna ek olarak işverenler, gözetim faaliyetini gerçekleştirmeden önce işçiye, bu faaliyetle ilgili ayrıntılı bilgi vermelidir. Kanun'un 20. maddesi gereğince; "Elde edilen bilgilerin yanlış ve eksik olması durumlarında kişinin bu verileri sildirmeyi ya da düzelttirmeyi talep etmesi mümkündür (Korkmaz, 2017, s. 227)". Yine bu Kanun uyarınca işverenler, topladıkları kişisel verilerin başkalarının eline geçmemesi, kanun dışı amaçlarla kullanılmaması, kaybolmaması ve tahrip olmaması için gerekli önemli almakla yükümlüdür (http-56).

BDSG Kanunu uyarınca; "İnsanların dini ve felsefi inancı, siyasi görüşü, cinsel hayatı ve sağlığı ile sendika üyeliğine dair bilgileri özel nitelikli veriler kapsamında ele alınmaktadır ve bu bilgilerin işlenmesi veri sahibinin onayı yoksa yasaktır (Korkmaz, 2017, s. 226)".

Federal Veri Koruma Kanunu'nda iki temel ilke yer almaktadır. Söz konusu ilkeler *veriden uzak durma* ve *veri miktarını küçültme* şeklinde ifade edilebilir. Buna göre "İşverenler; amaca uygun ve yeterli miktardaki veriyi toplamalı, gereğinden fazla veri toplama faaliyetinde bulunmamalıdır. Diğer yandan işçilere ait bu verileri işverenler, olabildiğince anonim şekilde depolamalıdır (Oğuz, 2013, s. 12)".

15 Aralık 1983 tarihinde Alman Anayasa Mahkemesinin ülkede yapılan nüfus sayımına ilişkin kararı ise kişisel verilerin işlenmesi açısından emsal teşkil etmektedir. 1983 yılında, "Alman Nüfus Sayımı Kanunu" doğrultusunda kişilerden ayrıntılı biçimde veri toplanması talep edilmiştir. Toplanan bu kişisel verilerin istatistiksel açıdan işlenebilmesi için bilgilerin açıklanması istenmiştir. Ancak bu Kanun'un, insanların kişisel haklarına bir saldırı niteliği taşımakta ve kişilerin *şeffaflaşmasına* sebebiyet vermekte olduğu düşünülmüştür. Bu Kanun'a karşı açılan davada kişilerin kendilerine ait veriler üzerinde söz sahibi olması gerektiği kararı, Anayasa Mahkemesi tarafından verilmiştir. Kişiler, verilerin işlenmesi esnasında söz sahibi olma hakkına sahip olacaktır. Mahkemenin verdiği bu kararla birlikte kişilere ait bilgilerin elde edilmesi, işlenmesi, biriktirilmesi ya da başkalarına aktarılmasına karşı bireylerin korunmasının gerekliliği temel alınmıştır. Bu bağlamda Alman Anayasa Mahkemesi nüfus sayımı işleminin durdurulmasını kararını vermiştir (Şimşek, 2008, s. 115-116; Civelek, 2011, s. 86-87).

Federal Veri Koruma Kanunu'nun bazı maddelerinde, kişisel verilerin korunmasının ihlaline yönelik düzenlemeler yer almaktadır. Nitekim Kanun'un 43. maddesi verilecek idari cezaları, 44. maddesi ise adli cezaları düzenlemektedir.

Gözetimi gerçekleştiren kişi kastî olarak ya da ihmalle; bu faaliyeti yasal olmayacak şekilde gerçekleştirirse, gözetim faaliyeti hakkında gözetlenen kişiyi bilgilendirmezse, verileri korumak için gerekli tedbirleri almazsa, veri sahibinin verileri değiştirmeyi ya da sildirmeyi talep etmesini engellemeye kalkarsa Federal Veri Koruma Kanunu uyarınca cezaya çarptırılacaktır. Bu Kanun'un 43. ve 44. maddelerine göre, elli bin Euro ila üç yüz bin Euro arasında para cezası ya da iki yıla kadar hapis cezası alacaktır. Bu para cezasının tutarı belirlenirken, işverenin yıl içerisinde kazandığı paranın miktarı göz önünde bulundurulmaktadır. Kesilecek para cezası, işverenin bir yıllık kazancından daha fazla olacak şekilde ayarlanmaktadır (Korkmaz, 2017, s. 228-229).

13/11/1998 tarihli "Alman Ceza Kanunu (Strafgesetzbuch – StGB)" içerisinde kişisel verilerin ihlal edilmesine dair cezalar bulunmaktadır. Bu Kanun'un 201. maddesi uyarınca; "Kişinin özel konuşmalarını gizli biçimde kaydedenlere, üçüncü kişilerin bu kayıtlara ulaşmasını sağlayanlara ve konuşmanın içeriğini açık bir şekilde ifşa edenlere üç yıldan fazla olmayacak şekilde hapis cezası ya da para cezası verilmektedir (StGB, m. 201)".

18/1/1972 tarihli, işyeri kurullarına sahip işyerlerinde uygulanan "Betriebsverfassungsgesetz - BetrVG" isimli Kanun'un 87. maddesine göre; "Hem işyerlerinde bulunan işyeri kurulları hem de işverenler, işçinin gözetlenmesi faaliyetiyle ilgili önlemler almakla yükümlüdür. Aynı zamanda işverenler; işçinin çalışma sırasındaki davranışlarını ve çalışma performansını denetlemek amacıyla gözetim yapabilme hakkına sahip olacaktır. Bu gözetim faaliyetini gerçekleştirecek olan işveren, işyeri kurulunu bu faaliyet hakkında bilgilendirmeli ve kurulun onayını almakla yükümlü olacaktır (BetrVG, m. 87)".

Son olarak, Alman vatandaşlarının siber gözetim faaliyetiyle ilgili AİHM'ye başvurduğu bazı dava dosyalarına değinmek yerinde olacaktır. AİHM, gelen dava dosyalarını inceleme aşamasında 8. maddeden yararlanmaktadır. "Niemietz Almanya'ya karşı" isimli, başvuru numarası 13710/88 olan ve 16 Aralık 1992 tarihinde alınan kararın 29. paragrafına göre; kişinin özel hayatı, dış dünyadan ayrı düşünülecek kadar dar bir kavram değildir. Bu nedenledir ki, özel hayatın kapsamı içerisine iş alanı da dahil edilmelidir. Mahkeme gerek özel gerekse çalışma hayatı çerçevesinde yapılan telefon görüşmelerinin dinlenmesini özel hayata müdahale kapsamında değerlendirmiştir (Niemietz v. Germany adlı karar; Küzeci, 2010, s. 152).

"Klass ve diğerleri Almanya'ya karşı" adıyla bilinmekte olan, 5029/71 başvuru numaralı ve 6 Eylül 1978 tarihli karara göre, kişisel verilerin korunmasına ilişkin ilk ve aynı zamanda en önemli karar olma özelliğini taşımaktadır. Gerhard Klass adlı Alman vatandaşı ve bir grup insanın oluşturduğu grup, Alman Anayasası'nın 10. maddesinin ikinci fıkrasının ve bu madde esas alınarak düzenlenmiş olan "Mektup, Posta ve Telekomünikasyonun Gizliliğinin Sınırlandırılmasına İlişkin Kanun"un AİHS'yle ters düştüğü gerekçesiyle AİHM'ye başvurmuştur. Davayı açma gerekçeleri ise şu şekildedir: Alman devleti, halkı gözetleme hakkına sahiptir. Ancak, gözetlediği vatandaşlarını bu durumdan haberdar etmeden onları gözetlemeye devam etmektedir. Aynı zamanda gözetlenen kişilerin, devlete dava açma hakkı bulunmamaktadır. Tam olarak, vatandaşın devleti dava etme hakkının kısıtlanıyor olması da bu davanın temel sebebini oluşturmaktadır. AİHM, olay incelemesinin ardından bu kişilerin mağdur oldukları kanısına varmış ve telefonla yapılan konuşmaların gözetlenmesinin kişilerin özel hayatından bağımsız düşünülemeyeceğini belirtmiştir (Klass and Others v. Germany adlı karar; Küzeci, 2010, s. 153).

2.2.3. İtalya

22/12/1947 tarihli İtalya Anayasası'nda kişisel verilerin korunması ya da işyerinde siber gözetim faaliyetine yönelik herhangi bir koruyucu düzenleme yer almamaktadır.

İtalya, AK'nin 108 sayılı Sözleşmesi'ni 1981 yılında imzalamıştır. Ancak İtalya, 1996 yılına kadar kişisel verilerin korunmasına yönelik herhangi bir ulusal belge hazırlamamıştır. 31/12/1996 tarihli ve 675 sayılı "Kişisel Verilerin İşlenmesinde Bireylerin ve Diğer Konuların Korunmasına Yönelik Kanun" kabul edilmiştir. 675 sayılı bu Kanun'la AB'nin 95/46/EC sayılı Direktif'i de uygulamaya konmuştur. 675 sayılı Kanun'un yerini 1/1/2004 tarihli ve 196 sayılı "Kişisel Verilerin Korunması Kanunu" almıştır. Daha önce kişisel verilerin korunmasına ilişkin yapılmış olan tüm düzenlemeler, 196 sayılı Kanun'da toplanmıştır. Ancak 196 sayılı Kanun, AB'nin 2016/679 sayılı Genel Veri Koruma Yönetmeliği uyarınca güncellenmiştir (Korkmaz, 2017, s. 233; http-57).

2016/679 sayılı Yönetmelik'in 5. maddesinde düzenlenmiş olan veri koruma ilkeleri, İtalyan mevzuatına aktarılmıştır. Buna göre; kişisel veriler yasalara uygun, adil ve şeffaf bir biçimde işlenmek durumundadır. Bu verilerin toplanabilmesi için yasal ve açık bir amaç olması gereklidir. Ancak bu amaca uygun şekilde verilerin toplanması ve

işlenmesi faaliyeti gerçekleştirilebilecektir. Veriler, amaca uygun oranda toplanmalıdır. Amaç dışındaki bilgilerin toplanmaması önemlidir. İşlenen bu veriler, her daim güncel tutulmalı ve gerçek bilgilerden oluşmalıdır. Bilgilerde herhangi bir eksiklik ya da yanlışlık bulunması durumunda, silinmesi ya da düzeltilmesi işlemi yapılmalıdır. Kişisel verilerin işlenme amacı sona erdiğinde, veriler depolanmaya ya da işlenmeye devam edilmemelidir. Son olarak verileri işleyen kişiler, verilerin güvenliğini sağlamakla yükümlüdür (http-58).

Bununla birlikte verilerin sahipleri, verileri işleyen kişilerden bilgi alma hakkına sahiptir. Veri sahibi olan kimseler; kendisine ait bilgilerin ne amaçla işlendiği, hangi bilgilerinin bu faaliyet çerçevesinde toplandığı, ne kadar süre boyunca bilgilerin kayıt altında tutulacağı ve yasal sebepler doğrultusunda bu bilgileri sildirtebileceği ya da değiştirtebileceğini öğrenme hakkına sahiptir. Aynı zamanda veri sahipleri, toplanan verilerin bir kopyasını talep edebilecektir (http-58).

196 sayılı Kişisel Verilerin Korunması Kanunu'nun 161. maddesi uyarınca yaptırımlar düzenlenmiştir. Buna göre; kişisel verilerin sahiplerine, verilerin işlendiğine yönelik bilgi vermeyi reddeden veri işleyenlere üç bin ila on sekiz bin Euro arasında para cezası verilecektir. Eğer işlenen veriler kişinin dini ve felsefi inancına, siyasi görüşüne ya da sendika üyeliğine yönelik hassas nitelikli verilerse bu durumda ceza beş bin ila otuz bin Euro tutarında olacaktır (196 sayılı Kanun, m. 161).

Kişisel verilerin işlenmesi için belirlenen amacın ortadan kalkması sonucunda bilgileri silmek yerine saklamaya devam eden kişilere beş bin ila otuz bin Euro para cezası verilmesi 162. maddede düzenlenmiştir. Kişinin sağlığıyla ilgili bilgileri, yasal olmayacak bir biçimde verileri işleyenler tarafından başka kişilere açıklanırsa bu durumda, aynı şekilde beş bin ila otuz bin Euro tutarında para cezası kesilecektir (196 sayılı Kanun, m. 162).

Verileri işleyen kişi, kendisi ya da bir başkası adına kazanç sağlamak ya da verilerin sahibine zarar vermek için kişisel verileri işliyorsa bu durumda, altı ila on sekiz ay hapis cezasıyla cezalandırılacaktır (196 sayılı Kanun, m. 167).

İtalya, işverenlerin çalışma sırasında siber gözetim faaliyetiyle işçilerini denetlemesine yönelik bir kanun sahip ülke olması açısından önemlidir. 20/5/1970 tarihli ve 300 sayılı "İşçilerin Statüsü Kanunu", işçilerin siber gözetim araçlarıyla gözetlenmesiyle ilgili hükümler içermektedir (http-58).

300 sayılı Kanun'un 4. maddesi, 2015 yılı itibarıyla yeniden düzenlenmiştir. Bu düzenlemeyle birlikte 4. maddenin birinci fıkrası uyarınca; "Siber gözetim araçları bazı amaçlarla işçileri gözetlemek için kullanılabilecektir. Bu amaçlar; işyerinde güvenliğin sağlanması, eşyaların korunması ve üretimin arttırılması şeklinde özetlenebilmektedir". Bu maddeyle iki farklı düzenleme yapılmıştır. Bunlardan birincisi; işverenlerin siber gözetim araçlarıyla işçileri doğrudan gözetlenmesinin yasaklanmasıdır. 2015 yılında yapılan düzenlemeden önce işverenlerin işçilerini doğrudan gözetleme hakkı bulunmamaktaydı. İkinci düzenlemeye göre ise; siber gözetim faaliyetinin gerçekleştirilmesi için geçerli bir sebep gerekmektedir. İşyerindeki üretim miktarının arttırılması ve güvenliğin sağlanmasının yanı sıra işyerinde yer alan mal ve mülklerin korunması amacıyla siber gözetim yapılabilecektir. Dolayısıyla, işçilerin işyerindeki eşyalara kasti olarak zarar vermesinin önlenmesi için işverenler tarafından siber gözetim faaliyetine başvurulması 300 sayılı Kanun'un 4. maddesiyle mümkün olabilmektedir. Bütün bunlara ek olarak 4. madde uyarınca; "İşveren, siber gözetim faaliyetini gerçekleştirdiği araçlar ve bu faaliyetin kendisi hakkında işçiye bilgi vermekle yükümlüdür (Tebano, 2017, s. 4-5)".

Diğer bir ifadeyle, ilgili Kanun'un 4. maddesinde yapılan değişiklikle birlikte işverenler, geçerli bir sebep olmadığı sürece işyerinde siber gözetim faaliyetini gerçekleştiremeyecektir. Ancak işyerinde bir toplu iş sözleşmesinde siber gözetim faaliyetinin yer alması ya da işçinin rızasının alınması hallerinde işveren tarafından siber gözetim faaliyeti yapılabilecektir (Aloisi ve Gramano, 2019, s. 21-22).

300 sayılı Kanun'un 8. maddesine göre; "İşveren, işçisinin politik görüşüne, dini inancına ya da sendika üyeliğine ilişkin özel sayılan verilerini işleme hakkına sahip değildir. İşveren, siber gözetim faaliyetini gerçekleştirirken, bu tür özel nitelikli verileri toplayamayacaktır. Dolayısıyla, 300 sayılı Kanun'da 2015 yılında yapılan değişiklikler çerçevesinde, işçilerin siber gözetim faaliyetine karşı daha iyi korunabileceği görülmektedir (Tebano, 2017, s. 8)".

2.2.4. Amerika Birleşik Devletleri (ABD)

ABD'de kişisel verilerin ve özel hayatın gizliliği hakkının korunmasında Anayasa, federal kanunlar, eyalet kanunları ve içtihatlar rol oynamaktadır. Dolayısıyla Avrupa'daki kişisel verilerin korunması anlayışıyla kıyaslandığında ABD'nin konuya yaklaşımının biraz daha farklı olduğu görülmektedir. Aynı zamanda 17/9/1787 tarihli ABD Anayasası'nda kişisel verilerin korunmasına yönelik açıkça bir hüküm

bulunmamaktadır. Vatandaşların özel hayatının korunmasının temelinde, devletin halka hiçbir müdahalede bulunmaması koşulu yer almaktadır. Kişilere devlet tarafından müdahale edilmediği sürece, devletin herhangi bir düzenleme yapmasına gerek kalmadan özel hayatın gizliliği hakkının korunacağı varsayılmaktadır. Bu ifade, ABD Anayasası'nda *kişinin yalnız bırakılma hakkı* olarak geçmektedir. Dolayısıyla kişinin yalnız kalma hakkının gerçekleştirilmesiyle, özel hayatın gizliliğinin sağlanmış olduğu düşünülmektedir (Korkmaz, 2017, s. 238; Türkel, 2010, s. 43).

ABD Anayasası'nda kişisel verilerin korunması hakkında yapılan en dikkat çekici düzenleme "Fourth Amendment", diğer bir deyişle "Dördüncü Anayasa Değişikliği"dir (Tabak ve Konukpay, 2018, s. 120). Bu değişiklikle kamu sektöründe işçilerin, bir soruşturma kapsamında devlet tarafından makul ve yasal olmayan şekillerde aranmasına engel olunması amaçlanmıştır. Böylece işçilerin, özel hayatının gizliliğinin korunması ve özgürlük haklarının ihlal edilmesine karşı önlem alınması istenmektedir (http-59; Akyürek, 2011, s. 131-132).

Dördüncü Anayasa Değişikliği bağlamında arama yapılabilmesi için mahkeme tarafından izin verilmiş olması ve makul bir sebep doğrultusunda arama yapılabilmesi gerekmektedir. Herhangi bir makul sebebin olmadığı durumlarda mahkeme, arama faaliyetini kanun dışı kabul etmektedir. Dördüncü Anayasa Değişikliği'nde yer alan bu düzenleme, ABD Anayasa'sındaki kişilerin yalnız kalma hakkına dayanmaktadır (Watt, 2009, s. 31).

İlgili bu Anayasa Değişikliği'nin uygulanması bağlamında, 1987 tarihli ve 85-530 numaralı "O'Connor Ortega'ya karşı" isimli dava önemlidir. Dr. Ortega, Napa Eyalet Hastanesi'nde psikiyatrist ve mesleki eğitim uzmanı olarak görev almaktadır. Hastanenin yönetim müdürü Dr. O'Connor, Dr. Ortega'nın mesleğini icra ederken birtakım usulsüzlükler yaptığını düşünerek, Dr. Ortega'yı idari izinle hastaneden uzaklaştırmıştır. Ancak Dr. Ortega'nın izinli olduğu süre içerisinde bir araştırma ekibi, doktorun hastanedeki odasında arama yapmıştır. Bu arama kapsamında Dr. Ortega'nın çalışma masası ve dolabında bulunan özel yazışmalarının olduğu kartpostallar ve fotoğrafları gibi kişisel eşyaları da araştırma ekibi tarafından incelenmiştir. Dr. Ortega, kanıt toplanması ve işten atılması amacıyla odasındaki kişisel dosyaların arandığını belirtmiş ve Dördüncü Anayasa Değişikliği uyarınca kişisel haklarının ihlal edildiği gerekçesiyle mahkemeye başvurmuştur (Watt, 2009, s. 36-37).

Mahkemenin beş üyesi de bu olayda Dr. Ortega'nın makul orandaki mahremiyet beklentisini haklı bulmuştur. Bu olayda; doktorun çalıştığı hastanenin iç yönetmeliğinde, işçilerin kendilerine ait çalışma odalarındaki dolap ya da masalarında özel eşyalarını bulunduramayacaklarına yönelik herhangi bir düzenleme olmaması dolayısıyla doktorun mahremiyet hakkının korunmasını talep etmesi mahkeme tarafından makul karşılanmıştır. Dolayısıyla işçiler, kişisel verilerinin gizliliğin sağlanmasını talep etme hakkına sahiptir. Burada işçinin mahremiyet talebiyle işverenin işi ve işyerini yönetme ve kontrol etme faaliyeti arasında bir denge kurulması gerekmektedir. İşveren, gözetim faaliyetini gerçekleştirdiği sırada işçinin mahremiyetinin korunmasına önem vererek bu işlemi yerine getirmekle yükümlüdür (O'Connor v. Ortega adlı karar; Watt, 2009, s. 37-39; Tabak ve Konukpay, 2018, s. 121-123).

Bir diğer davada ise; Ontario Emniyet Müdürlüğünde çalışan Sergeants Quon isimli ABD vatandaşına, işvereni tarafından bir çağrı cihazı verilmiştir. Bu çağrı cihazı yirmi beş bin karaktere kadar gönderilen mesajlardan ücret kesintisi yapmayacaktır. Ancak karakter sayısı yirmi beş bini aştığında kullanıcıdan ekstra ücret talep edilecektir. Çalışma sırasında kullanılacak olan bu çağrı cihazlar verildiğinde işçilere bir belge imzalatılmıştır. Bu belge, Ontario şehrinde çalışan tüm işçilerin tabi olduğu "Bilgisayar Kullanımı, İnternet ve E-posta Sözleşmesi"dir. Bu sözleşmedeki düzenlemeler gereğince; "İşçilerin, iş sırasında kullanması gereken bu araçları iş dışı amaçlarla kullanması yasaktır. Aynı zamanda bu araçlardan yapılan her işlem kaydedilecektir ve işçilerin de bu nedenle mahremiyet hakkı çerçevesinde beklentiye girmemesi gerekmektedir". Quon, işe girdiği esnada bu sözleşmeyi imzalamıştır. Ancak Quon, çağrı cihazını kullanırken belli aylarda belirlenen miktardan daha fazla karakter kullanarak mesaj gönderdiği için çalıştığı polis merkezi mesajların içeriğini incelemeye almıştır. Bu inceleme sırasında Quon'un hem çalışma saatleri içerisinde mesaj gönderdiği hem de uygunsuz içerikli internet sitelerine erişim sağladığı kayıtlarına rastlanmıştır. Bu nedenle Quon işten çıkartılmıştır (Quon v. Arch Wireless Operating Company adlı karar). Bu olayın hemen ardından Quon, Ontario Mahkemesinde Dördüncü Anayasa Değişikliği düzenlemesinin ihlali uyarınca dava açmıştır. Mahkeme, Quon'un mahremiyet hakkına ilişkin beklentisini yasal kabul etmiştir. Ancak polis merkezinin gerçekleştirmiş olduğu gözetim faaliyetinin de amaca uygun olarak yapıldığına karar vermiştir. Ardından işçi, karara itiraz etme amacıyla bir üst

mahkemeye başvurmuştur. Temyiz mahkemesi ise, işçinin mahremiyet beklentisini onamanın yanı sıra polis merkezinde gerçekleştirilen gözetim faaliyetinin daha az mücadeleci bir yöntem kullanılarak yapılması gerektiğini belirtmiş, bu bağlamda bölge mahkemesinin kararının anayasaya aykırı olduğu gerekçesiyle verilen kararı bozmuştur. Temyiz Mahkemesinin verdiği bu kararı inceleyen Anayasa Mahkemesi ise, işveren tarafından işçinin mesajlarının gözetlenmesinin Anayasaya düzenlemelerine aykırı olmadığını ve işle ilgili yasal bir amaç güdülerek gözetimin yapıldığı kararını vermiştir. Aynı zamanda Dördüncü Anayasa Değişikliği kapsamında herhangi bir kişilik hakkı ihlalinin meydana gelmediğini çünkü işverenin, gözetimi aşırı müdahale yöntemine başvurmadan yaptığını belirtmiştir. Dolayısıyla mahkeme, işçinin makul şekilde mahremiyet hakkı olduğunu savunmaktadır. Ancak kamu sektöründeki işverenler de gereksiz ve fazla müdahaleci olmamak şartıyla gözetim faaliyetini gerçekleştirmekte serbest olacaktır (Sprague, 2010, s. 11-12; Tabak ve Konukpay, 2018, s. 123-124).

1968 yılı itibarıyla "Telefon Konuşmalarının Gizlice Dinlenmesine Yönelik Federal Kanun (Federal Wiretap Act – FWA)" yürürlüğe konmuştur (Sproule, 2002, s. 71). Bu Kanun'da; "Kişiler arasındaki sözlü iletişimin ya da telefon, telsiz gibi cihazlar üzerinden gerçekleştirilen konuşmaların dinlenmesi, hatta dinlenmeye çalışılması, dinlenen konuşmalardan elde edilen bilgilerin kullanılması ve bu bilgilerin başkalarına açıklanması yasaklanmıştır. İşverenlerin, işçilerinden onay alması durumunda yapılan görüşmeleri dinlemeleri mümkün olabilecektir (http-60; Tekergül, 2010, s. 41)".

1980'li yıllara gelindiğinde teknolojik gelişmelerin hızla artması sonucunda bu Federal Kanun'daki düzenlemeler yetersiz kalmaya başlamıştır. Bu nedenle 1986 tarihinde "Elektronik Haberleşmenin Gizliliği Kanunu (Electronic Communications Privacy - ECPA)" ABD Kongresi tarafından yürürlüğe konmuştur (Sprague, 2010, s. 18; http-61; Tabak ve Konukpay, 2018, s. 127). ABD Kongresi'nin 1986 tarihli bu Kanun'u çıkarmasındaki temel amaç; teknolojideki gelişmeler çerçevesinde ortaya çıkan yeni mahremiyet problemlerine yönelik düzenlemeler yapılmasıdır. Bu Kanun, özellikle kişilerin e-posta yoluyla haberleşmesi hakkındaki düzenlemeleri içermektedir. İlgili Kanun ile çalışma sırasında işverenlerin, işçilere siber gözetim uygulaması mümkün olabilecektir (Watson, 2001, s. 82-83; Mathis ve Jackson, 2010, s. 520).

Bu Kanun uyarınca, işverenlerin işçilerinin e-postalarını denetleyebilmesi için iki temel koşulun sağlanmış olması gerekmektedir. Bu koşullardan birincisi; internet ya da telefon hizmetini sağlayan kuruluşun görevi kapsamında ya da bu kuruluşa ait hakların

korunması gereken durumlarda kişilerin arasındaki iletişim izlenebilecektir. İkinci koşulda; işin yürütülmesine uygun bir amaç çerçevesinde işverenin gözetim yapabilmesi mümkün olacaktır. Dolayısıyla işverenin, yasal ve makul bir gerekçeyle gözetim faaliyeti yapması gerekmektedir. Örneğin; müşteri memnuniyetinin değerlendirilmesi açısından işçinin e-posta üzerinden yaptığı konuşmalara erişim sağlanabilecektir. Son koşula göre ise; işverenler, e-posta üzerinden gözetim yapacağını işçisine söylemek ve işçinin onayını almakla yükümlüdür. Aynı zamanda neden bu gözetime ihtiyaç duyulduğunu da işçiye açıklamak durumundadır. Bütün bunlara ek olarak işveren tarafından, işçinin işyerinde kullanması için özellikle tahsis edilmiş iş e-postası üzerinden gözetim faaliyet yapılabilecektir. Ancak işveren bu gözetim faaliyeti sırasında, belirlenmiş gözetim amacının dışına çıkmamakla yükümlüdür (Watson, 2001, s. 84-85; DiLuzio, 2000, s. 746-748).

Bu bağlamda mahkemenin verdiği bir kararı incelemek yerinde olacaktır. Michael A. Smyth adındaki işçi, iş sözleşmesinin haksız şekilde feshedildiğini ve özel hayat hakkının ihlal edildiğini gerekçe göstererek dava açmıştır. Olay şu şekilde gerçekleşmiştir: İşçi, evinde bulunan kişisel bilgisayarından, işvereninin ona sağlamış olduğu iş e-postası aracılığıyla birtakım e-postalar göndermiştir. Ardından işveren, işçinin göndermiş olduğu bu e-postalara erişim sağlamış ve e-postalarda yer alan bilgilerin işyeri yönetimine aykırılık teşkil ettiği gerekçesiyle işçinin iş sözleşmesini sonlandırmıştır. Söz konusu olay, işyerinde kullanması amacıyla işçiye verilen e-posta üzerinden gerçekleştiği için mahkeme, işçinin özel hayatının gizliliğinin ihlal edilmesinin mümkün olamayacağını belirtmiştir (Smyth v. The Pillsbury Company adlı karar; Tekergül, 2010, s. 43).

ABD'de 26 Ekim 2001 tarihinde, "The USA Patriot Act" adıyla ABD Vatanseverlik Kanunu kabul edilmiştir. Bu Kanunla terör faaliyetlerinin önüne geçilmesi ve önlemler alınması çerçevesinde kişisel verilerin korunmasına yönelik bazı kanunlarda değişiklik yapılmıştır. Ancak yapılan düzenlemelerle devletin, kişisel verileri işlemesinin önü açıldığı düşünülmektedir. ABD Vatanseverlik Kanunu, ECPA'da birtakım değişiklikler yapılmasını sağlamıştır. Yeni düzenlemeler uyarınca devlet tarafından yetkilendirilmiş kişiler, gönderilen e-postaların hangi adrese gittiğine ve erişim sağlanmış web sitelerinin hangileri olduğuna ulaşabilme hakkına sahiptir. Vatanseverlik Kanunu'nda, vatandaşların birbiriyle kurduğu iletişimin kapsamına ulaşılması yasaklanmıştır. Ancak federal araştırmacı olarak yetkilendirilmiş kişiler,

şüpheli olduğunu düşündükleri kişilerin internet kullanımını inceleme hakkına sahiptir. Dolayısıyla bu federal araştırmacılar kişinin kimlerle konuştuğu, kimlere e-posta gönderip aldığı ve ziyaret ettiği siteler hakkında bilgi sahibi olabilecek ve gerektiğinde kişisel verileri kaydedebilecektir. Vatanseverlik Kanunu'nun bu düzenlemeleri göz önüne alındığında kişisel verilerin korunması ve özel hayatın gizliliği açısından problem yaratabilecek olduğu düşünülmektedir (Korkmaz, 2017, s. 255).

ABD'de merkezi anlamda bir veri koruma kanunu olmaması sebebiyle, düzenlenmiş herhangi bir yaptırım da bulunmamaktadır. Ancak Elektronik Haberleşmenin Gizliliği Kanunu'nda izinsiz olarak kişisel verilere erişilmesi, toplanması ve işlenmesi durumunda, bu işlemi gerçekleştirenler açısından belli yaptırımlar düzenlenmiştir. Eğer işverenler; işçinin verilerine zarar vermek, bu verilerden özel ya da ticari kazanç sağlamak ve kişisel verileri kötü niyetli olarak kullanmak isterse beş yıla kadar hapis cezasıyla yargılanabilecektir. Bu ek olarak, işçi ya da işverenlerin eyaletlerde açılan davalarda, ilgili kanunlar ve yönetmelikler uyarınca mahkeme, uygun cezayı verebilmektedir (http-61 ve http-62).

2.2.5. İngiltere

İngiltere, diğer AB üyesi olan ülkelerin içerisinde yazılı bir Anayasa'ya sahip olmayan tek ülke olma özelliğini taşımaktadır. İngiltere'de, çalışma hayatında kişisel verilerin ve özel hayatın gizliliğinin korunması, ABD'de bu konunun ele alınış biçimiyle benzerlik göstermektedir. Diğer bir yandan da İngiltere'nin AB üyeliği sebebiyle, ABD'ye kıyasla İngiltere'de kişisel verilerin korunmasına yönelik çıkarılan temel kanunlar bulunmaktadır (Abrahamse, 2014, s. 19-20).

İşyerinde işçilere uygulanan siber gözetim faaliyetiyle ilgili imzalanmış olan kanunlar şu şekildedir:

- 1998 tarihli "İnsan Hakları Kanunu (Human Rights Act)",
- 1998 tarihli "Veri Koruma Kanunu (Data Protection Act)",
- 2000 tarihli "Araştırmanın İşleyişini Düzenlemeye Yönelik Kanun (The Regulation of Investigatory Powers Act)",
- 2000 tarihli "Telekomünikasyon -İletişimin Durdurulması- Yönetmeliği (Telecommunications -Interception of Communications-Regulations)",
- 2011 tarihli "İstihdam Uygulamaları Veri Koruma Yönetmeliği (Employment Practices Data Protection Code)" (Lockwood, 2018, s. 208).

İngiltere'de 1984 tarihinde "Veri Koruma Kanunu" imzalanarak yürürlüğe girmiştir. İngiltere'nin ilk veri koruma mevzuatını oluşturan bu Kanun, aynı zamanda Dünya çapında en kapsamlı veri koruma kanunu olma özelliğini taşımaktadır. İlgili Kanun hem OECD'nin hem de Avrupa Konseyi'nin kişisel verilerin korunmasına yönelik düzenlemelerini esas alarak hazırlanmıştır (Cunha, 2013, s. 101; Korkmaz, 2017, s. 257). Veri Koruma Kanunu'nun yürürlüğe girmesi AK'nin 108 sayılı Sözleşmesi'nden üç yıl sonra gerçekleşmiştir ve 1998 tarihine kadar geçerliliğini korumuştur (Civelek, 2011, s. 87; Rodrigues, Wilson ve Schanz, 2001, s. 90-91).

1995 yılında AB'nin kişisel verilerin korunması amacıyla imzaladığı 95/46/EC sayılı Direktif'i İngiltere, 1998 yılı itibarıyla ulusal hukukundaki Veri Koruma Kanunu'yla uyumlaştırmış ve yürürlüğe konmuştur. Kamu ve özel sektör ayrımı yapmaksızın tüm kurum ve kuruluşlarda geçerli olan bu Kanun gereğince, işverenler işçilerinin bilgilerini doğru ve meşru bir biçimde işlemekle yükümlüdür. Gerek bilgisayar aracılığıyla gerekse elle dosyalanarak depolanmış olan işçi verileri, ilgili Kanun uyarınca işverenler tarafından koruma altında tutulmalıdır (Lockwood, 2018, s. 208-209). 25/5/2018 tarihli ve 95/46/EC sayılı Direktif'in yerini alan "Genel Veri Koruma Yönetmeliği" çerçevesinde İngiltere'nin Veri Koruma Kanunu'nda düzenlemeler yapılarak Yönetmelik'le uyumlu hale getirilmiştir (http-63). Yapılan son düzenlemeyle birlikte bu Kanun yedi bölüme ayrılmıştır. Kanun'da yer alan bölümler sırasıyla şu şekildedir:

1. Bölüm: Başlangıç Hükümleri,
2. Bölüm: Genel Veri İşleme Hükümleri,
3. Bölüm: Kanunları Uygulama Sürecine Yönelik Hükümler,
4. Bölüm: İstihbarat Servisinin İşleyişine Yönelik Hükümler,
5. Bölüm: Bilgi Komisyonu'na Yönelik Hükümler,
6. Bölüm: Yaptırımlara Yönelik Hükümler ve
7. Bölüm: Tamamlayıcı ve Final Hükümleridir (http-39).

İlgili Kanun'da 1998 tarihi öncesinde, "Veri Koruma Ofisi" bulunmaktadır. Ancak 1998 yılı itibarıyla Kanun'da yapılan değişiklik sonucunda, "Bilgi Komiserliği Ofisi (Information Commissioner's Office – ICO)" oluşturulmuştur. Kanun'un 2018 yılında düzenlenen halinde de bu ofis yer almaktadır. Bilgi Komiserliği Ofisi, kişisel verileri koruma amacıyla oluşturulmuş bağımsız bir kuruluştur (http-64). Ofis'in görevleri arasında; verileri işleyen kişilerin Kanun'a uygun olarak veri işleme faaliyetini

gerçekleştirmesini sağlamak, Kanun'un işleyişi hakkında veri işleyenleri bilgilendirmek, veri işleyenlere rehberlik etmesi amacıyla uygulama kodları geliştirmek ve yıllık olarak Parlamento Meclisi'ne rapor sunmak vardır (Cunha, 2013, s. 102).

Veri Koruma Kanunu gereğince veriler adil ve hukuka uygun bir biçimde işlenmelidir. Kişisel verilerin işlenmesinden sorumlu olan kişi, bir amaç doğrultusunda verileri işlemeyi gerçekleştirmekle yükümlüdür. Verileri işleyen kişi, bu amacın geçerli olduğu süre boyunca verileri işleyebilmekte ve depolayabilmektedir. Söz konusu amaç; yasaya uygun olarak belirlenmelidir. Kişiler keyfi olarak veri işleme faaliyetinde bulunma hakkına sahip değildir. Kişiler, verilerinin işlendiğinden haberdar olmalıdır ve verilerinde eksiklik ya da yanlışlık olması durumunda verilerin düzeltilmesini talep etme hakkına sahiptir. Toplanacak olan veriler, amaca uygun oranda toplanmalı ve amacın sona ermesi durumunda veri işleme ve depolama işlemi sona erdirilmelidir. İlgili veriler; kişinin özel hayat ve kişisel verilerin korunması hakkını ihlal etmeyecek biçimde işlenmeli ve korunmalıdır (Civelek, 2011, s. 88).

İngiltere Parlamentosu'nun 1998 tarihinde yürürlüğe koyduğu İnsan Hakları Kanunu'nda; bireyin özel ve aile hayatının, oturduğu evinin ve kurduğu iletişiminin kendisine ait bir hak olduğu ve bu haklara saygı duyulması gerektiğine yönelik hükmünü içeren AİHS'nin 8. maddesi aynı ifadelerle yer almaktadır. Böylece İngiltere'de özel hayatın gizliliğine yönelik hakkın oluşmasına zemin hazırlamıştır (Savaş, 2009, s. 108; Lockwood, 2018, s. 208). İnsan Hakları Kanunu'nda mevcut olan bu maddeyle işçilerin özel hayatının mahremiyeti hakkı korunmaktadır. Örneğin; işveren, işçiye özel amaçlı kullanımı için ayrı bir cep telefonu tahsis etmişse, bu telefondan yapılan görüşmeleri engelleme hakkına sahip değildir. Böyle bir durumda işçi, 8. madde uyarınca dava açma hakkına sahip olacaktır (Lockwood, 2018, s. 208).

İngiltere'nin yukarıda bahsetmiş olduğumuz kanunlarında, çalışma hayatında işverenler tarafından uygulanan siber gözetim faaliyetine çok fazla değinilmediği görülmektedir. Ancak İngiltere mevzuatında, çalışma hayatında işçilere ait verilerin ve işçilerin özel hayatının gizliliğinin korunmasına ilişkin düzenlemelerin olduğu bilinmektedir. 2000 tarihi itibarıyla yürürlüğe giren "Araştırmanın İşleyişini Düzenlemeye Yönelik Kanun (The Regulation of Investigatory Act)" bu düzenlemelerden biridir. Bu Kanun'da yer alan hükümler; AB'nin 97/66/EC sayılı telefon, kamera ve cep telefonu gibi ağ sistemleri üzerinden işlenen verilerin korunmasına yönelik düzenlemeleri içeren Direktifiyle uyumlu olacak biçimde

oluşturulmuştur. İlgili Kanun'un birinci bölümü uyarınca, kişilerin kurduğu iletişim etkinliğini kasıtlı olarak engellemek yasaya aykırıdır. Diğer bir ifadeyle, işçinin telefon görüşmelerini ya da e-posta göndermesini engellemek bu kapsamda yer almaktadır. İletişim engellenebilmesi yalnızca bir hukuki gerekçeyle mümkündür. Dolayısıyla işveren; işyerinde telefon hattı üzerinden konuşan iki işçisinin konuşmasını kasıtlı olarak engelleme hakkına sahip değildir. İşveren her iki tarafın da rızasını aldıysa, bu durumda aralarındaki konuşmayı engelleyebilecektir (Abrahamse, 2014, s. 24; http-65).

İlgili Kanun'un ikinci bölümüne göre; yasal bir amaç doğrultusunda işverenler, işçilerini gözetime tabi tutabilme hakkına sahip olacaktır. Söz konusu yasal amaçlar; ulusal güvenliğin sağlanması, herhangi bir suçun tespit edilmesi veya önlemesi, kamu güvenliğinin sağlanması ve halk sağlığının korunması şeklinde örneklendirilebilir. Buna ek olarak işveren, gözetleyeceği işçisine bu durumu mutlaka bildirerek, onayını almak zorundadır (http-65).

2000 yılı itibarıyla yürürlüğe konan bir diğer yasa, "Telekomünikasyon – İletişimin Durdurulması Yönetmeliği"dir. Bu Yönetmelik işverenlere, işçilerinin iletişim faaliyetini durdurma hakkı tanımaktadır. Ancak iletişim durdurulması belli durumlar söz konusu olduğunda geçerli olacaktır. İşverenin işi yürütebilmesi, ulusal güvenliğin sağlanması, işlenen bir suçun tespit edilmesi veya önlenmesi ve işyerinde kullanılan telekomünikasyon sistemlerinin izinsiz kullanıldığının tespit edilmesi ile bunun önlenmesini sağlamak amacıyla işveren, işçilerinin iletişimini durdurabilmekte ve kaydedebilmektedir. Burada unutulmaması gereken en önemli nokta; işverenin yalnızca iş ve işin yürütülmesiyle ilişkili olarak iletişim faaliyetini durdurabilme yetkisinin olmasıdır. İşveren, keyfi olarak işçilerinin iletişimini engelleme ya da dinleme hakkına sahip olmamaktadır. Buna ek olarak işverenler, kendileri ve iş hakkında bilgi paylaşımı yapılıp yapılmadığını kontrol edebilmek için işçilerinin iletişim faaliyetini denetleme hakkına sahiptir. Ancak bu faaliyeti kayıt altına alması, Yönetmelik gereğince yasaklanmıştır. Bu Yönetmelik kapsamında toplanan bilgiler konusunda işçiye bilgi verilmesi ve işçinin açık onayının alınması gerekmektedir. İşveren, işçiden toplanan verilerin; iş sözleşmesinin devamlılığı için gerekli, işçinin meşru menfaatlerinin korunması adına önemli ve yasal gerekliliklerin yerine getirilmesi adına elde edildiğini işçiye açıklamakla yükümlüdür (http-66; Abrahamse, 2014, s. 25-26; Savaş, 2009, s. 109).

1998 tarihli Veri Koruma Kanunu'nun 51. maddesinde yer alan Bilgi Komiserliği Ofisi tarafından ilgili Kanun'un işverenlerce uygulanmasına yardımcı olmak amacıyla 2011 tarihli "İstihdam Uygulamaları Veri Koruma Kodu (Employment Practices Data Protection Code)" yayınlanmıştır. İşverenler 1998 tarihli Kanuna uymakla yükümlüdür. Bu Kod, işverenlere rehberlik etmesi için hazırlanmıştır. İlgili Kod; 1998 tarihli Veri Koruma Kanunu ve 2000 tarihli Araştırma Yetkileri Kanunu ile uyumlu bir şekilde düzenlenmiştir (http-67).

İstihdam Uygulamaları Veri Koruma Kodu; işe alınmadan önceki aday işçileri, işyerinde çalışan sözleşmeli ya da geçici işçileri ve işyerinde daha önce çalışmış ancak şu anda çalışmıyor olan eski işçileri kapsamına almaktadır. Kodun üçüncü bölümü işyerinde yapılan siber gözetim faaliyetine yönelik düzenlemeleri kapsamaktadır. Buna göre; işverenlerin, işçinin işyerinde ürettiği işin miktarını ve kalitesini kontrol etmek amacıyla gözetim yapması mümkündür (http-67).

Kod, işçilerin korunması için işyerinde sürekli olarak siber gözetim faaliyetinin uygulanması yerine şüpheli durumlarda gözetimin uygulanmasını tavsiye etmektedir. Aynı zamanda işverenin tüm işçileri değil, riskli davranışlarda bulunan işçileri gözetlemesi de önerilmektedir. Bunlara ek olarak; işverenin kesintisiz gözetim faaliyetindense, işçilerin denetlenmesi ve işin kontrol edilmesiyle daha az müdahaleci bir yaklaşım göstermesi mümkün olacaktır. İşverenler, bu Kod'un tavsiyesi doğrultusunda gözetim faaliyeti yaptıklarını işçilerine bildirmekle yükümlüdür. Toplanan kişisel verileri koruma altında tutmalı ve elde edilen bilgilerin bir kopyasını veri sahibi işçilere vermelidir (http-67).

Siber gözetimin gerçekleştirilmesindeki amaç ve bu amaç doğrultusunda yapılacak gözetimin yaratacağı faydalar işveren tarafından belirlenmelidir. Böylece işverenin gözetimi işçiye karşı daha az müdahaleci bir hal alacaktır. İşyerinin kurallarının ve standartlarının uygulanabilmesi için gözetim yapılıyorsa, yapılan gözetimin niteliği ile kapsamını ifade eden politika belirlenmeli ve bu politika işçilere açıklanmalıdır (http-67).

Yapılacak olan gözetim; telefon, e-posta, internet gibi araçlar üzerinden gerçekleştirilecekse, işverenin bir "Elektronik İletişim Araçlarının Kullanımı Politikası" hazırlaması ilgili Kod tarafından tavsiye edilmektedir. Hazırlanan bu belgede, işçilerin hangi koşullarda telefon ve bilgisayarı kullanabileceği ya da hangi durumda bilgisayar

üzerinden giriş yaptıkları web sitelerinin kontrol edileceği gibi bilgiler işçilere verilmelidir (http-67).

Kod uyarınca işçinin e-postaları gözetleniyorsa işverenler, özel ve kişisel olduğunu tahmin ettikleri e-postalarını açmamaya özen göstermelidir. İşçiye, işyeri içerisindeyken kişisel e-postalarına erişme izni tanınmışsa bu e-postalar sadece istisnai durumlar ortaya çıktığında gözetlenmelidir. Eğer işçinin e-postalarında yer alan veriler işveren tarafından saklanacaksa ne kadar süre boyunca bu verilerin saklanacağı işçiye bildirilmelidir (http-67).

Kameralarla işçilerin gözetlenmesi faaliyeti de bu Kod kapsamında ele alınmıştır. İşverenler, sürekli olarak işçilerin görüntülerini kayıt altına almamalıdır. İşyerinde hırsızlık gibi işyerinin ve işçilerin güvenliğini tehdit eden bir durumun ortaya çıkması halinde kameralarla siber gözetim faaliyetine başvurulmalıdır. Ancak işverenler, işçinin kullanımına ayrılmış olan tuvalet ve duş gibi özel alanlarda kamerayla gözetim yapma hakkına sahip değildir. Bununla birlikte işverenler, kamerayla siber gözetim faaliyetini gerçekleştirdiğini işçiye söylemekle yükümlüdür. Ancak gözetimin gizli bir biçimde yapılması gerektiği durumda işveren, bunu söylemeyebilme hakkına sahiptir (http-67).

Data Koruma Kanunu'ndaki düzenlemelerin ihlal edilmesi durumunda, ihlali gerçekleştiren kişilere birçok yaptırım öngörülmüştür. Kişisel verilerinin işlenmesinden etkilenen bireyler, Bilgi Komiserliği Ofisi'ne başvurarak şikâyette bulunabilecektir. Bu doğrultuda ihlali gerçekleştiren kişiler beş yüz bin Sterlin'e kadar para cezasıyla cezalandırılabilecektir. Miktarın ne kadar olacağı, durumun ağırlığına göre kararlaştırılmaktadır. Buna ek olarak mahkemelerde dava açma hakkına sahiptirler. İşyerlerinde meydana gelen kişisel verilerin ve özel hayatın gizliliğinin korunması hakkında Data Koruma Kanunu ile İstihdam Uygulamaları Veri Koruma Kodu'nun ihlaline yönelik açılan dava sayısı yok denecek kadar azdır. Bu nedenle verilecek cezalar öngörülememektedir (http- 67).

Ancak son zamanlarda İngiltere'nin AB üyeliğini sonlandırmak istemesine yönelik tartışmalar, ülkenin Data Koruma Kanunu'ndaki hükümlerinde değişiklik yapılıp yapılmaması gerektiği ikilemini ortaya çıkartmıştır. İngiltere'nin AB'den Çekilme Kanunu'nun (European Union – Withdrawal Act) üçüncü bölümünde yer alan düzenleme uyarınca İngiltere'nin AB'den çıkması durumunda, AB'nin Genel Veri Koruma Yönetmeliği hükümleri İngiltere'nin mevzuatına dahil edilecektir (http-68; http-69).

3. TÜRK HUKUKUNDA İŞYERİNDEKİ SİBER GÖZETİM MEKANİZMALARINA YÖNELİK YASAL DÜZENLEMELER

Siber gözetim faaliyetinin en önemli parçası, işçilere ait verilerin toplanmasıdır. Önceki bölümlerde bahsettiğimiz üzere, işçilerin sadece siber gözetim faaliyetine karşı korunması değil, aynı zamanda işçilerin kişisel verilerinin ve özel hayatının gizliliğinin de korunması çok önemli bir gerekliliktir.

24/7/2012 tarihli ve 28363 sayılı Resmî Gazete'de yayımlanan "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik"in 3. maddesinde kişisel verinin tanımı; "Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler şeklinde yapılmıştır (http-70)". Dolayısıyla, kişisel veriler kavramının en önemli yapı taşının bilgi ögesi olduğu açıkça görülmektedir. Bireyin özel, ekonomik, sosyal hayatına ve iş ilişkilerine dair tüm bilgileri, kişisel veri kavramı kapsamındadır. Kişisel bilgiler; bireyin giydiği kıyafetin markası ve adı soyadı gibi alenen bilinebilir bilgiler olabileceği gibi cinsel yönelimi ya da siyasi görüşü gibi saklı tuttuğu bilgiler de olabilmektedir. Kişinin sahip olduğu veya önceden geçirmiş olduğu hastalıklar, maddi durumu, medeni hali ve kullandığı sosyal medya hesabının şifresi gibi gizli ya da gizli olmayan birçok bilgi, kişisel veri kavramının kapsamı içerisinde yer almaktadır (Uncular, 2014, s. 19). Bu bağlamda Türk Hukukunda işyerinde siber gözetim faaliyetine ve işçilerin kişisel verilerinin korunmasına yönelik düzenlemeler incelenecektir.

3.1. 1982 Anayasası

Teknolojik gelişmelere bağlı olarak yapılan siber gözetim faaliyetiyle bireylere ait verilerin elde edilmesi, işlenmesi, depolanması ya da başka kişilere devredilmesinin önüne geçilmesi açısından hukuksal düzenlemelerin yapılması çok önemlidir. Nitekim bireyin kişisel verilerinin korunması hakkının, diğer hak ve özgürlüklerini kullanabilmesiyle yakından ilişkili olduğu yadsınamaz bir gerçektir. Eğer bireyler kendilerine ait verilerinin korunması hakkına sahip olamazsa, diğer temel hak ve özgürlüklerini de kullanmaktan yoksun kalabilecektir (Şimşek, 2008, s. 112-113).

9/11/1982 tarihli ve 17863 sayılı Resmî Gazete'de yayımlanmış olan 1982 Anayasası, Danışma Meclisi üyeleri içerisinden seçilerek oluşturulan Anayasa Komisyonu tarafından hazırlanmıştır. Öncelikle Danışma Meclisi'nde, daha sonra da Milli Güvenlik Konseyi'nde (MGK) bu Anayasa tasarısı üzerinde konuşularak kabul edilmiştir. 7 Kasım 1982 tarihinde ise bu Anayasa, halk oylamasına sunulmuş ve

%91,37 oranında kabul oyu alarak kabul edilmiştir (Gözübüyük, 2013'ten aktaran Çoban İnce, 2018, s. 154). Ancak 16 Nisan 2017 tarihinde Türkiye'de zorunlu olarak yapılmış olan son halkoylamasıyla Anayasamızda birtakım değişikliklerin gerçekleştirilmesi hedeflenmiştir. Anayasanın 18 maddesinde yapılacak değişikliği temel alan bu referandum, %51,41 oyla kabul edilmiştir (Küçük ve Doğan, 2019, s. 1; Altıntaş, 2019, s. 24).

Anayasamızda, işyerinde işverenler tarafından gerçekleştirilen siber gözetim faaliyetine yönelik herhangi bir düzenleme yer almamaktadır. Bunun yanı sıra, işverenler, işçilerini siber gözetim faaliyeti çerçevesinde denetlediğinde işçilere ait kişisel verilere de erişmiş olacaktır. Kişisel veri kavramı, siber gözetim faaliyetinden ayrı düşünülemeyecek kadar önem taşımaktadır. Bu nedenle işverenler, işçilerinin hem özel hayatının gizliliğini hem de kişisel verilerini koruyarak siber gözetim faaliyetini gerçekleştirmekle yükümlüdür (Özdemir, 2010, s. 252).

Önceki bölümde değindiğimiz AB Temel Haklar Şartı, ülkemiz tarafından 2000 yılı itibarıyla kabul edilmiştir. Bu gelişmenin hemen ardından, 9/11/1982 tarihli ve 17863 sayılı Türkiye Cumhuriyeti Anayasasında kişisel verilerin ve özel hayatın korunmasına ilişkin düzenlemeler yapılmıştır (Küzeci, 2010, s. 285). Buna göre; Anayasanın dördüncü bölümündeki 20. madde uyarınca; "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz olduğu vurgulanmıştır (1982 Anayasası, m. 20)".

13.05.2010 tarihli ve 27580 sayılı Resmî Gazete'de yayımlanmış olan 5982 sayılı "Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkındaki Kanun" un 2. maddesiyle Anayasanın 20. maddesine ek bir fıkra getirilmiştir. Bu ek fıkra şu şekildedir:

> MADDE 20 – 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 (1982 Anayasası, m. 20).

Görülmektedir ki, Anayasa'nın 20. maddesindeki özel hayatın gizliliğinin ve kişilere ait verilerin korunmasına ilişkin hak, AİHS'nin 8. maddesiyle paralel bir biçimde düzenlenmiştir. 20. madde uyarınca; işçiler, kendilerine ait olan kişisel verilerin işverenleri tarafından işlendiğini bilme hakkına sahiptir. Bu kişisel verilerde herhangi

bir eksiklik ya da yanlışlık olduğu durumda işçiler, işverenden bu verilerin güncellenmesini ya da silinmesini talep edebilecektir. Bütün bunlara ek olarak, kişisel verilerin belirlenmiş ve meşru bir amaçla kullanılması da önemlidir. İşveren, işyerinin verimliliğini ile üretilen mal ve hizmetlerin kalitesini arttırmak amacıyla işçinin telefon görüşmelerini ya da e-posta konuşmalarını gözetlemesi meşru ve belirlenmiş bir amaç çerçevesinde ele alınabilecektir. Böyle bir amacın olmadığı durumlarda işveren, siber gözetim faaliyetiyle elde ettiği kişisel verileri depolamak ve işlemek için işçinin kendisinden onay almak zorunda kalacaktır.

Anayasanın 20. maddesindeki düzenlemeye ek olarak, 21. ve 22. maddelerindeki hükümler de siber gözetim açısından önem taşımaktadır. 21. maddede yer alan *konut dokunulmazlığı* ile 22. maddede yer alan *haberleşme özgürlüğüne* yönelik hükümler de kişisel verilerin korunması ve özel hayatın gizliliği hakkı çerçevesinde kabul edilmektedir (1982 Anayasası, m. 21 ve m. 22).

Her Türk vatandaşı, Anayasanın 20. maddesi gereğince hem özel hem de aile hayatına saygı gösterilmesini talep etme hakkına sahiptir. Başka hiçbir vatandaş tarafından kişinin özel hayatına müdahalede bulunulamaz. Benzer bir durum Anayasanın 21. ve 22. maddeleri için de geçerlidir. 21. maddede yer alan konut dokunulmazlığı hükmü şu şekildedir:

> MADDE – 21 Kimsenin konutuna dokunulamaz. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin konutuna girilemez, arama yapılamaz ve buradaki eşyaya el konulamaz (1982 Anayasası, m. 21).

21. maddede bahsedilen özel durumlardan biri olmadığı sürece hiç kimse tarafından, bir başka vatandaşın konut dokunulmazlığı ihlal edilemez. Buradan anlaşıldığı üzere, işverenler de işçilerinin konutuna müdahalede bulunma hakkına sahip değildir.

Günümüzde çalışma biçimlerinin esnekleşmesiyle işe gelmeden evden çalışma yaygınlaşmaktadır (Canbey – Özgüler, 2018, s.381). Anayasanın 21. maddesi gereğince işveren, işçisinin özel konutunda cep telefonu, kamera ve bilgisayar gibi araçlar yardımıyla keyfi biçimde siber gözetim faaliyetini yapma hakkına sahip değildir. İlgili

kanun maddesinde de açıklanan özel durumlar söz konusu olduğunda hâkim kararı doğrultusunda konut dokunulmazlığı ihlal edilebilecektir (Özdemir, 2010, s. 252-253).

Anayasanın 22. maddesinde ise, haberleşme hürriyetine ilişkin bir hüküm yer almaktadır. İlgili bu madde gereğince:

> MADDE – 22 Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz (1982 Anayasası, m. 22).

Anayasada yer alan 22. maddeye göre, kişilerin haberleşmesinin gizliliği kesin bir hak olarak belirtilmiştir. Dolayısıyla işverenler, 22. maddede belirtilen özel durumlar olmadıkça işçinin yaptığı telefon görüşmelerini dinleme hakkına sahip olamayacaktır. Aksi halde işverenler, işçilerinin özel hayatının ve haberleşmesinin gizliliğinin hakkını ihlalini gerçekleştirmiş olacaktır (Özdemir, 2010, s. 252-253).

Sonuç olarak Anayasada, işyerindeki siber gözetim faaliyetine yönelik doğrudan bir düzenleme olmamasına rağmen; işçilerin özel hayatı, kişisel verileri, konut dokunulmazlığı ve haberleşme özgürlüğü bağlamında Anayasada koruyucu hükümlerin yer aldığını söylemek mümkün olacaktır.

3.2. 4721 Sayılı Türk Medeni Kanunu (TMK)

1996 yılında Adalet Bakanlığı tarafından bir komisyon kurulmuştur. Bu komisyon, bugünkü TMK tasarısını hazırlamakla görevlendirilmiştir. Komisyonun hazırladığı Medeni Kanun Tasarısı, 1998 yılında Adalet Bakanlığı tarafından yayımlanmıştır. 1999 yılında bu kanun tasarısında yapılan değişiklik üzerine Medeni Kanun 1999 Tasarısı meydana gelmiştir. Bu Tasarı, günümüzde geçerliliğini koruyan 4721 sayılı Türk Medeni Kanunu'nun son tasarı metni olarak bilinmektedir (Başpınar, 2003, s. 79).

8/12/2001 tarihli ve 24607 sayılı Resmî Gazete'de yayımlanmış olan 4721 sayılı TMK'de, kişisel verilerin korunmasına ve siber gözetim faaliyetine ilişkin herhangi bir düzenleme bulunmamasının yanı sıra, bazı hükümler kişisel verilerin korunmasıyla bağdaştırılabilmektedir. Kişisel veriler kavramı, kişilik hakkından ayrı düşünülemez. Buna ek olarak; işverenlerin işçilerini gözetlemesi faaliyeti de işçinin kişiliğine yönelik

bir müdahaleyi ifade etmektedir (Küzeci, 2010, s. 296-297; Savaş, 2009, s. 116; Okur, 2013, s. 36).

4721 sayılı TMK'nin 24. maddesinin ikinci fıkrasının bu bağlamda incelenmesi önem arz etmektedir. Buna göre; "Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır (4721 sayılı Kanun, m. 24/2)". İlgili madde uyarınca işçilerini siber gözetim faaliyetiyle gözetleyen işverenler, hukuka uygun gerekçelerle bu gözetlemeyi gerçekleştirme hakkına sahiptir. Aksi taktirde yapılan siber gözetim faaliyeti hukuka aykırı bir nitelik taşıyor olacaktır. İşverenlerin, işçilerini gözetleme hakkı iş sözleşmesinden doğan bir sorumluluktur. Bu denetimin yapılabilmesi sınırlı çerçevede mümkündür. Siber gözetim faaliyetleri, işçilerin kişilik haklarına karşı müdahale özelliği taşıdığından, söz konusu olan siber gözetleme, hukuka uygun olarak yapılmalıdır. Hukuka uygunluk sebepleri arasında işverene kanun tarafından verilmiş olan yetkinin kullanılması, üstün nitelikteki menfaat ve işçinin rızası vardır. İşveren tarafından yapılan siber gözetim faaliyeti kanun tarafından işverene tanınmış yetkiye dayanmıyorsa ve üstün nitelikteki menfaat söz konusu değilse bu durumda işçinin onayı, en temel hukuki dayanağı meydana getirecektir (Okur, 2013, s. 37).

Doktrinde yer alan bir görüşe göre; teknolojik gelişmeler ışığında işyerlerinin korunması da giderek önemli bir konu halini almaktadır. İşyerlerinin ve işverenlerin haklı menfaatlerinin korunabilmesi amacıyla kameralarla siber gözetim faaliyetinin yapılması gerekmektedir. Buna ek olarak, kamera ile gerçekleştirilen siber gözetim faaliyetinde ölçülülük ilkesine uygun davranmak gerekmektedir. İşçinin, çalışma saatleri içerisinde keyfi molalar vermesini önlemek adına işverenlerin kameralarla gözetim yapması ölçülülük ilkesine uymaktadır. Bunun yanı sıra, işçiler için ayrılmış tuvalet ve duşların bulunduğu alanların işverenler tarafından kameralarla gözetlenmesi ise ölçülülük ilkesini ihlal eden bir faaliyet olarak kabul edilmektedir. Dolayısıyla siber gözetim faaliyetinin amacı ve ölçülü bir biçimde gerçekleştirilmesi önem taşımaktadır (Ertürk, 2002'den aktaran, Savaş, 2009, s. 116).

Kişilerin, kişilik hakkına bir başkası tarafından saldırması sonucundaki yaptırım ilgili kanunun 25. maddesinde düzenlenmiştir. Bu madde uyarınca; "Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir (4721

sayılı Kanun, m. 25/1)". Diğer bir deyişle işçiler, kişilik haklarına yönelik işverenler tarafından saldırı gerçekleştirilmesinin engellenmesini, mevcut saldırının durdurulmasının sağlamasını ya da daha önceden kişilik hakkına işveren tarafından saldırılmışsa bu saldırının hukuka aykırı olduğunun tespit edilmesini hâkimden talep edebilme hakkına sahiptir.

İlgili maddenin ikinci fıkrasına göre; "Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir (4721 sayılı Kanun, m. 25/2)". İşverenin, çalışma ortamında işçiye uyguladığı siber gözetimi faaliyeti sebebiyle işçinin kişilik haklarının çiğnenmesi durumu söz konusu olduğunda, 25. maddenin ikinci fıkrası uyarınca işçilerin *kişilik hakkını koruyucu dava* açabilmesi hakkı mevcuttur.

25. maddenin beşinci fıkrasına göre; "Davacı, kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yeri mahkemesinde dava açabilir (4721 sayılı Kanun, m. 25/5)". 4721 sayılı Kanun'un 25. maddesi çerçevesinde işçiler, işverene karşı maddi ve manevi tazminat davası açmakta özgür olduğu görülmektedir.

4721 sayılı Kanun'un 25. maddesinde yer alan davaların açılabilmesi için işveren tarafından işlenen kişisel verilerin, hukuka aykırı bir biçimde işlenmiş olması gerekmektedir. Zarar ya da kusurun bulunması zorunluluğu yoktur. İşçi çalışmaya devam ettiği sırada böyle bir dava açtığı için işveren tarafından işine son verilemez. Diğer bir deyişle, işverenin açılan dava sebebiyle iş sözleşmesini feshetme hakkı bulunmamaktadır (Uncular, 2012, s. 105).

3.3. 6098 Sayılı Türk Borçlar Kanunu (TBK)

1998 yılında Adalet Bakanlığı tarafından Borçlar Kanunu Tasarısı hazırlanması için harekete geçilmiştir. 2002 yılında bazı üniversitelerin öğretim üyeleri, Adalet Bakanlığı'ndaki görevli kişiler ve halk arasından seçilmiş bazı kişiler bir araya gelmiş ve Borçlar Kanunu için bir tasarı hazırlamıştır. Bu kanun tasarısının görüşülmesinin ardından 6098 sayılı TBK 4/2/2011 tarihli ve 27836 sayılı Resmî Gazete'de yayımlanmış ve kabul edilmiştir (Başpınar, 2011, s. 4).

6098 sayılı TBK'nin 393. maddesinde iş sözleşmesinin tanımı verilmiştir. Buna göre; "Hizmet sözleşmesi, işçinin işverene bağımlı olarak belirli veya belirli olmayan süreyle işgörmeyi ve işverenin de ona zamana veya yapılan işe göre ücret ödemeyi üstlendiği sözleşmedir (6098 sayılı Kanun, m. 393/1)". Bu anlamda iş sözleşmesinin; iş görme, ücret ödeme ve bağımlılık unsurlarından oluştuğu ifade edilmektedir.

Bağımlılık unsuru gereğince işçiler, işverenlerinin emir ve talimatları altında ve işverenin denetiminde çalışmaktadır. Bununla birlikte işçiler; işyerinin, işin ve işverenin meşru menfaatlerini korumakla yükümlüdür. Bu esnada işveren ise, işçiyi gözetme borcunu yerine getirerek hem fiziksel olarak işçinin bütünlüğünü hem de işçinin kişisel hak ve değerlerini korumak zorundadır (Yiğit, 2013, s. 29-32).

6098 sayılı TBK'nin 417. maddesinde *işçinin kişiliğinin korunması* şeklinde verilmiş bir düzenleme yer almaktadır. Bu maddenin birinci fıkrasında; aralarında bir hizmet ilişkisi bulunan işverenin işçisine karşı yükümlülükleri açıklanmıştır. Bu madde uyarınca; "İşveren, hizmet ilişkisinde işçinin kişiliğini korumak ve saygı göstermek ve işyerinde dürüstlük ilkelerine uygun bir düzeni sağlamakla, özellikle işçilerin psikolojik ve cinsel tacize uğramamaları ve bu tür tacizlere uğramış olanların daha fazla zarar görmemeleri için gerekli önlemleri almakla yükümlüdür (6098 sayılı Kanun, m. 417/1)".

417. maddenin ikinci fıkrasına göre, "İşveren, işyerinde iş sağlığı ve güvenliğinin sağlanması için gerekli her türlü önlemi almak, araç ve gereçleri noksansız bulundurmak; işçiler de iş sağlığı ve güvenliği konusunda alınan her türlü önleme uymakla yükümlüdür (6098 sayılı Kanun, m. 417/2)".

417. maddenin üçüncü fıkrasında ise; "İşverenin yukarıdaki hükümler dâhil, kanuna ve sözleşmeye aykırı davranışı nedeniyle işçinin ölümü, vücut bütünlüğünün zedelenmesi veya kişilik haklarının ihlaline bağlı zararların tazmini, sözleşmeye aykırılıktan doğan sorumluluk hükümlerine tabidir (6098 sayılı Kanun, m. 417/3)".

6098 sayılı TBK'nin 417. maddesinden anlaşılacağı üzere; maddenin birinci fıkrasında işçinin kişilik haklarının manevi boyutu koruma altına alınmıştır. Aynı maddenin ikinci fıkrasında ise, işçinin çalışma esnasında fiziksel bütünlüğünün korunmasına yönelik bir düzenleme mevcuttur. Son olarak, 417. maddenin üçüncü fıkrası uyarınca işverenin, işçisinin maddi ve manevi bütünlüğünü korumaması durumunda ortaya çıkabilecek sorumluluklar açıklanmıştır (Yiğit, 2013, s. 33).

İşyerinde, işçinin hem maddi hem de manevi bütünlüğünü korumak amacıyla işveren tarafından 6098 sayılı TBK'nin 417. maddesi uyarınca siber gözetim faaliyeti gerçekleştirilebilecektir. İşçilerin örneğin diğer işçiler tarafından psikolojik ya da cinsel tacize uğraması söz konusu olduğunda; kamera, cep telefonu ve ses kaydı yapan siber gözetim araçlarıyla iş ortamı gözetlenebilecektir. Benzer bir biçimde, işçinin sadece manevi anlamda korunması değil, vücut bütünlüğünün de korunması işverenin

sorumluluğu altındadır. Buna göre; işçinin çalışma sırasında giymesi gereken baret, tulum ya da bel destekli emniyet kemeri gibi koruyucu kıyafetleri giyip giymediğini denetlemek için işverenler kameralarla işçileri gözetleme hakkına sahiptir (Tekergül, 2010, s. 69).

6098 sayılı TBK'nin 417. maddesine aykırı davranarak işçisinin kişilik haklarına saldırıda bulunan işverenlere uygulanacak yaptırım, 58. maddede düzenlenmiştir. Bu madde uyarınca:

> MADDE 58 – Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir. Hâkim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir (6098 sayılı Kanun, m. 58).

İlgili maddede yer alan hüküm incelendiğinde kişilik hakkına saldırıda bulunulan işçinin, gördüğü manevi zararın karşılığı olarak, manevi zarar adıyla işverenin bir miktar para ödemesini talep etme hakkına sahip olduğu görülmektedir. İşçinin uğradığı bu manevi zarar, para ödemesi şeklinde sağlanabileceği gibi, hâkim kararı doğrultusunda para ödemesi yerine işçinin herhangi bir ödeme giderinin karşılanması ya da alacağı tazminata eklenmesi şekilde de işverenden temin edilebilecektir.

6098 sayılı TBK'nin 419. maddesinde kişisel verilerin kullanımına yönelik bir düzenleme yer almaktadır. Bu madde uyarınca; "İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir (6098 sayılı Kanun, m. 419)".

İşveren tarafından gerçekleştirilen siber gözetim faaliyetiyle elde edilen kişisel veriler, 6098 sayılı TBK'nin 419. maddesi uyarınca sadece belli durumlar söz konusu olduğunda kullanılabilecektir. İşçinin işe yatkınlığı ya da iş sözleşmesinin gerçekleştirilebilmesi için gerekli olan durumlarda işveren tarafından işçiye ait kişisel verilerin kullanılması mümkün olacaktır. Bu bağlamda, işveren; işyerinin ve işin meşru menfaatlerini korumak ve üretilen mal ile hizmetin iyileştirilmesini sağlamak amacıyla işçinin müşterilerle yaptığı telefon ya da e-posta görüşmelerini gözetleme hakkına sahiptir. Bununla birlikte; örneğin, müşteri hizmetleri sorumlusu olarak çalışan işçinin gün içerisindeki performansını değerlenmek adına da 6098 sayılı TBK'nin 419. maddesi uyarınca telefon görüşmeleri üzerinden siber gözetim faaliyetini gerçekleştirerek kişisel verilere erişim sağlayabilecektir (Tekergül, 2010, s. 71-72).

3.4. 5237 Sayılı Türk Ceza Kanunu (TCK)

1 Mart 1926 tarihli ve 765 sayılı TCK, İtalya'nın Ceza Kanunu esas alınarak hazırlanmıştır. Ancak 765 sayılı TCK'nin dilinin sadeleştirilmesi ve bazı yeni düzenlemeler yapılması amacıyla bazı tasarı metinleri oluşturulmuştur. 2003 yılında hazırlanan TCK Tasarısı'nın kabul edilmesiyle 5237 sayılı TCK, 12/10/2004 tarihli ve 25611 sayılı Resmî Gazete'de yayımlanarak kabul edilmiştir (Aydın, 2004, s. 249-252).

5237 sayılı TCK'nin dokuzuncu bölümü, özel hayatın gizliliğine yönelik suçları düzenleyen hükümleri içermektedir. 132. maddenin birinci fıkrasında haberleşmenin gizliliğinin ihlal edilmesi hakkındaki yaptırımlar yer almaktadır. Buna göre; "Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır (5237 sayılı Kanun, m. 132/1)". İşyerinde, işçisinin örneğin telefonla yaptığı görüşmelerini dinlemek suretiyle, işçilerin haberleşme hakkını ihlal eden işverenlere hapis ceza verileceği bu hüküm uyarınca açıktır. İşçinin konuşmalarının kaydedilmesi sonucunda işverenin alacağı ceza bir kat daha artacaktır. İşçinin başka kişilere gönderdiği ya da başkalarından aldığı e-postaların işveren tarafından depolanması da bu madde kapsamında değerlendirilmektedir.

5237 sayılı TCK'nin 132. maddesinin ikinci fıkrasında; "Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır ibaresi yer almaktadır (5237 sayılı Kanun, m. 132/2)". Bu hüküm uyarınca, kişilerin yaptığı görüşmelerin içeriğinin üçüncü kişilere açıklanmasının cezai nitelikte olduğu görülmektedir.

132. maddenin üçüncü fıkrası uyarınca ise; "Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır (5237 sayılı Kanun, m. 132/3)". 132. maddenin ilgili fıkrasına göre; işverenlerin işçileriyle yaptığı konuşmaların içeriğini, işçinin onayı olmaksızın ve hukuka aykırı bir biçimde başka kaynaklara yayması durumunda, yine bir ila üç yıl arası ceza alacağı düzenlemesi mevcuttur.

İşyerinde işverenlerin gerçekleştirdiği siber gözetim faaliyetiyle bağlantılı olan bir başka yaptırım ise ilgili Kanun'un 133. maddesinde yer almaktadır. Söz konusu bu madde, kişilerin yaptığı konuşmaların gözetlenmesi ve kaydedilmesini içermektedir. Buna göre; "Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi,

iki yıldan beş yıla kadar hapis cezası ile cezalandırılır (5237 sayılı Kanun, m. 133/1)". Benzer bir biçimde 133. maddenin üçüncü fıkrasına göre:

> MADDE 133 (3) – Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dört bin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur (5237 sayılı Kanun, m. 133/3).

133. maddenin ilgili fıkralarında yer alan hükümler uyarınca; işverenlerin, işçilerinin yaptığı görüşmeleri hukuka aykırı biçimde ve işçilerin onayı olmaksızın dinlemesi, kaydetmesi ya da başka kişilere aktarması suç kabul edildiği görülmektedir.

5237 sayılı TCK'nin 134. maddesiyle; bireylerin özel hayatının gizliliğinin ihlal edilmesinin de bir suç unsuru olduğu düzenlemesi yapılmıştır. Buna göre; "Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır (5237 sayılı Kanun, m. 134/1)".

134. maddenin ikinci fıkrası uyarınca; "Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur (5237 sayılı Kanun, m. 134/2)". Diğer bir deyişle, TCK'nin 134. maddesine göre; işverenlerin kameralar ya da ses kayıt cihazları yardımıyla gerçekleştirdiği siber gözetim faaliyeti, işçinin özel hayatının gizliliğine karşı tehdit oluşturmaktadır. Bu maddeyi ihlal eden işverenler, hapis cezasıyla cezalandırılacaktır.

5237 sayılı TCK'nin 135. maddesi ise, kişisel verilerin kayıt altına alınmasına yönelik yaptırımları içermektedir. Bu madde şöyle düzenlenmiştir:

> MADDE 135 – Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır (5237 sayılı Kanun, m. 135).

BM, ILO ve AB'nin belgelerinde olduğu gibi 5237 sayılı TCK'nin 135. maddesinde de kişilere ait bazı özel verilerin kayıt altına alınmasına daha fazla yaptırım uygulanmaktadır (Küzeci, 2010, s. 309-310).

İlgili Kanun'un 136. maddesi uyarınca ise, "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır ibaresi yer almaktadır (5237 sayılı Kanun, m. 136)". Dolayısıyla

işverenlerin, işçilerden siber gözetim yoluyla edindiği hem birtakım özel verileri kayıt altına almaması hem başka kişilere bu bilgileri iletmemesi gerekmektedir.

Kişilere ait verileri kullananların nitelikleri bakımından alacakları cezalar 137. madde uyarınca düzenlenmiştir. Buna göre; "Yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi halinde, verilecek ceza yarı oranında artırılır (5237 sayılı Kanun, m. 137)".

İlgili Kanun'un 138. maddesinde kişilere ait bilgilerin, kanunların belirlediği sürenin dolması itibarıyla sistemden silinmesi gerektiği belirtilmiştir. İşçilerinden, veri toplamış olan işverenler, kanunların belirlemiş olduğu bu süre dolduğunda işçilerin verilerini kaydettikleri sistem üzerinden silmediği taktirde TCK'nin 138. maddesinin birinci fıkrası uyarınca; "Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir (5237 sayılı Kanun, m. 138/1)". Eğer Ceza Muhakemesi Kanunu uyarınca belirlenmiş hükümlere göre ortadan kaldırılması gereken kişisel veriler suçun konusunu oluşturuyorsa bu durumda; "Verilecek cezanın bir kat arttırılacağı yaptırımı 138. maddenin ikinci fıkrasında düzenlenmiştir (5237 sayılı Kanun, m. 138)".

3.5. 5271 Sayılı Ceza Muhakemesi Kanunu (CMK)

17/12/2004 tarihli ve 25673 sayılı Resmî Gazete'de yayımlanmış olan 5271 sayılı CMK'nin kabul edilmesiyle 4/4/1929 tarihli ve 1412 sayılı Ceza Muhakemeleri Usulü Kanunu yürürlükten kaldırılmıştır. 5271 sayılı CMK uyarınca, ülkemizde ceza muhakemesinin ne şekilde yapılması gerektiğine ilişkin düzenlemeler yapılmıştır (http-71).

CMK'nin beşinci bölümünde *telekomünikasyon yoluyla gerçekleştirilen iletişim faaliyetinin denetlenmesine* yönelik hükümler verilmiştir. 135. madde gereğince, kişilerin iletişim faaliyetlerinin gözetlenebilmesi için birtakım koşulların sağlanması gerekmektedir. Bu koşullar şu şekilde ifade edilmiştir:

> MADDE 135 (1) – Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, ağır ceza mahkemesi veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Cumhuriyet savcısı kararını derhâl mahkemenin onayına sunar ve

> mahkeme, kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya mahkeme tarafından aksine karar verilmesi hâlinde tedbir Cumhuriyet savcısı tarafından derhâl kaldırılır. Bu fıkra uyarınca alınacak tedbire ağır ceza mahkemesince oy birliğiyle karar verilir. İtiraz üzerine bu tedbire karar verilebilmesi için de oy birliği aranır (5271 sayılı Kanun, m. 135/1).

Bu hükümden de anlaşılacağı üzere, kişiler arasında gerçekleştirilen iletişimin gözetlenebilmesi için kişinin şüpheli ya da sanık olması koşulu aranmaktadır. Kişinin kuvvetli derecede şüphe sebeplerine sahip olması veya kişinin işlemiş olduğu suça ilişkin delil bulunamıyor olması gerekmektedir. Aynı zamanda, hâkim ya da gecikmesinde sakınca bulunan durumlarda Cumhuriyet savcısının kararı doğrultusunda bu iletişim gözetlenebilecektir (Türkel, 2010, s. 80).

Buna ek olarak; 135. madde kapsamında iletişiminin gözetlenebilmesi için, kişinin belli suçları işlemiş olması gerekmektedir. Bu suçlar 135. maddenin sekizinci fıkrasında verilmiştir. Buna göre; "TCK'nin 79. ve 80. maddelerindeki göçmen kaçakçılığı ile insan ticareti yapma, 81, 82 ve 83. maddelerindeki kasten adam öldürme suçu, 94. ve 95. maddelerindeki işkence etme, birinci fıkrası hariç olmak üzere 102. maddesindeki cinsel saldırıda bulunma, 103. maddesindeki çocuğa yönelik cinsel istismar, 142. maddesindeki nitelikli hırsızlık yapma, 148. ve 149. maddelerindeki yağma, 188. maddesindeki uyuşturucu madde üretme ve ticaretini yapma, 197. maddesindeki parada sahtecilik yapma, 227. maddesindeki fuhuş yapma, 235. maddesindeki ihaleye fesat karıştırma, 252. maddesindeki rüşvet alma veya verme, 282. maddesindeki suçla elde edilmiş mal varlığını aklama, 302. maddesindeki devletin birliği ile ülkenin bütünlüğünü bozma, 309, 311, 312, 313, 314, 315 ve 316. maddelerindeki anayasal düzene ve bu düzenin işleyişine yönelik suçları işleme ve 328, 329, 330, 331, 333, 334, 335, 336 ve 337. maddelerindeki devlet sırlarına yönelik suçlar ve casusluk yapma; "Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanun" un 12. maddesindeki silah kaçaklığı; "Bankalar Kanunu" nun 22. maddesindeki zimmet suçu; "Kaçakçılıkla Mücadele Kanunu" içerisinde yer alan suçlar ve "Kültür ve Tabiat Varlıklarını Koruma Kanunu" nun 68. ve 74. maddelerinde yer alan suçlar sebebiyle kişinin iletişimi gözetlenebilmektedir (5271 sayılı Kanun, m. 135/8)".

Benzer bir biçimde 5271 sayılı CMK'nin 140. maddesi uyarınca, TCK'de yer alan bazı suçlar sebebiyle işçiye yönelik kuvvetli şüphe sebeplerinin olduğu durumlarda ve suçla ilgili delil bulunamadığı durumda şüpheli veya sanık işçinin hem kamuya açık hem de işyerindeki faaliyetleri siber gözetim araçları kullanılarak izlenebilecek, görüntü

ve ses kaydı yapılabilecektir. Sözü edilen bu suçlar; "TCK'nin 79, 80. maddelerindeki göçmen kaçakçılığı ile insan ticareti, 81,82 ve 83. maddelerindeki kasten öldürme, 142. maddesindeki nitelikli hırsızlık, 148 ve 149. maddelerindeki yağma ve 188. maddesindeki uyuşturucu madde üretme ve imal etme, 197. maddesindeki parada sahtecilik yapma, 227. maddesindeki fuhuş yapma, 235. maddesindeki ihaleye fesat karıştırma, 252. maddesindeki rüşvet verme, 282. maddesindeki suçla elde edilmiş mal varlığını aklama, 302. maddesindeki devletin birliği ile ülkenin bütünlüğünü bozma, 309, 311, 312, 313, 314, 315 ve 316. maddelerindeki anayasal düzene ve bu düzenin işleyişine yönelik suçları işleme ve 328, 329, 330, 331, 333, 334, 335, 336 ve 337. maddelerindeki devlet sırlarına yönelik suçlar ve casusluk yapma gibi suçları kapsamaktadır (5271 sayılı Kanun, m. 140/1)".

5271 sayılı CMK'nin 140. maddesinin ikinci fıkrası uyarınca; "Teknik araçlarla izlemeye ağır ceza mahkemesi tarafından oy birliğiyle karar verilir. İtiraz üzerine bu tedbire karar verilebilmesi için de oy birliği aranır (5271 sayılı Kanun, m. 140/2)". 140. maddenin üçüncü fıkrasına göre; "Teknik araçlarla izleme kararı en çok üç haftalık süre için verilebilir. Bu süre gerektiğinde bir hafta daha uzatılabilir. Mahkeme, bu süreye ek olarak bir defadan fazla olmamak ve toplam dört haftayı geçmemek üzere teknik araçlarla izleme süresini arttırabilecektir (5271 sayılı Kanun, m. 140/3)".

5271 sayılı CMK'nin 140. maddesinin üçüncü fıkrasından da anlaşılacağı üzere, siber gözetim faaliyetinin sürekli olarak gerçekleştirilmesi mümkün değildir. Ağır ceza mahkemesi tarafından verilen gözetleme kararı, en fazla üç haftalık süre içinde uygulanabilecektir. Böylece kişilerin özel hayatının gizliliğinin korunması ve daha az müdahaleci bir yaklaşımla gözetlenmesi sağlanacaktır.

Son olarak, 140. maddenin beşinci fıkrasında, "Bu madde hükümleri, kişinin konutunda uygulanamaz ibaresi yer almaktadır (5271 sayılı Kanun, m. 140/5)". CMK'nin 140. maddesi incelendiğinde işverenlerin, siber gözetim araçlarıyla işçilerini izleyebilmesinin yalnızca mahkeme kararı doğrultusunda gerçekleştirilebileceği görülmektedir. Günümüzde yaygın olan esnek çalışma biçimlerinden evden çalışma yöntemini kullanan işçilerin yaşadığı evde, işveren tarafından siber gözetim faaliyetinin yapılamayacağı da 140. madde kapsamında açıklanmıştır.

3.6. 4857 Sayılı İş Kanunu

15/6/1936 tarihli ve 3330 sayılı Resmî Gazete'de yayımlanmış olan 3008 sayılı İş Kanunu, Türk İş Hukuku'nun en önemli belgesi olarak kabul edilmektedir. 3008 sayılı Kanun, otuz yıl boyunca yürürlükte kalmıştır. 3008 sayılı Kanun, 18/7/1968 tarihli ve 12953 sayılı Resmî Gazete'de yayımlanmış olan 931 sayılı İş Kanunu'nun kabul edilmesiyle yürürlükten kaldırılmıştır. 931 sayılı İş Kanunu, yalnızca üç yıl uygulanabilmiştir. 1970 yılında 931 sayılı İş Kanunu, Anayasa Mahkemesi tarafından şekil yönünden iptal edilmiştir. 931 sayılı Kanun'un iptalinden bir yıl sonra, 1/9/1971 tarihli ve 13943 sayılı Resmî Gazete'de yayımlanmış olan 1475 sayılı İş Kanunu yürürlüğe girmiştir. Son olarak, 10/6/2003 tarihli ve 25134 sayılı Resmî Gazete'de yayımlanmış olan 4857 sayılı İş Kanunu'nun kabul edilmesiyle, 1475 sayılı İş Kanunu'nun yürürlükten kaldırılmıştır (Güven ve Aydın, 2013, s. 5-6).

4857 sayılı İş Kanunu'nda işverenin uyguladığı siber gözetim faaliyetine yönelik bazı düzenlemeler dolaylı olarak yer almaktadır. İş sözleşmesi aracılığıyla işçi ve işveren arasında bir bağ kurulmaktadır. İş sözleşmesi, güven ilişkisi temellerine dayanan bir sözleşme olma özelliğine sahiptir. İşçinin hem işverenin hem de işyerinin çıkarlarını koruma borcuna uyması gerektiği gibi, benzer biçimde işveren de işçiyi koruma ve gözetme borcunu yerine getirmekle yükümlüdür. İş Kanunu'nun 8. maddesine göre; "İş sözleşmesi, bir tarafın (işçi) bağımlı olarak iş görmeyi, diğer tarafın (işveren) da ücret ödemeyi üstlenmesinden oluşan sözleşmedir (4857 sayılı Kanun, m. 8)". Buna göre, iş ilişkisinin temelini işçinin bağımlılık unsuru ile işverenin ücret ödeme görevi oluşturmaktadır. İş sözleşmesindeki bağımlılık unsuruyla anlatılmak istenen, işverenin gözetim ve denetim faaliyeti çerçevesinde ve yine işverenin verdiği talimatlara uyarak işçinin işini yapmasıdır. Bu bağlamda işçiye ait verilerin işveren tarafından kötüye kullanılmaması de önem arz etmektedir (Süzek, 2008, s. 346; Uncular, 2012, s. 39-50).

İşverenin kanuna, imzalanmış olan toplu iş sözleşmesine ve iş sözleşmesine aykırı olmayacak bir biçimde işin düzgünce yürütülmesini sağlaması ile işçilerin davranışlarını işyerine uygun şekilde düzenlemesi hakkı ise yönetim hakkı çerçevesinde ele alınmaktadır. Yönetim hakkını kullanan işveren, bu hakkı keyfiliğe kaçmamak ve adil davranmak koşuluyla gerçekleştirmelidir (Uncular, 2012, s. 39-41).

İşçi, iş görme borcunu yerine getirdiği sırada işvereni de işçiyi yönetmekte, gözetlemekte ve denetlemektedir. İşverenler gerek işçinin gerekse işyerinin

verimliliğinin artmasını sağlamak, işyeri maliyetlerini düşürmek ya da işyerinde güvenliği ve denetimi sağlamak gibi amaçlar çerçevesinde işçileri gözetlemektedir. Önceki bölümlerde bahsettiğimiz üzere işveren bu gözetim faaliyetini gerçekleştirirken çeşitli siber gözetim araçlarından yardım almaktadır. Bu gözetim faaliyeti, yasal bir temele dayandırılarak yapılmalıdır. Örneğin; işçinin hırsızlık yapmasının, diğer işçileri taciz etmesinin önüne geçilmesi ya da iş verimliliğinin arttırılması amacıyla işveren, gözetimi gerçekleştirebilmektedir. Bütün bunlardan daha da önemlisi, işverenin bu gözetim faaliyetini objektif ve haklı bir menfaat doğrultusunda ve işçinin onayını almak suretiyle gerçekleştirmesinin gerekliliğidir (Küzeci, 2010, s. 304). İşveren tarafınca işçinin kişisel verilerinin korunması bu çerçevede ele alınmalıdır (Süzek, 2008, s. 346).

4857 sayılı İş Kanunu'nun 5. maddesi uyarınca işverenler, işyerinde çalışan işçiler arasında ayrım yapmamakla yükümlüdür. 5. maddeye göre; "İş ilişkisinde dil, ırk, renk, cinsiyet, engellilik, siyasal düşünce, felsefî inanç, din ve mezhep ve benzeri sebeplere dayalı ayrım yapılamaz (4857 sayılı Kanun, m. 5)".

Bununla birlikte İş Kanunu'nun 12. ve 13. maddeleri uyarınca; "Belirli süreli iş sözleşmesi ile çalıştırılan işçi, ayırımı haklı kılan bir neden olmadıkça, salt iş sözleşmesinin süreli olmasından dolayı belirsiz süreli iş sözleşmesiyle çalıştırılan emsal işçiye göre farklı işleme tâbi tutulamaz (4857 sayılı Kanun, m. 12)". Benzer şekilde kısmî ve tam süreli çalışan işçiler arasında ayrım yapılamayacağı düzenlemesine 13. maddede yer verilmiştir. Buna göre, "Kısmî süreli iş sözleşmesi ile çalıştırılan işçi, ayırımı haklı kılan bir neden olmadıkça, salt iş sözleşmesinin kısmî süreli olmasından dolayı tam süreli emsal işçiye göre farklı işleme tâbi tutulamaz (4857 sayılı Kanun, m. 13)".

4857 sayılı Kanun'un 12. ve 13. maddeleri incelendiğinde görülmektedir ki işverenler; sadece çalışma sırasında değil, aynı zamanda siber gözetim faaliyetini gerçekleştirirken de işçiler arasında herhangi bir ayrım yapma hakkına sahip değildir. Örneğin; işverenler sadece kısmi zamanlı çalışan işçileri gözetleyemezler ya da kendisiyle aynı siyasi görüşü paylaşmayan işçisinin telefonlarını dinleyemezler.

4857 sayılı Kanun'un 75. maddesi uyarınca işverenler, her işçisi için bir özlük dosyası tutmakla yükümlüdür. Bu özlük dosyasında işçinin sadece kimlik bilgilerinin değil, her türlü belgenin de işverenler tarafından saklanması gerekmektedir. Gerektiği durumlarda bu özlük dosyası işveren tarafından, yetkili kişilere gösterilmelidir. Ancak işçinin haklı çıkarlarını kapsayan bilgilerin, işveren tarafından başkalarına

açıklanmaması da Kanun'un 75. maddesinde düzenlenmiştir (4857 sayılı Kanun, m. 75). 4857 sayılı İş Kanunu'nda yer alan 75. madde, işçinin kişisel verilerinin korunması bağlamında önemlidir. İlgili maddedeki hüküm, özellikle uluslararası belgelerdeki düzenlemelerle kıyaslandığında işçinin kişisel verilerinin korunmasında yetersiz kalmaktadır (Uncular, 2012, s. 32).

İşverenin, işçinin özlük dosyasını tutmaması durumunda 4857 sayılı İş Kanunu'nun 104. maddesi uyarınca; "…75 inci maddesindeki işçi özlük dosyalarını düzenlemeyen işveren veya işveren vekiline bin iki yüz Türk Lirası idari para cezası verilir (4857 sayılı Kanun, m. 104)".

Bireylerin kişisel verilerinin korunmasına yönelik problemler işe girmeden önce başlamakta ve kişi işten çıktıktan sonra da devam etmektedir. Dolayısıyla işçinin kişisel verilerinin korunmasının sadece çalışma süresince geçerli olduğunu söylemek yanlış olacaktır. Bu bağlamda işveren, işçiyi işe almadan önce, işe uygunluğunu tespit etmek amacıyla birtakım veriler talep edebilmektedir. Kişinin adı, soyadı, oturduğu evin adresi, önceki iş yerinin adı ve adresi gibi bilgiler işverenin iş görüşmesi esnasında talep ettiği veriler arasında yer almaktadır. İşveren, işçinin bu verilerini başka kişilere aktarmamakla yükümlüdür (Küzeci, 2010, s. 301).

İşçinin, çalışma esnasında kişisel verilerinin gizliliğinin işveren tarafından ihlal edildiği durumda, işçi ve işveren arasındaki iş ilişkisi çekilmez bir hal alabilecektir. Bu bağlamda İş Kanunu'nun, 24. maddesinin ikinci fıkrası uyarınca düzenlenmiş olan *ahlak ve iyi niyet kurallarına aykırı durumlar ve benzerleri* hükmü bağlamında işçiye haklı nedene dayanan fesih imkânı sağlanmaktadır. 24. maddenin ikinci fıkrasının a, b ve d bentleri uyarınca:

> MADDE 24 (2) – Süresi belirli olsun veya olmasın işçi, aşağıda yazılı hallerde iş sözleşmesini sürenin bitiminden önce veya bildirim süresini beklemeksizin feshedebilir:
> a) İşveren iş sözleşmesi yapıldığı sırada bu sözleşmenin esaslı noktalarından biri hakkında yanlış vasıflar veya şartlar göstermek yahut gerçeğe uygun olmayan bilgiler vermek veya sözler söylemek suretiyle işçiyi yanıltırsa.
> b) İşveren işçinin veya ailesi üyelerinden birinin şeref ve namusuna dokunacak şekilde sözler söyler, davranışlarda bulunursa veya işçiye cinsel tacizde bulunursa
> d) İşçinin diğer bir işçi veya üçüncü kişiler tarafından işyerinde cinsel tacize uğraması ve bu durumu işverene bildirmesine rağmen gerekli önlemler alınmazsa. (4857 sayılı Kanun, m. 24/2).

İş Kanunu'nun 24. maddesi gereğince işveren, işçiye siber gözetim faaliyetini gerçekleştirdiğini açıklamakla yükümlü olacaktır. İşverenin, siber gözetimi yaptığını

işçiden saklamaması ve gözetim faaliyetini gerçekleştirmesine rağmen bu konuda yalan söylememesi bu madde bağlamında önemlidir. İş sözleşmesinin esaslı unsurlarından biri, işçinin işverene olan bağımlılığıdır. Bu bağımlılık gereğince işçi, işverenin gözetim ve denetim faaliyetleri çerçevesinde işi ifa etmek durumundadır. Dolayısıyla işverenin, işin yapılması esnasında işçiyi gözetlediğini bildirmemesi 24. madde kapsamında ele alınmalıdır (Savaş, 2009, s. 124).

Bütün bunlara ek olarak işverenin, işçisinin kişisel verilerinin gizliliğini ihlal etmesi, ahlak ve iyi niyet kurallarına aykırı durumlar ve benzerleri kapsamında ele alınabileceği için işçi iş sözleşmesini 24. maddenin ikinci fıkrası uyarınca haklı nedene dayanarak feshetme hakkına sahiptir (Uncular, 2012, s. 108). Diğer bir deyişle, işyerinde uygulanan siber gözetim faaliyetiyle işçiye ait kişisel veriler işçinin aleyhine sonuç doğuracak şekilde kötü amaçla kullanılıyorsa, İş Kanunu'nun 24. maddesinin ikinci fıkrası uyarınca işçi, iş sözleşmesini feshedebilecektir.

İşçilerin, işverenler tarafından işyerinde kameralar yardımıyla görüntülerinin kayıt altına alınması, telefon konuşmalarının dinlenmesi ve e-postayla yaptığı görüşmelerin içeriğine erişilmesi gibi siber gözetim faaliyetlerine dayanarak iş sözleşmesini sonlandırması söz konusu olabilecektir. Aydın'ın (2002, s. 221) görüşüne göre; iş mahkemeleri tarafından işverenin, işçisinin özel hayatının ve kişisel verilerinin gizliliği hakkını ihlal edip etmediğinin tespitinin yapılması gerekmektedir. İşveren, işçisinin özel hayatının gizliliğini ihlal etmişse bu durumda İş Kanunu'nun 24. maddesinin ikinci fıkrasında yer alan ahlak ve iyi niyet kurallarına aykırı durumlar ve benzerleri uyarınca işçi, iş sözleşmesini feshedebilecektir.

Kişisel verilerinin gizliliği hakkı ihlal edilmiş olan işçi, haklı nedenle iş sözleşmesinin feshi yoluna başvurabileceği gibi, buna ek olarak tazminat isteme hakkına da sahiptir. İşçinin tazminat talep etme hakkı İş Kanunu'nun 26. maddesinin ikinci fıkrasında düzenlenmiştir (4857 sayılı Kanun, m. 26/2).

İşçinin iş sözleşmesini derhal feshetme hakkı bulunduğu gibi, işveren açısından da derhal fesih hakkı mevcuttur. İş Kanunu'nun 25. maddesinin ikinci fıkrasının a, c, d, e, h ve ı bentlerinde yer alan ahlak ve iyi niyet kurallarına aykırı durumlar ve benzerleri hükmüne göre:

> MADDE 25 (2) – Süresi belirli olsun veya olmasın işveren, aşağıda yazılı hallerde iş sözleşmesini sürenin bitiminden önce veya bildirim süresini beklemeksizin feshedebilir:
> a) İş sözleşmesi yapıldığı sırada bu sözleşmenin esaslı noktalarından biri için gerekli vasıflar veya şartlar kendisinde bulunmadığı halde bunların kendisinde bulunduğunu ileri

sürerek, yahut gerçeğe uygun olmayan bilgiler veya sözler söyleyerek işçinin işvereni yanıltması.

c) İşçinin işverenin başka bir işçisine cinsel tacizde bulunması.

d) İşçinin işverene yahut onun ailesi üyelerinden birine yahut işverenin başka işçisine sataşması, işyerine sarhoş yahut uyuşturucu madde almış olarak gelmesi ya da işyerinde bu maddeleri kullanması.

e) İşçinin, işverenin güvenini kötüye kullanmak, hırsızlık yapmak, işverenin meslek sırlarını ortaya atmak gibi doğruluk ve bağlılığa uymayan davranışlarda bulunması.

h) İşçinin yapmakla ödevli bulunduğu görevleri kendisine hatırlatıldığı halde yapmamakta ısrar etmesi.

ı) İşçinin kendi isteği veya savsaması yüzünden işin güvenliğini tehlikeye düşürmesi, işyerinin malı olan veya malı olmayıp da eli altında bulunan makineleri, tesisatı veya başka eşya ve maddeleri otuz günlük ücretinin tutarıyla ödeyemeyecek derecede hasara ve kayba uğratması (4857 sayılı Kanun, m. 25/2).

İşverenler, iş sözleşmesini haklı nedenle feshetmenin yanı sıra İş Kanunu'nun 26. maddesinin ikinci fıkrası uyarınca işçiden tazminat talep etme hakkına sahip olacaktır (4857 sayılı Kanun, m. 26/2).

4857 sayılı İş Kanunu'nun 25. maddesinin ikinci fıkrasında bulunan düzenlemeleri siber gözetim bağlamında örneklendirmek yerinde olacaktır. Bu bağlamda işçinin; işyerine ait önemli mesleki bilgileri, başka bir rakip şirkete aktardığı işveren tarafından gözetim faaliyetiyle tespit edildiğinde, sözleşmenin haklı feshi gerçekleştirilebilecektir. Çalışma sırasında uyuşturucu, alkol ya da sigara gibi zararlı maddeleri kullanmaması gereken işçinin, işveren tarafından kameralarla gözetlenebilmesi de benzer biçimde İş Kanunu'nun 25. maddesi kapsamında yer almaktadır. Bununla birlikte sadakat borcu gereğince işçinin, işyerindeki iş saatleri içerisinde internet üzerinden çeşitli sitelere erişim sağlayarak işi aksatması, 25. maddedeki ahlak ve iyi niyet kurallarına aykırı durumlar ve benzerleri kapsamında ele alınabilecektir. İşverenler bu nedenle işçinin iş saatleri içerisindeki internet ve bilgisayar kullanımını gözetleyebilme hakkına sahiptir. İşçi, işverenine karşı sadakat borcunu yerine getirmeyerek iş saatleri içerisinde bilgisayar ve interneti kişisel amaçlı kullandığı durumda işveren tarafından haklı sebeple işten çıkartılabilecektir. Bütün bunlara ek olarak işçinin, diğer işçilere cinsel tacizde bulunduğuna yönelik şikayetlerin olması durumunda da işveren tarafından işçi kamera, ses kayıt cihazı ya da telefon gibi siber gözetim araçlarıyla gözetlenebilecektir.

Aydın'ın (2002, s. 221) bu konudaki görüşüne göre işyerinin, işin ve işverenin meşru menfaatlerinin korunması amacıyla işyerinde siber gözetim faaliyeti gerçekleştirilebilecektir. Burada önemli olan nokta, işçinin özel hayatının ve kişisel verilerinin gizliliği hakkının işveren tarafından ihlal edilmemesidir. İşverenin yaptığı siber gözetimle elde edilen veriler sonucunda haklı bir sebep doğuyorsa işveren, 4857 sayılı İş Kanunu'nun 25. maddesinin ikinci fıkrası uyarınca işçinin iş sözleşmesini derhal sonlandırabilecektir. Tüm bunlara ek olarak, işletme ve işin gereği için haklı bir sebep olmadığı halde işverenin; merak ya da kızgınlık gibi gerekçelerle siber gözetim faaliyetinde bulunması hukuka aykırıdır. Haklı ve yasal bir sebebe dayanmayan siber gözetim faaliyetiyle işçilerin özel hayatının ve kişisel verilerinin gizliliği hakkı ihlal edilmiş olacaktır. Böyle bir sebeple işverenin işçiyi işten çıkartması, haksız fesih durumunu doğuracaktır ve işçinin zararının giderilmesi gerekecektir.

3.7. 6331 Sayılı İş Sağlığı ve Güvenliği Kanunu

30/6/2012 tarihli ve 28339 sayılı Resmî Gazete'de yayımlanmış olan 6331 sayılı İSGK, AB'nin 12/6/1989 tarihli ve 89/391/EEC sayılı Direktifi tarafından mevzuatımıza kazandırılmıştır. 6331 sayılı Kanun ile, işyerlerinde iş sağlığı ve güvenliğinin sağlanması hedeflenmiştir. Bu amaçla, Kanun hem işverenlere hem de işçilere birtakım sorumluluklar yüklemektedir (Çalışkan, 2016, s. 145-148).

6331 sayılı İSGK'de işyerinde uygulanan siber gözetim faaliyetine ilişkin açık bir hüküm yer almamaktadır. Bununla birlikte Kanun'un 15. maddesinde yer alan sağlık gözetimine ilişkin düzenleme, siber gözetim faaliyetiyle bağlantılı olarak ele alınabilmektedir.

6331 sayılı Kanun'un 15. maddesinin birinci fıkrasında işverenin sağlık gözetimi yapmasına ilişkin bir düzenleme yer almaktadır. Bu maddenin a bendine göre; "İşveren, çalışanların işyerinde maruz kalacakları sağlık ve güvenlik risklerini dikkate alarak sağlık gözetimine tabi tutulmalarını sağlamakla yükümlüdür (6331 sayılı Kanun, m. 15/1)".

Kanun'un 15. maddesinin birinci fıkrasının b bendi uyarınca işverenler tarafından işçilere sağlık muayenesi yapılması gerektiği düzenlenmiştir. Buna göre; "İşverenler; işçilerin işe girmesi ile iş değişikliği yapması, işçilerin iş kazası ya da meslek hastalığına yakalanması sebebiyle işten uzaklaşarak bir süre sonra tekrar işe geri dönmek istemesi ve çalışma sırasında Bakanlık tarafından belirlenmiş aralıklarla işin

niteliği ve işyerinin tehlike sınıfına göre sağlık gözetimi yapmakla yükümlüdür (6331 sayılı Kanun, m. 15/1)".

15. madde bağlamında işverenler, işçilerinin sağlığının ve güvenliğinin korunması için sağlık gözetimi yapmakla yükümlüdür. Buradan hareketle, siber gözetimde kullanılan araçlardan biri olan kameralar aracılığıyla işverenler örneğin; şantiyede çalışan işçinin, ortaya çıkabilecek risklere karşı önlem alıp almadığını gözetlemekten sorumludur. Şantiye alanının ışıklandırmasını ve işçilere verilen baret, tulum ya da belden bağlamalı emniyet kemerlerini giyip giymediklerini işverenler, kameralarla gözetleyebilmektedir. Burada yapılacak olan siber gözetim faaliyeti, işverenin ve işyerinin meşru menfaatlerinden çok, işçinin sağlığının ve güvenliğinin sağlanması için gerekli görülmektedir.

6331 sayılı Kanun'un 15. maddesinin beşinci fıkrasında; "Sağlık muayenesi yaptırılan çalışanın özel hayatı ve itibarının korunması açısından sağlık bilgileri gizli tutulur ifadesi yer almaktadır (6331 sayılı Kanun, m. 15)". 15. maddenin birinci fıkrasında bahsedilmiş olan sağlık muayenesinden elde edilen işçinin kişisel verileri, kişilerin özel hayatının gizliliğinin korunması hakkı çerçevesinde işverenler tarafından korunmak durumundadır.

6331 sayılı Kanun'un 15. maddesinde yer alan düzenlemelere işverenler tarafından uyulmaması durumundaki yaptırımlar, 6331 sayılı Kanun'un 26. maddesinin birinci fıkrasının f alt bendinde düzenlenmiştir. Buna göre; "15 inci maddesinin birinci ve ikinci fıkralarında belirtilen yükümlülükleri yerine getirmeyen işverene … bin Türk Lirası miktarında para cezası uygun görülmüştür (6331 sayılı Kanun, m. 26)".

3.8. 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)

Ülkemizin AB üyeliği için 2013 yılının Ekim ayından, 2014 yılının Eylül ayına kadar geçen sürede kaydettiği ilerlemeyle ilgili AB tarafından bir rapor düzenlenmiştir. "AB 2014 yılı İlerleme Raporu" adı verilen bu raporda, 2010 yılında yapılan Anayasa değişikliğinden itibaren kişisel verilerin korunmasıyla ilgili herhangi bir düzenleme yapılmadığı belirtilmiştir. Mevzuattaki bu eksiklik sebebiyle kişisel verilerin yeteri kadar korunmadığına dair endişelerin ortaya çıktığı bu raporda ifade edilmiştir. Dolayısıyla AB 2014 yılı İlerleme Raporu'nda, kişisel verilerin korunması hakkında ülkemizde bir kanun oluşturulması gerekli görülmüştür (Türkiye 2014 yılı İlerleme Raporu, s. 3-6).

Kişisel verilerin korunmasına yönelik bir mevzuat oluşturulması amacıyla ülkemizde birtakım çalışmalar yürütülmüştür. Adalet Bakanlığı'nın oluşturmuş olduğu bir komisyon tarafından üç yıl boyunca çalışmalar yapılmıştır. Bu çalışmaların sonunda 2003 yılı itibarıyla "Kişisel Verilerin Korunması Kanun Tasarısı" ortaya çıkmıştır. Bu Kanun Tasarısı'nın hazırlanmasında 108 sayılı AK Sözleşmesi ile 2016/679 sayılı Genel Veri Koruma Yönetmeliği esas alınmıştır. Bu Kanun Tasarısı'nın Türkiye Büyük Millet Meclisi (TBMM) tarafından kabul edilmesiyle 6698 sayılı KVKK 7/4/2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir (Dülger, 2016, s. 106-107).

6698 sayılı yedi bölüm ve otuz üç maddeden oluşmaktadır. Bu Kanun'un düzenlenmesiyle amaçlanan; "Bireylerin kişisel verilerinin işlenmesi sırasında özel hayatın gizliliği hakkı gibi temel hak ve özgürlüklerinin korunmasının sağlanması olarak belirtilmiştir. Aynı zamanda bu Kanun, kişisel verilerin işlenmesi faaliyetini gerçekleştiren gerçek ya da tüzel kişilerin sorumluluklarını ve uymaları gereken hükümleri içermektedir (6698 sayılı Kanun, m. 1)".

6698 sayılı Kanun'un kapsamına 2. maddede yer verilmiştir. Buna göre; "Kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağı Kanun'un 2. maddesinde düzenlenmiştir (6698 sayılı Kanun, m. 2)".

Bu Kanun'un 2. maddesi uyarınca, kişisel verilerin işlenmesi yalnızca siber gözetim araçlarıyla sınırlandırılmamıştır. Bilgisayar gibi siber gözetim araçlarının yanı sıra elle işlenen veriler de bu Kanun kapsamında koruma altındadır. Buna ek olarak, kişisel verilerin işlenmesi faaliyeti sadece işverenler tarafından değil, tüzel kişilerce de gerçekleştirilebilecektir.

6698 sayılı Kanun'un ikinci bölümünde kişisel verilerin işlenmesine yönelik düzenlemelere yer verildiği görülmektedir. Kişisel verilerin işlenebilmesi için gereken koşullar 4. madde bağlamında şu şekilde verilmiştir: "Kişisel veriler hukuka ve dürüstlük kurallarına uygun şekilde işlenmeli, doğru ve güncel olmalı, belirli ve meşru amaçlar için işlenmeli, işlendiği amaçla bağlantılı bir biçimde sınırlı ve ölçülü olmalı ve belirlenen amaç doğrultusunda gereken süre boyunca saklanmalıdır (6698 sayılı Kanun, m. 4)".

Diğer bir ifadeyle 6698 sayılı Kanun'un 4. maddesi uyarınca, kişisel veriler KVKK ve diğer kanunlarda yer alan esaslara göre işlenebilecektir. İlgili maddeye göre kişisel veriler hem hukuk kurallarına hem de dürüstlük kurallarına uyacak biçimde işlenmelidir. Kişilere ait bu bilgilerin doğru olması ve sürekli olarak güncel tutulması gerekmektedir. Verileri işleyen kişiler belirli ve yasal bir amaç için bu faaliyeti gerçekleştirmek zorundadır. Aynı zamanda bu veriler, işlendikleri amaca uygunluk göstermeli, sınırlı ve ölçülü olmalıdır. Son olarak veriler, hangi amaç doğrultusunda işleniyorsa, o amacın geçerli olduğu süre boyunca kayıtlı tutulmalıdır. Süre dolduktan sonra verilerin silinmesi gerekecektir.

6698 sayılı Kanun'un 5. maddesinin birinci fıkrasına göre; "Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez (6698 sayılı Kanun, m. 5/1)". 5. maddenin ikinci fıkrasında düzenlenen durumlardan herhangi biri var olduğunda, kişinin onayına ihtiyaç duyulmaksızın kendisine ait kişisel verilerin işlenmesi işlemi gerçekleştirilebilecektir. 5. maddenin ikinci fıkrasına göre verilerin işlenebilmesi için; "…Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması gerekmektedir (6698 sayılı Kanun, m. 5/2)".

İlgili Kanun'un 6. maddesinde *özel nitelikli* olarak tanımlanan kişisel veriler açıklanmıştır. Bu özel nitelikli kişisel verilerin hangi durumlarda işlenebileceğine yönelik bir düzenlemeye yer verilmiştir. Buna göre 6. maddenin birinci fıkrası uyarınca; "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veri olarak tanımlanmaktadır (6698 sayılı Kanun, m. 6/1)".

6698 sayılı Kanun'un 6. maddesinin ikinci fıkrasına göre; "Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır (6698 sayılı Kanun, m.

6/2)". 6 maddenin üçüncü fıkrası uyarınca; "Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir (6698 sayılı Kanun, m. 6/3)".

6698 sayılı Kanun ile birlikte işçiye ait olan ve özel nitelikli sayılan etnik kökeni, sendika üyeliği ya da dini inancı gibi verilerinin işveren tarafından işlenmesi engellenmiştir. İşçinin sağlığıyla ilgili kişisel verileri söz konusu olduğunda ise, işveren tarafından bu verilerin işlenebilmesi için işçinin onayına ihtiyaç duyulmaktadır.

"Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir (6698 sayılı Kanun, m. 7/1)". Kanun'un 7. maddesi uyarınca işçilerin kişisel verilerinin işveren tarafından belirlenmiş bir amaç dışında kullanımının ya da depolanmasının önüne geçilmesi amaçlanmıştır. İşverenin meşru menfaatleri doğrultusunda belirlenmiş olan amaç ortadan kalktığı zaman, işçilerin kişisel verilerinin işçinin isteği üzerine silinmesi ya da anonim hale getirilmesi de bu Kanun tarafından düzenlenmiştir. Bu düzenlemeyle işçinin kişisel verilerinin gizliliğinin ihlal edilmesinin önüne geçilmesi amaçlanmıştır.

6698 sayılı Kanun'un 8. maddesine bakıldığında, kişisel verilerinin başkalarına aktarılmasının yasaklandığı görülmektedir. 8. maddenin birinci fıkrası uyarınca; "Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz (6698 sayılı Kanun, m. 8/1)". Kişisel verilerin hangi durumlarda veri sahibinin rızası olmadan başkalarına aktarılabileceği ise 8. maddenin ikinci fıkrasında düzenlenmiştir. Buna göre; "5. maddenin ikinci fıkrasında ve yeterli önlemler alınmak kaydıyla, 6. maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir (6698 sayılı Kanun, m. 8/2)".

Kanun'da yapılmış olan bu düzenlemeyle birlikte işçiye ait kişisel verilerin, işveren tarafından üçüncü kişilere iletilmesinin önüne geçilmiştir. Diğer bir ifadeyle, işçinin kişisel verilerinin gizliliği bu madde bağlamında korunma altına alınmıştır.

6698 sayılı Kanun'un üçüncü bölümünde haklar ve yükümlülükleri açıklayıcı düzenlemeler mevcuttur. 10. maddenin birinci fıkrası uyarınca; "Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ve 11. maddede sayılan diğer hakları konusunda bilgi vermekle yükümlüdür (6698 sayılı Kanun, m. 10/1)".

10. maddede yer alan hükümle birlikte işverenin, işçiden gizli bir biçimde gözetim yaparak işçinin verilerine erişmesinin önüne geçilmesi amaçlanmıştır. İşçiye ait kişisel veriler toplanırken, siber gözetim faaliyetinde bulunan işverenin ne amaçla bu gözetimi gerçekleştirdiğini ve işçinin verilerine erişim sağladığını açıklaması zorunlu kılınmıştır. Böylece işçi hem siber gözetim faaliyetinden hem de kişisel verilerinin işlendiğinden haberdar olacaktır. Sadece kişisel verilerin toplanması ve işlenmesi sırasında değil, aynı zamanda başka kişilere bu verilerin aktarılması durumunda da işçilerin bilgilendirilmesi gerekmektedir.

Verileri işlenen kişilerin sahip olduğu haklar 11. maddenin birinci fıkrasında açıklanmıştır. Buna göre; "Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, 7. maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir (6698 sayılı Kanun, m. 11)".

İşçinin, siber gözetim faaliyetiyle elde edilen kişisel verileri hakkında bilgilendirilmesi gerektiği 6698 sayılı Kanun'un 11. maddesinde düzenlenmiştir. İşçinin iş sırasında kullandığı cep telefonundaki mesajları işveren tarafından gözetleniyorsa, hangi mesajlarının okunduğu ve neden bu gözetim faaliyetinin gerçekleştirildiği gibi bilgiler işçiye verilmek zorundadır. İşçiden toplanan verilerde herhangi bir eksiklik, yanlışlık ya da değişiklik olması durumunda işçi, verilerin değiştirilmesini işverenden

talep etme hakkına sahiptir. Bütün bunlara ek olarak işçi, kendisine ait verilerin işveren tarafından kanuna aykırı olarak toplandığını fark ederse, uğradığı zararın giderilmesi için talepte bulunabilecektir.

6698 sayılı Kanun çerçevesinde verileri işleyen kişilere birtakım sorumluluklar yüklenmektedir. Madde 12'nin birinci fıkrası uyarınca; "Veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek ile hukuka aykırı olarak erişilmesini önlemek ve verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır (6698 sayılı Kanun, m. 12/1)".

12. maddenin ikinci fıkrası uyarınca; "Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur (6698 sayılı Kanun, m. 12/2)". İlgili maddenin üçüncü fıkrasına göre; "Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır (6698 sayılı Kanun, m. 12/3)". 12. maddenin dördüncü fıkrası uyarınca; "Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder (6698 sayılı Kanun, m. 12/4)". 12. maddenin sonuncu fıkrasına göre ise; "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir (6698 sayılı Kanun, m. 12/5)". Bahsedilen bu Kişisel Verileri Koruma Kurumu ise; "Cumhurbaşkanı tarafından görevlendirilmiş bakanlardan oluşmaktadır ve Ankara'da bulunmaktadır (6698 sayılı Kanun, m. 19)".

6698 sayılı Kanun'un 12. maddesinde yer alan düzenlemeleri örneklendirmek yerinde olacaktır. Buna göre; işverenler, siber gözetim faaliyetiyle elde ettikleri kişisel verileri korumakla yükümlüdür. Bu anlamda işverenler, gereken tüm önlemleri alarak işçinin kişisel verilerinin gizliliğini sağlamakla görevlendirilmiştir. İşveren yerine, işverenin yetkilendirdiği bir başka kişi verilerin işlenmesi faaliyetini yürütüyorsa bu durumda hem verileri işleyen kişi hem de işveren ortaklaşa sorumluluk altında olacaktır. 12. madde çerçevesinde işveren, verilerin işlenmesi sırasında işyerinde 6698 sayılı

Kanun'da yer alan düzenlemelere uyulup uyulmadığını denetlemekle yükümlüdür. Diğer bir deyişle, siber gözetimi gerçekleştiren işveren, buradan edindiği kişisel verilerin 6698 sayılı Kanun'a uygun bir biçimde işlenmesini sağlamakla görevlidir. İşveren, işçinin verilerini yalnızca meşru ve belirli bir amaç doğrultusunda işleme hakkına sahiptir. Meşru ve belirlenmiş bir amaca, işyerinin verimliliğinin artması örnek gösterilebilir. İşverenin, işyerinin ve işçilerin verimliliğini kontrol amacıyla yaptığı siber gözetim faaliyetinden elde ettiği kişisel verileri depolamasında 12. madde bağlamında sakınca bulunmamaktadır. Meşru ve belirlenmiş bir sebeple verileri işleyen işverenler, bu verileri amaca aykırı olarak kullanamayacaktır ya da başkalarına aktaramayacaktır. Verileri işlemekle görevlendirilen kişinin, işyerindeki iş sözleşmesi sona erse bile, bu hüküm geçerli olmaktadır. Son olarak, görevli kişi, verilere başka bir kişi tarafından erişildiğini fark ettiği anda bu durumu hemen işverene ve Kişisel Verileri Koruma Kurumu'na bildirmekle yükümlü olacaktır.

6698 sayılı Kanun'da kişisel verilerin işlenmesi faaliyetinin yaptırımları da düzenlenmiştir. 17. maddenin birinci fıkrası uyarınca; "Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140. madde hükümleri uygulanır (6698 sayılı Kanun, m. 17/1)".

6698 sayılı Kanun'un 17. maddesinin ikinci fıkrasına göre; "Bu Kanunun 7. maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır (6698 sayılı Kanun, m. 17/2)".

Son olarak, 6698 sayılı Kanun'da kişisel verilerin işlenmesiyle ilgili suçların yaptırımlarına da yer verilmiştir. Bu bağlamda 18. madde uyarınca; "Bu Kanun'un; 10. maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar, 12. maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar, 15. maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar ve 16. maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verilir. Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır (6698 sayılı Kanun, m. 18/1-2)".

SONUÇ

Sanayi Devrimi sonrasında işyerlerinin sayısının artması, üretim faaliyetlerinin gelişmesi ve teknolojide meydana gelen yeniliklerin önlenemez yükselişiyle birlikte çalışma hayatında bilgisayar, telefon ve kamera gibi teknolojik cihazlar kullanılarak işverenlerce gerçekleştirilen siber gözetim faaliyeti giderek artmıştır. Siber gözetim faaliyetinin en önemli parçasını işçilere ait veriler oluşturmaktadır. Kimliği belirlenmiş ya da belirlenmesi mümkün olan bireylere ait kişisel verilerin, siber gözetim faaliyeti kapsamında korunması büyük bir gerekliliktir.

İşçinin, gözetim ve denetim faaliyeti çerçevesinde ve işvereninin verdiği talimatlar doğrultusunda işini yapma borcu olduğu gibi, işveren de işçisini korumak ve işçisinin haklarını gözetmekle yükümlüdür. Bu bağlamda sadece işçinin kişiliğinin korunması ve gözetilmesi değil, aynı zamanda işçinin kişiliğiyle bağlantılı olan kişisel verilerinin de korunması ve özel hayatının gizliliğinin sağlanması gerekmektedir.

Teknolojinin her geçen gün hızlı bir biçimde ilerlemesi sonucunda, işyerinde işveren tarafından uygulanan siber gözetim faaliyetiyle işçinin özel hayatına ilişkin müdahalenin sınırları giderek genişlemektedir. İşçilerin, bu müdahalelerden etkilenmemesi, özel hayatlarının gizliliğinin muhafaza edilmesi ve kişisel verilerinin korunması bu bağlamda giderek önem kazanmaktadır. Kanımızca gerek uluslararası gerekse ulusal belgelerde yer alan düzenlemelerin teknolojiyle paralel doğrultuda gelişmemesi en önemli eksikliktir. Her geçen gün gelişen siber gözetim faaliyetlerinde işçinin kişiliğinin ve kişisel verilerin korunması için kapsamlı hukuki düzenlemelere ihtiyaç duyulmaktadır.

Uluslararası belgelerde hem siber gözetim faaliyetine hem de işçiye ait kişisel verilerin korunmasına yönelik yeni düzenlemeler yapılması gerektiği tarafımızca önerilmektedir. OECD'nin kişisel verilerin korunmasıyla ilgili belgeleri mevcuttur. Bu anlamda en güncel belgesi 2002 tarihi itibarıyla yürürlüğe konmuştur. "Bilgi Sistemlerinin Güvenliğine İlişkin OECD Rehber İlkeleri: Güvenlik Kültürüne Doğru" adıyla yayınlanan bu belgenin hükümlerine bakıldığında, özellikle işyerinde işçiler ile işverenler arasındaki siber gözetim faaliyetini tanımlayan ve buna uygun düzenlemeler içeren bir belge olmadığı görülmektedir. Dolayısıyla OECD tarafından siber gözetim faaliyetinde işçiyi koruyan düzenlemelerin yer aldığı yeni bir düzenlemenin yapılması önerilebilir.

BM'nin yapmış olduğu düzenlemeler de kişisel verilerin korunmasına yöneliktir. "Bilgisayar Aracılığıyla Toplanmış Kişisel Veri Dosyalarına İlişkin Rehber İlkeler" adındaki BM belgesinde, bireylere ait kişisel verilerin toplanmasıyla ilgili düzenlemeler yapıldığı görülmektedir. Ancak hem bu belgede hem de diğer BM belgelerinde özellikle işyerindeki siber gözetim faaliyetine ilişkin herhangi bir düzenleme bulunmamaktadır. Bu bağlamda, işçilerin siber gözetim faaliyeti sırasında korunmasına yönelik birtakım düzenlemeler yapılması tavsiye edilebilir.

Ülkelerdeki düzenlemelere bakıldığında, Almanya'nın mevcut Anayasa'sında da tıpkı ülkemizde olduğu gibi kişisel verilerin korunmasına yönelik herhangi bir düzenleme bulunmadığı görülmektedir. Siber gözetim faaliyetinin temelinde kişisel verilerin bulunduğu düşünüldüğünde, bu verilerin korunması öncelikle Anayasal hükümlerle sağlanmalıdır. Bu bağlamda Alman Anayasası'nda kişisel verilerin korunmasına yönelik düzenlemeler eklenerek, mevcut eksikliklerin giderilmesi gerekmektedir.

Tüm teknolojik gelişmelere ev sahipliği yapan ve bu nedenle teknolojinin kötüye kullanılması riskinin daha fazla olduğunu düşündüğümüz ABD'nin işyerinde siber gözetim faaliyetine ve kişisel verilerin korunmasına ilişkin düzenlemeler yapma konusunda çok geç kalmış olduğu söylenebilir. Buna ek olarak siber gözetim faaliyetiyle gözetlenen işçilere ve bu işçilere ait verilerin korunmasına yönelik birtakım düzenlemelerin ABD'nin mevzuatına eklenmesi önerilebilir.

Ülkemizde yer alan kanun ve yönetmelikler incelendiğinde, çalışma hayatında işçinin kişisel verilerinin korunması anlamında ne yazık ki yeterli düzenlemelerin olmadığı görülmektedir. Mevcut Anayasa'da çalışma hayatında işlenen kişiler verilerle ilgili bir düzenleme olmamasının yanı sıra, günlük hayatta da kişisel verilerin işlenmesine yönelik herhangi bir düzenleme bulunmamaktadır. Dolayısıyla, Anayasa'da kişisel verilerin korunmasına yönelik doğrudan bir düzenleme yapılabilir.

4857 sayılı İş Kanunu'nun 24. ve 25. maddelerinde dolaylı olarak hem işçinin kişisel verilerinin hem de işverenin iş ve işyeriyle ilgili verilerinin korunmasının gerekliliğine yönelik düzenleme yapılmıştır. Bu bağlamda İş Kanunu'nda işçinin kişisel verilerinin korunması ve özel hayatının gizliliğinin sağlanması bakımından doğrudan düzenlenmiş hükümlere yer verilmesi yerinde olacaktır. İşverenin hangi durumlarda siber gözetim faaliyetini gerçekleştirmesinin gerekli olduğu, hangi elektronik cihazları kullanabileceği ve verileri nasıl işlemesi gerektiğinin açıkça düzenlendiği hükümler,

ilgili Kanun'a eklenmelidir. Nitekim işçiler böylece, bu düzenlemeler karşısında mahremiyet haklarının ihlal edildiğini düşünmeyecektir. Bu Kanun'da yapılan düzenlemelere uyulmamasına ilişkin cezai yükümlülüklere ise 5327 sayılı TCK kapsamında yer verilebilir. Dolayısıyla kişisel görüşümüz, hem 4857 sayılı hem de 5327 sayılı kanunlardaki eksikliklerin, yapılacak düzenlemelerle giderilmesi yönündedir.

Ülkemiz, çalışma hayatında uygulanan siber gözetim faaliyetine ilişkin düzenlemeleri hem uluslararası belgelere hem de diğer ülkelere kıyasla daha geç yapmıştır. AB 2014 yılı İlerleme Raporu'nda Türkiye'de kişisel verilerin korunmasına yönelik düzenlemelerin eksikliğinin vurgulanmıştır. Gerek özel hayatın gizliliğinin sağlanması gerekse bireylere ait kişisel verilerin korunması amacıyla ülkemizde 2016 yılında, 6698 sayılı KVKK yürürlüğe konmuştur. Ancak Almanya'da, kişisel verilerin korunmasına yönelik ilk kez 1970 yılında kanun çıkartıldığı göz önünde bulundurulduğunda ülkemizdeki bu Kanun'un, dünya genelinde çok geç yürürlüğe konduğu söylenebilmektedir. Dolayısıyla ülkemizde, kişisel verilerin korunması anlamında KVKK'de hem daha detaylı düzenlemeler yapılması hem de bu düzenlemelerin titizlikle uygulanması önerilebilir.

Kişisel verilerin korunması anlamında ülkemizdeki temel eksikliğin giderilmiş olmasının yanı sıra halen siber gözetim faaliyetine yönelik herhangi bir kanun bulunmamaktadır. Tarafımızca mevzuattaki bu boşluk, ülkemizdeki siber gözetim faaliyetinin işverenler tarafından kötüye kullanılmasına olanak tanıyabilmektedir. Ayrıca işçiler açısından da özellikle kişisel verilerinin korunması ve mahremiyet bağlamında olumsuzluklar yaşanmasına sebep olabilmektedir. Bu olumsuzlukların giderilmesi ve işçilerin mağduriyetinin ortadan kaldırılması için bir an önce gerekli düzenlemelerin yapılması önerilebilir. Diğer bir deyişle, gözetim ve siber gözetim kavramlarının tanımlanmasıyla, işyerinde uygulanan bu faaliyete karşı işçilerin nasıl korunabileceğine yönelik hükümlerin yer aldığı bir kanun oluşturulabilir. Sonuç olarak, böyle bir düzenlemenin yapılmasıyla hem işverenler için siber gözetimin sınırları belirlenebilir hem de işçilerin siber gözetim faaliyetine karşı özel hayatının gizliliği ile kişisel verilerinin korunması sağlanabilir.

KAYNAKÇA

Abrahamse, S.R. (2014). *Electronic communications in the workplace*. Yüksek Lisans Tezi. Cape Town: University of Cape Town.

Akçakaya, V. (2009). Üniversiteler için kişisel web site çözümü sabancı üniversitesi örneği: myWeb. *11. Akademik Bilişim Konferansı*'nda sunulan bildiri. Şanlıurfa: Harran Üniversitesi.

Akgül, A. (2013). *Kişisel verilerin korunması açısından idarenin hukuki sorumluluğu ve yargısal denetimi*. Doktora Tezi. Kocaeli: Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü.

Aksoy, H.C. (2008). *Kişisel verilerin korunması*. Yüksel Lisans Tezi. Ankara: Ankara Üniversitesi, Sosyal Bilimler Enstitüsü.

Akyürek, G. (2011). *Özel hayatın gizliliğini ihlal suçu*. Ankara: Seçkin Yayıncılık.

Alder, G.S., Noel, T.W. ve Ambrose, M.L. (2006). Clarifying the effects of internet monitoring on job attitudes: the mediating role of employee trust. *Information & Management*, 43, 894–903.

Algan, E. (1999). Fotoğraf okuma ve görüntü çözümlemesine giriş. Eskişehir: Çözüm İletişim Yayınları'ndan aktaran Göktepe, E. (2015). *Geçmişten günümüze hareketli görüntü ve türkiye'de animasyonun gelişimi*. Yüksek Lisans Tezi. İstanbul: İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü.

Aloisi, A. ve Gramano, E. (2019). Artificial intelligence is watching you at work: digital surveillance, employee monitoring and regulatory issues in the eu context. *Comparative Labor Law & Policy Journal*, 1 (1), 1-25.

Al-Rjoub, H., Zabian, A. ve Qawasmeh, S. (2008). Electronic monitoring: the employees point of view. *Journal of Social Sciences*, 4 (3), 189-195.

Altıntaş, M. (2019). 16 Nisan 2017 referandumunun gazete manşetlerindeki sunumu: hürriyet, sabah, sözcü ve posta örneğiyle. *Erciyes İletişim Dergisi*, 6 (1), 17-34.

Ariss, S.S. (2002). Computer monitoring: benefits and pitfalls facing management. *Information & Management*, 39, 553-558.

Atak, S. (2010). Avrupa konseyi'nin kişisel veriler açısından sağladığı temek güvenceler. *Türkiye Barolar Birliği Dergisi*, 87, 90-120.

Avcı, N. (1999). *Enformatik Cehalet*. İstanbul: Kitabevi Yayınları.

Avcı, Ö. (2015). Dijital yaşamın dijital özne(l)leri: herkes ya da hiç kimse. *Uşak Üniversitesi Sosyal Bilimler Dergisi*, 8 (1), 249-266.

Aydemir, M. (2012). *İşyerinde mahremiyet olgusu*. İstanbul: Beta Yayıncılık.

Aydın, U. (2002). *İş hukukunda işçinin kişilik hakları*. Eskişehir: Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Yayınları.

Aydın, D. (2004). Yeni türk ceza kanunu'nun hazırlanış süreci. *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, 59 (4), 249-263.

Bajc, V. (2007). Debating surveillance in the age of security. *American Behavioral Scientist*, 50 (12), 1567-1591.

Başaran, F. (1998). Yeni bir iletişim ortamı: internet. *Birikim Dergisi*, 110, 1-5.

Başaran. F. (2010). Yeni iletişim teknolojileri, alternatif iletişim olanakları. *Mülkiye Dergisi*, 34 (269), 255-270.

Başpınar, V. (2003). Türk medeni kanunu ile aile hukukunda yapılan değişiklikler ve bu konuda bazı önerilerimiz. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 52 (3), 79-101.

Başpınar, V. (2011). 6098 sayılı türk borçlar kanunu'na ilişkin şeklî yönden genel değerlendirme. *6098 Sayılı Türk Borçlar Kanunu Sempozyumu*, 3-15.

Baştürk, E. (2016). *Gözetimin soykütüğü*. İstanbul: Kalkedon Yayıncılık.

Bauman, Z. (1997). *Özgürlük* (Çev: V. Erenus). İstanbul: Sarmal Yayınevi.

Bauman, Z. (1998). *Globalization: the human consequences*. Oxford: Polity Press.

Bennett, C.J ve Raab, C.D. (2004). *The governance of privacy: policy instruments in global perspective*. London: Ashgate Publishing.

Bentham, J., Watkin, C.P., Werret, S., Çoban, B. ve Özarslan, Z. (2008). *Panoptikon: gözün iktidarı* (Çev: B. Çoban ve Z. Özarslan). İstanbul: Su Yayınevi.

Bilgin, A.B. (2016). Avrupa birliği hukukunda hukukun genel ilkeleri. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 74 (1), 73-94.

Binark, İ. (1979). Bilgi işlem, bilgi işlem sistemleri, tarihçe, bilgisayarlar ve ülkemizdeki durum. *Türk Kütüphaneciliği Dergisi*, 28 (4), 181-206.

Botan, C. (1996). Communication work and electronic surveillance: a model for predicting panoptic effects. *Communication Monographs*, 63(4), 293-313.

Boyanov, K. (2003). John vincent atanasoff: the inventor of the first electronic digital computing. *International Conference on Computer Systems and Technologies-CompSysTech*, s. 1-7. Sofia, Bulgaria.

Bozkurt, V. (2000). Gözetim ve internet: özel yaşamın sonu mu?. *Birikim Dergisi*, 136, 75-81.

Bölükbaş, Ö.Ö. (2014). *İnsan hakları ve elektronik gözetim*. Yüksek Lisans Tezi. Konya: Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü.

Briggs, A. ve Burke, P. (2011). Medyanın toplumsal tarihi: gutenberg'den internet'e. İstanbul: Kırmızı Yayınları'ndan aktaran Cizmeci, E. (2015). Yeni medya ve serbest zaman. F. Aydoğan (Editör), *İletişim çalışmaları* içinde (81-99). İstanbul: Derin Yayınları.

Bük, A. (2015). *Elektronik ortamda saklanan kişisel verilerin elde edilmesi/değiştirilmesi suretiyle işlenen suçların ceza hukuku açısından değerlendirilmesi*. Doktora Tezi. Ankara: Polis Akademisi, Güvenlik Bilimleri Enstitüsü.

Büyük, K. ve Keskin, U. (2012). Panoptikon'un elektronik dirilişi: etik bir sorun olarak işyeri izleme. *İş Ahlakı Dergisi*, 5 (10), 55-88.

Campbell-Kelly, M., Aspray, W., Ensmenger, N. ve Yost, J.R. (2014). *Computer: a history of the information machine*. Philadelphia: Westview Press.

Can, İ. (2004). Almanya'da devletin yapısı ve vergi sisteminin anayasal temelleri. *Maliye Dergisi*, 145, 1-60.

Canbey-Özgüler, V. (2005). Bilgi ekonomisinde istihdamın değişen yapısı ve işgücü özellikleri. *Çimento İşveren Dergisi*, 19 (5), 23-41.

Canbey – Özgüler, V. (2015). Yeni teknolojiler ve türkiye'de bilişim iletişim teknolojileri uygulamaları. V. Canbey – Özgüler (Editör), *Yeni teknolojiler ve çalışma hayatı* içinde (s. 208-242). Eskişehir: Anadolu Üniversitesi Açıköğretim Yayınları.

Canbey – Özgüler, V. (2018). Yeni teknolojiler ve örgütler. M. Zencirkıran (Editör), *Örgüt sosyolojisi* içinde (s. 371-401). Bursa: Dora Yayıncılık.

Carayon, P. (1993). Effect of Electronic performance monitoring on job design and worker stress: review of the literature and conceptual model. *Human Factors*, 35 (3), 385-395.

Carayon, P. (1994). Effects of electronic performance monitoring on job design and worker stress: results of two studies. *International Journal of Human-Computer Interaction*, 6 (2), 177-190.

Castells, M. (2010). *The information age: economy, society, and culture, volume I the rise of the network society*. West Sussex: Blackwell Publishing.

Civelek, D.Y. (2011). *Kişisel verilerin korunması ve bir kurumsal yapılanma önerisi*. Uzmanlık Tezi. T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı.

Connolly, R. ve McParland, C. (2012). Dataveillance: employee monitoring & information privacy concerns in the workplace. *Journal of Information Technology Research*, 5 (2), 31-45.

Cozzetto, D.A. ve Pedeliski, T.B. (1996). Future implications for managers privacy and the workplace. *Human Resource Management Review*, 6 (3), 21-31.

Cunha, M.V.A. (2013). *Market integration through data protection: an analysis of the insurance and financial industries in the eu*. London: Springer Science + Business Media.

Çakır, M. (2015). *İnternette gösteri ve gözetim*. Ankara: Ütopya Yayınevi.

Çalışkan, S. (2016). *Yöneticilerin 6331 sayılı iş sağlığı ve güvenliği kanunu ile getirilen uygulamalara yönelik algı ve beklentilerinin analizi: marmara bölgesi örneği*. Doktora Tezi. Karabük: Karabük Üniversitesi, Sosyal Bilimler Enstitüsü.

Çaycı, A. E. ve Çaycı, B. (2017). Dijital iletişim çağında teknolojinin açığa çıkardıkları: gözetim ve mahremiyet. *The Turkish Online Journal of Design Art and Communication*, 7 (1), 36-46.

Çetin, M. ve Asıl, S. (2017). Günümüz toplumunda gözetim olgusu. *Üçüncü Sektör Sosyal Ekonomi Dergisi,* 52 (1), 180-205.

Dabosville, B. (2013). Protection of employees' personal information and privacy in france. *Le Monde,* 1 (1), 31-47.

DiLuzio, S. (2000). Workplace e-mail: it's not as private as you might think. *Journal of Corporate Law*, 25 (3), 741-760.

Dolgun, U. (2005a). Çalışma yaşamında gözetim. *Sosyal Siyaset Konferansları Dergisi*, 0 (49), 507-539.

Dolgun, U. (2005b). *Enformasyon toplumundan gözetim toplumuna*. Ankara: Eki Kitabevi.

Dolgun, U. (2008). *Şeffaf hapishane yahut gözetim toplumu*. İstanbul: Ötüken Neşriyat.

Dönmez, A. (2001). Bilgisayarcı matematikçiler. *Doğuş Üniversitesi Dergisi*, 2 (2), 29-38.

D'Urso, S. C. (2006). Who's watching us at work? toward a structural-perceptual model of electronic monitoring and surveillance in organizations. *Communication Theory*, 13 (3), 281-303.

Dülger, M.V. (2016). Kişisel verilerin korunması kanunu ve türk ceza kanunu bağlamında kişisel verilerin ceza normlarıyla korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi,* 3 (2), 101-167.

Dülger, M.V. (2018). İnsan hakları ve temel hak ve özgürlükler bağlamında kişisel verilerin korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 5 (1), 71-143.

Ekinci, B.T. (2017). Video kliplerde zamanın ve mekânın sunumu: sinemagraf. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi,* 4 (12), 825-842.

Ekiz, H., Vatansever, F., Zengin, A. ve Demir, Z. (2000). Hesaplamanın tarihi ve bilgisayarların gelişimi. *Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 4 (1-2), 73-81.

Erdoğdu, A. (1972). Ceza yargılama yöntemi yasası terimleri sözlüğü. Ankara: Türk Dil Kurumu Yayınları'ndan aktaran Bölükbaş, Ö.Ö. (2014). *İnsan hakları ve elektronik gözetim*. Yüksek Lisans Tezi. Konya: Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü.

Eren, H. ve Zülfikar, H. (1985). *Anayasa sözlüğü*. Ankara: Türk Tarih Kurumu Basımevi.

Erkan, H. (2015). Yeni iletişim ve bilişim teknolojilerinin ortaya çıkışı. V. Canbey – Özgüler (Editör), *Yeni teknolojiler ve çalışma hayatı* içinde (s. 2-39). Eskişehir: Anadolu Üniversitesi Açıköğretim Yayınları.

Ertürk, Ş. (2002). İş ilişkisinde temel haklar. Ankara: Seçkin Yayınevi'nden aktaran Savaş, F.B. (2009). İş hukukunda "siber gözetim". *Çalışma ve Toplum Dergisi*, 3, 97-132.

Everett, A.M., Wong, Y.Y. ve Paynter, J. (2004). Balancing employee and employer rights: an international comparison of e-mail privacy in the workplace. *Journal of Individual Employment Rights,* 11 (4), 291-310.

Fernandez, J. (2004). Right and wrongs of e-mail monitoring. Mumbai: CXO Today'den aktaran Kierkegaard, S. (2005). Privacy in electronic communication – watch your e-mail: your boss is snooping!. *Computer Law & Security Report*, 1, 226-236.

Foucault, M. (1995). *Discipline and punish: the birth of the prison*. England: Penguin Books.

Garfinkel, S.L. ve Grunspan, R.H. (2018). *The computer book: from the abacus to artificial intelligence, 250 milestones in the history of computer science*. New York: Sterling Publishing.

George, J.F. (1996). Computer-based monitoring: common perceptions and empirical results. *MIS Quarterly*, 20 (4), 459-480.

Giddens, A. (1985). *The Nation-state and violence*. United Kingdom: Polity Press.

Giddens, A. (2000). *Tarihsel materyalizmin çağdaş eleştirisi* (Çev: Ü. Tatlıcan). İstanbul: Paradigma Yayınları.

Giddens, A. (2006). *Sociology*. Cambridge: Polity Press.

Godfrey, B. (2000). Electronic work monitoring: an ethical model. *The Second Australian Institute Conference on Computer Ethics*, s. 18-21. Canberra, Australia.

Göktepe, E. (2015). *Geçmişten günümüze hareketli görüntü ve türkiye'de animasyonun gelişimi*. Yüksek Lisans Tezi. İstanbul: İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü.

Gören, Z. (1992). Türk-Alman hukukunda kişiliğin korunması. *Anayasa Yargısı Dergisi*, 92, 165-184.

Gözübüyük, Ş. (2013). Anayasa Hukuku. Ankara: Turhan Kitabevi'nden aktaran Çoban İnce, İ. (2018). 1982 *Anayasası döneminde yasama ve yürütme ilişkilerinin evrimi*. Doktora Tezi. İzmir: Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü.

Grupe, F.H., Kuechler, W. ve Sweeney, S. (2003). Dealing with data privacy protection: an issue for the 21st century. *EDPACS: The EDP Audit, Control, and Security Newsletter*, 30 (7), 4-19.

Güçlü, N. (2001). Stres yönetimi. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi*, 21 (1), 91-109.

Güntürk, M.S. (2012). *Türk yüksek mahkemeleri ve avrupa insan hakları mahkemesi kararları ışığında özel hayatın gizliliğinin korunması*. Ankara: Seçkin Yayıncılık.

Güven, O.Ö. (2012). *Gözetimin neoliberal "risk" bağlamında dönüşümü ve mobese kameraları*. Doktora Tezi. İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü.

Güven, E. ve Aydın, U. (2013). *Bireysel İş Hukuku*. Eskişehir: Nisan Kitabevi.

Güven, O.Ö. (2014). Gözetim tekniklerinin güç ilişkileri bağlamında dönüşümü ve toplumsal denetim. *Atatürk İletişim Dergisi*, 7, 79-112.

Güven, S.K. (2016). Gözetimin toplumsal meşruiyeti. H. Köse (Editör), *Medya Mahrem* içinde (s. 173-198). İstanbul: Ayrıntı Yayınları.

İbiş, S. ve Batman, O. (2014). Elektronik gözetim uygulamalarının çalışanlar üzerindeki etkileri: istanbul'daki seyahat acentaları üzerine bir araştırma. *13. Geleneksel Turizm Paneli,* 1-12.

İşman, A. (2001). Bilgisayar ve eğitim. *Sakarya Üniversitesi Eğitim Fakültesi Dergisi,* 2, 1-34.

Kalaman, S. (2013). Özel hayatın gizliliği, kitle iletişim araçları ve yasal düzenlemeler. N. Ankaralıgil (Editör). *Medya ve iletişim politikaları: güncel tartışmalar, düzenlemeler* içinde (155-192). İzmir: Tibyan Yayıncılık.

Karahisar, T. (2011). Özel hayatın gizliliği ve internette işlenen suçlar. *II. Medya ve Etik Sempozyumu,* 1-9.

Kaya, Z. (2006). *Öğretim teknolojileri ve materyal geliştirme*. Ankara: Pegem A Yayıncılık.

Kayabaş, İ. (2016). Mobil teknolojiler. T.V. Yüzer ve M.E. Mutlu (Editörler), *Yeni iletişim teknolojileri* içinde (s. 100-133). Eskişehir: Anadolu Üniversitesi Basımevi.

Keser, A. (2005). Elektronik postanın örgütlerde kullanımı ve çalışanların elektronik posta kullanımlarına yönelik bir araştırma. *İş Güç Endüstri İlişkileri ve İnsan Kaynakları Dergisi*, 7 (1), 58-80.

Keskenler, M.F. ve Keskenler, E.F. (2017). Bulanık mantığın tarihi gelişimi. *Takvim-i Vekayi,* 5 (1), 1-10.

Kılıç, S. (2005). *Bilişim endüstrisinin elektronik doküman yönetimine yaklaşımı*. Yüksek Lisans Tezi. İstanbul: Marmara Üniversitesi, Türkiyat Araştırmaları Enstitüsü.

Kılıç, L. (2015). Durağan ve hareketli görüntünün öyküsü. T.F. Uçar (Editör), *Görsel kültür* içinde (s. 103-132). Ankara: Saray Matbaacılık.

Korkmaz, İ. (2017). *Kişisel verilerin ceza hukuku kapsamında korunması*. Ankara: Seçkin Yayıncılık.

Koskela, H. (2000). 'The gaze without eyes': video-surveillance and the changing nature of urban space. *Progress in Human Geography*, 24 (2), 243-265.

Kutup, N. (2010). İnternet ve sanat, yeni medya ve net.art. *12. Akademik Bilişim Konferansı*'nda sunulan bildiri. Muğla: Muğla Sıtkı Koçman Üniversitesi.

Küçük, A. ve Doğan, B. (2019). Türkiye'de 2017 anayasa değişikliği kapsamında yürütmenin asli düzenleme yetkisi ve mahfuz düzenleme alanı. *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, 9 (1), 1-60.

Küzeci, E. (2010). *Kişisel verilerin korunması*. Doktora Tezi. Ankara: Ankara Üniversitesi, Sosyal Bilimler Enstitüsü.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. ve Wolff, S. (2009). A brief history of the internet. *ACM SIGCOMM Computer Communication Review*, 39 (5), 22-31.

Lessig, L. (2006). *Code, version 2.0*. New York: Basic Books.

Lockwood, G. (2018). Workplace monitoring and surveillance: the british context. *Athens Law Journal*, 4 (3), 205-228.

Lyon, D. (1994). *The electronic eye*. United States: Polity Press.

Lyon, D. (2006). *Gözetlenen toplum* (Çev: G. Soykan). İstanbul: Kalkedon Yayıncılık.

Lyon, D. (2006). Gözetlenen toplum (Çev: G. Soykan). İstanbul: Kalkedon Yayıncılık'tan aktaran Bölükbaş, Ö.Ö. (2014). *İnsan hakları ve elektronik gözetim*. Yüksek Lisans Tezi. Konya: Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü.

Lyon, D. (2007). *Surveillance studies: an overview*. Cambridge: Polity Press.

Lyon, D. (2013). *Gözetim çalışmaları* (Çev: A. Toprak). İstanbul: Kalkedon Yayıncılık.

Martin, B. (1998). *Information liberation challenging the corruptions of information power*. London: Freedom Press.

Marx, K. (1992). *Capital: a critique of political economy volume one*. Middlesex: Penguin Classics.

Marx, G.T. (2015). Surveillance studies. *International Encyclopedia of the Social & Behavioral Sciences*, 2 (23), 733-741.

Mathis, R.L. ve Jackson, J.H. (2010). *Human resource management*. Ohio: South-Western College Pub.

Mattelart, A. (2012). *Gözetimin küreselleşmesi* (Çev: O. Gayretli ve S.U. Karacan). İstanbul: Kalkedon Yayıncılık.

Menekşe, N.Z., Kılıç, F., Akan, N.Y., Öcal, S., Ataoğlu, D., Tekil, E., Çakır, Ü., Penezoğlu, Y., Küçükkaya, M. ve Germeyan, B. (2001). *Değişim.tr: internetle gelişimde türkiye*. İstanbul: Türkiye İş Bankası Kültür Yayınları.

Mitchell, W. J. (1996). *City of bits*. Cambridge: The Mit Press.

Morar, F.S. (2014). Reinventing machines: the transmission history of the leibniz calculator. *The British Journal for the History of Science,* 48 (1), 123-146.

Moussa, M. (2015). Monitoring employee behavior through the use of technology and issues of employee privacy in america. *Sage Open,* 5 (2), 1-13.

Norris, C., McCahill, M. ve Wood, D. (2004). The growth of cctv: a global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance & Society,* 2 (2/3), 110-135.

Nurdoğan, A.K. (2018). Uluslararası çalışma örgütünün (uçö-ilo) yüzüncü yıl dönümü ve türkiye ilişkileri. *Bitlis Eren Üniversitesi Akademik İzdüşüm Dergisi,* 3 (4), 78-95.

Oğuz, H. (2013). Elektronik ortamda kişisel verilerin korunması, bazı ülke uygulamaları ve ülkemizdeki durum. *Uyuşmazlık Mahkemesi Dergisi,* 0 (3), 1-38.

Okur, Z. (2005). İşyerinde işçinin bilgisayar ve interneti özel amaçlı kullanımının iş ilişkisine etkisi. *Kamu-İş Dergisi,* 8 (2), 47-75.

Okur, Z. (2013). *İş hukukunda elektronik gözetleme*. İstanbul: Legal Kitabevi.

Önder, A.R. (1966). *Yasa dili sözlüğü*. Ankara: Türk Tarih Kurumu Basımevi.

Önok, M. (2013). Avrupa siber suçlar sözleşmesi ışığında siber suçlarla mücadelede uluslararası adli işbirliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,* 19 (2), 1229-1269.

Özbek, M. (2015). Avrupa siber suçlar sözleşmesinin türk ceza hukukuna etkileri. Article Letter.

Özçağlayan, M. ve Çelik, R. (2014). Sosyal medyada kendini ifade, teşhir ve gözetim: gözetimin sayısal bilgiyle dönüşümü nitel bir çalışma. *Dijital İletişim Etkisi Uluslararası Akademik Konferansı'nda* sunulan bildiri. İskenderiye, İstanbul.

Özdemir, H. (2010). İşyerinde işçilerin izlenmesi ve işçinin kişilik haklarının korunması. *Erzincan Üniversitesi Hukuk Fakültesi Dergisi,* 14 (1-2), 231-270.

Özger, Ö. (2017). Gözetim kavramının tarihsel gelişimi ve elektronik gözetim. *Siber Politikalar Dergisi,* 1 (1), 11-37.

Özön, N. (1981). *Sinema ve televizyon terimleri sözlüğü*. Ankara: Ankara Üniversitesi Basımevi.

Parlak, H. (2005). *İnternet ve türkiye'de internetin gelişimi*. Bitirme Ödevi. Elâzığ: Fırat Üniversitesi, Mühendislik Fakültesi.

Pearce, G. ve Platten, N. (1998). Achieving personal data protection in the european union. *Journal of Common Market Studies*, 36 (4), 529-547.

Pease-Watkin, C. (2003). Bentham's panopticon and dumont's panoptique. *UCL Bentham Project Journal of Bentham Studies*, 6 (1), 1-8.

Petersen, J. K. (2001). *Understanding surveillance Technologies: spy devices, their origins & applications*. Boca Raton: CRC Press LLC.

Pirim, H. (2006). Yapay zekâ. *Journal of Yaşar University*, 1 (1), 81-93.

Rodrigues, R.J., Wilson, P. ve Schanz, S.J. (2001). *The regulation of privacy and data protection in the use of electronic health information: an international perspective and reference source on regulatory and legal issues related to personal-identifiable health databases*. Washington: PAHO.

Rosenblum, M.F. (1990). The expanding scope of workplace security and employee privacy issues. *DePaul Business Law Journal*, 3 (77), 77-118.

Rubenstein, K.S. (2016). *Computer monitoring in the workplace: performance effects and perceptions*. Uzmanlık Tezi. New Jersey: Seton Hall University, The Department of Psychology.

Ryan, J. (2010). *A history of the internet and the digital future*. London: Reaktion Books.

Saka, E. (2019). Türkiye'de internet. E. Saka (Editör), *Yeni medya çalışmaları 5 türkiye internet tarihi* içinde (s. 4-72). İstanbul: Alternatif Bilişim Derneği.

Savaş, F.B. (2009). İş hukukunda "siber gözetim". *Çalışma ve Toplum Dergisi*, 3, 97-132.

Schermer, B.W. (2007). *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance*. Leiden: Leiden University Press.

Sencer, M. (1981). *Yöntembilim terimleri sözlüğü*. Ankara: Türk Dil Kurumu Yayınları.

Sevimli, K.A. (2006). *İşçinin özel yaşamına müdahalenin sınırları*. İstanbul: Legal Yayıncılık.

Sharp, V. (1996). *Computer education for teachers*. Iowa: Brown and Benchmark Publishers'dan aktaran İşman, A. (2001). Bilgisayar ve eğitim. Sakarya Üniversitesi Eğitim Fakültesi Dergisi, 2, 1-34.

Smith, M.J., Carayon, P., Sanders, K.J., Lim, S.Y. ve LeGrande, D. (1992). Employee stress and health complaints in jobs with and without electronic performance monitoring. *Applied Ergonomics*, 23 (1), 17-27.

Solove, D. J. (2004). *The digital person, technology and privacy in the information age*. New York: New York University Press.

Soysal, T. (2005). İnternet servis sağlayıcılarının hukuki sorumlulukları. *Türkiye Barolar Birliği Dergisi*, 61, 304-339.

Soysal, T. (2007). Elektronik posta yoluyla kişilik haklarına müdahaleden doğan hukuki sorumluluk. *Ankara Barosu Dergisi*, 65 (1), 144-167.

Soysal, A. (2009). İş yaşamında stres. *Çimento İşveren Dergisi*, 1, 17-40.

Sprague, R. (2010). Applying the electronic communications privacy act in the workplace: struggling to keep pace with paradigm shifts in technology. *SSRN Electronic Journal*, 1, 1-38.

Sproule, C.M. (2002). The effect of the usa patriot act on workplace privacy. *Cornell Hotel and Restaurant Administration Quarterly*, 43 (5), 65-73.

Staples, W.G. (2007). *Encyclopedia of privacy, volumes 1&2*. London: Greenwood Press.

Süzek, S. (2008). *İş hukuku*. İstanbul: Beta Yayıncılık.

Şan-Aslan, P. (2019). Fotoğraf ve sanat etkileşimi. *Ulakbilge Sosyal Bilimler Dergisi*, 7 (32), 53-61.

Şimşek, O. (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması*. İstanbul: Beta Yayıncılık.

Tabak, U. ve Konukpay, C. (2018). Güncel uluslararası içtihatlar çerçevesinde işyerinde izleme uygulamaları ve özel yaşamın korunması. *Suç ve Ceza Ceza Hukuku Dergisi*, 1, 115-172.

T.C. Millî Eğitim Bakanlığı. (2012). *Grafik ve fotoğraf: pinhole (iğne deliği) kamera*. Ankara.

Tebano, L. (2017). Employees' privacy and employers' control between the italian legal system and european sources. *Labour & Law Issues*, 3 (2), 1-20.

Tekeli, H. (1994). *Bilgi çağı*. İstanbul: Simavi Yayınları'ndan aktaran Erkan, H. (2015). Yeni iletişim ve bilişim teknolojilerinin ortaya çıkışı. V. Canbey – Özgüler (Editör), Yeni teknolojiler ve çalışma hayatı içinde (s. 2-39). Eskişehir: Anadolu Üniversitesi Açıköğretim Yayınları.

Tekergül, M. (2010). *İşyerinde elektronik gözetim uygulamaları*. Yüksek Lisans Tezi. İstanbul: Kadir Has Üniversitesi, Sosyal Bilimler Enstitüsü.

TMMOB Elektrik Mühendisleri Odası. (2009). *Elektronik gözaltı dünyası. İletişim Özgürlüğüne Müdahale Raporu*. Ankara: TMMOB Elektrik Mühendisleri Odası.

Tremblay, M. (2010). *Cyber-surveillance*. Encyclopedic Dictionary of Public Administration.

Turan, E. (2011). Fotoğraf: belleği olan ayna. *Sanat-Tasarım Dergisi,* 1 (2), 19-24.

Turhan, M. (2010). *Siber güvenliğin sağlanması, dünya uygulamaları ve ülkemiz için çözüm önerileri*. Uzmanlık Tezi. Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Tükel, İ. (2012). Modern örgütlerde yabancılaşma ve kafka'nın "dönüşüm" romanının bu bağlamda analizi. *Dokuz Eylül Üniversitesi Edebiyat Fakültesi Dergisi,* 1 (2), 34-50.

Türkel, N. (2010). *Özel Hayatın Gizliliğini İhlal Suçu.* Yüksek Lisans Tezi. İzmir: Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü.

Uçar, Ö., Uçar, T.F., Kılıç, L., Orhon, N. ve Taşçıoğlu, M. (2015). *Görsel kültür*. Ankara: Saray Matbaacılık.

Uncular, S. (2012). *İş ilişkisinde işçinin kişisel verilerinin korunması*. Yüksek Lisans Tezi. İstanbul: Galatasaray Üniversitesi, Sosyal Bilimler Enstitüsü.

Uncular, S. (2014). *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*. Ankara: Seçkin Yayıncılık.

Uzgören, E. (1999). Bilgi toplumunda uluslararası rekabetedebilirlik avantajının yaratılmasına yönelik stratejik yaklaşım: devingen yaratıcılık (innovation). *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi,* 1, 165-176.

Varol, A. ve Baştürk, İ. (2015). Hukuki ve teknik boyutuyla elektronik tebligat ile kayıtlı elektronik posta sistemi. *Ankara Barosu Dergisi,* 1, 263-278.

Yaşa, S. (2016). *Bilgi ve iletişim teknolojileri sektöründe girişim sermayesi uygulamaları*, Bilgi Toplumu Dairesi Başkanlığı.

Yılmaz, F. (2015). *Türkiye'deki bilişim suçlarının sosyolojik bir analizi: tehditler ve çözüm stratejileri*. Yüksek Lisans Tezi. Eskişehir: Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü.

Yılmaz, G. (2005). Elektronik performans izleme sistemlerinin çalışanlar ve işletmeler üzerindeki etkileri. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 4 (7), 1-19.

Yiğit, E. (2013). *İşyerinde internet ve e-posta kullanımının izlenmesi ve gözetlenmesi*. Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü.

Vorvoreanu, M. ve Botan, C.H. (2000). Examining electronic surveillance in the workplace: a review of theoretical perspectives and research findings. *Annual International Communication Association Conference*, s. 1-32. Acapulco, Mexico.

Walby, K. (2005). Open-street camera surveillance and governance in canada. *Canadian Journal of Criminology and Criminal Justice*, 47 (4), 655-684.

Watson, N. (2001). The private workplace and the proposed "notice of electronic monitoring act": is "notice" enough? *Federal Communications Law Journal*, 54 (1), 79-102.

Watt, J.R. (2009). *Electronic workplace surveillance and employee privacy – a comparative analysis of privacy protection in avustralia and the united states*. Yüksek Lisans Tezi. Brisbane: Queensland University of Technology, Faculty of Law.

Weatherall, Josephine A.C. ve Haskey, J.C. (1976). Surveillance of malformations. *British Medical Bulletin*, 2 (1), 39-44.

Weckert, J. (2005). *Electronic monitoring in the workplace*. Hershey, Pa.: IGI Global.

Werrett, S. (1999). Potemkin and the panopticon: samuel bentham and the architecture of absolutism in eighteenth century russia. *UCL Bentham Project Journal of Bentham Studies*, 2 (1), 1-25.

Whitaker, R. (1999). *The end of privacy*. New York: The New Press.

Zuboff, S. (1988). In the age of the smart machine: the future of work and power. New York: Basic Books'dan aktaran Lyon, D. (1994). *The electronic eye*. United States: Polity Press.

Zureik, E. (2003). Theorizing surveillance: the case of the workplace. D. Lyon (Editörler), *Surveillance as Social Sorting* içinde (s. 31-57). New York: Routledge.

http-1: https://dictionary.cambridge.org/ (Erişim tarihi: 31.09.2018).

http-2: http://www.tdk.gov.tr/ (Erişim tarihi: 01.10.2018).

http-3: http://www.moment-expo.com/bilgisayarlardan-once-hesap-yapan-makineler (Erişim tarihi: 05.10.2018).

http-4: http://www.uralakbulut.com.tr/wp-content/uploads/2012/12/babbage.pdf (Erişim tarihi: 07.10.2018).

http-5: https://atabilgisayardonanim.files.wordpress.com/2011/10/bilgisayar-ve-bilgisayarin-tarihcesi2.pdf (Erişim tarihi: 07.10.2018).

http-6: http://www.madran.net/wp-content/uploads/2013/09/btu100_1_ek_bilgisayarin_tarihcesi.pdf (Erişim tarihi: 07.10.2018).

http-7: https://www.teknonce.com/super-bilgisayar-nedirne-ise-yarar.html (Erişim tarihi: 07.10.2018).

http-8: https://tr.wikipedia.org/wiki/Merkez%C3%AE_i%C5%9Flem_birimi (Erişim tarihi: 10.10.2018).

http-9: https://en.wikipedia.org/wiki/PDP-8 (Erişim tarihi: 11.10.2018).

http-10: https://tr.wiktionary.org/wiki/manyetik_disk (Erişim tarihi: 12.10.2018).

http-11: https://tr.wikipedia.org/wiki/Intel_4004 (Erişim tarihi: 12.10.2018).

http-12: https://tr.wikipedia.org/wiki/Moore_yasas%C4%B1 (Erişim tarihi: 13.10.2018).

http-13: https://igotoffer.com/apple/apple-ii (Erişim tarihi: 13.10.2018).

http-14: https://www.muhendisbeyinler.net/yapay-zeka-ve-bulanik-mantik-nedir/ (Erişim tarihi: 13.10.2018).

http-15: http://temelag.blogspot.com/2012/10/protokol-nedir.html (Erişim tarihi: 13.10.2018).

http-16: https://www.karel.com.tr/bilgi/tcp-ip-nedir-nasil-calisir (Erişim tarihi: 14.10.2018).

http-17: https://dralabay.wordpress.com/2014/08/29/web-teknolojilerinin-gelisimi-ve-hayatimiza-etkileri/ (Erişim tarihi: 15.10.2018).

http-18: https://www.bilimcag.com/nedir/web-1-0-2-0-3-0-nedirfarklari-nelerdir/ (Erişim tarihi: 15.10.2018).

http-19: https://tr.wikipedia.org/wiki/E-Devlet_(T%C3%BCrkiye) (Erişim tarihi: 17.10.2018).

http-20: https://masivaturk.com/turkiyede-internetin-tarihi-ve-gelisimi (Erişim tarihi: 17.10.2018).

http-21: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates (Erişim tarihi: 18.10.2018).

http-22: https://finance.yahoo.com/news/the-first-ever-email--the-first-tweet--and-12-other-famous-internet-firsts-181209886.html (Erişim tarihi: 20.10.2018).

http-23: http://sozluk.gov.tr/ (Erişim tarihi: 21.10.2018).

http-24: https://yordama.com/kameranin-tarihcesi/ (Erişim tarihi: 22.10.2018).

http-25: https://ncc.metu.edu.tr/sites/default/files/Bilim-teknoloji-merkezi-deneyler.pdf (Erişim tarihi: 22.10.2018).

http-26: http://www.birkarefotograf.com/dijital-fotograf-makinelerinin-dogusu/ (Erişim tarihi: 22.10.2018).

http-27: http://bestdergisi.com.tr/arsiv-eski/kuresel-cctv-pazar-analizi/ (Erişim tarihi: 23.10.2018).

http-28: http://sozluk.gov.tr/ (Erişim tarihi: 23.10.2018).

http-29: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates (Erişim tarihi: 23.10.2018).

http-30: https://www.amanet.org/articles/the-latest-on-workplace-monitoring-and-surveillance/ (Erişim tarihi: 24.10.2018).

http-31: https://www.forbes.com/sites/cherylsnappconner/2015/07/31/wasting-time-at-work-the-epidemic-continues/#224ef231d942 (Erişim tarihi: 25.10.2018).

http-32: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN (Erişim tarihi: 26.10.2018).

http-33: https://www.ekodialog.com/ekonomi_kurumlari/iktisadi_kalkinma_orgutu.html (Erişim tarihi: 27.10.2018).

http-34: http://disiliskiler.kulturturizm.gov.tr/TR-22153/ekonomik-isbirligi-ve-kalkinma-orgutu-oecd.html (Erişim tarihi: 27.10.2018).

http-35: http://www.mfa.gov.tr/iktisadi-isbirligi_ve-gelisme-teskilati-_oecd_.tr.mfa (Erişim tarihi: 27.10.2018).

http-36: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (Erişim tarihi: 27.10.2018).

http-37: http://www.oecd.org/internet/ieconomy/declarationontransborderdataflows.htm (Erişim tarihi: 05.11.2018).

http-38: https://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm (Erişim tarihi: 05.11.2018).

http-39: http://www.oecd.org/sti/ieconomy/1840065.pdf (Erişim tarihi: 05.11.2018).

http-40: http://www.oecd.org/internet/ieconomy/oecdprivacystatementgenerator.htm (Erişim tarihi: 05.11.2018).

http-41: http://www.oecd.org/sti/ieconomy/32493366.PDF (Erişim tarihi: 25.11.2018).

http-42: https://www.un.org/en/charter-united-nations/index.html (Erişim tarihi: 30.11.2018).

http-43: https://www.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d22/c016/tbmm22016089ss0150.pdf (Erişim tarihi: 01.12.2018).

http-44: https://www.refworld.org/pdfid/3ddcafaac.pdf (Erişim tarihi: 02.12.2018).

http-45: https://www.ilo.org/ankara/about-us/WCMS_372874/lang--tr/index.htm (Erişim tarihi: 03.12.2018).

http-46: https://www.ilo.org/ankara/about-us/WCMS_372872/lang--tr/index.htm (Erişim tarihi: 03.12.2018).

http-47: https://www.ilo.org/dyn/normlex/en/f?p=1000:11200:0::NO:11200:P11200_COUNTRY_ID:102893 (Erişim tarihi: 04.12.2018).

http-48: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf (Erişim tarihi: 04.12.2018).

http-49: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=kyl1NFgc (Erişim tarihi: 05.12.2018).

http-50: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=TqaZ6za9 (Erişim tarihi: 05.12.2018).

http-51: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Erişim tarihi: 06.12.2018).

http-52: http://disiliskiler.kulturturizm.gov.tr/TR-127495/avrupa-birligi.html (Erişim tarihi: 07.12.2018).

http-53: https://europa.eu/european-union/about-eu/eu-in-brief_en (Erişim tarihi: 08.12.2018).

http-54: https://tr.wikipedia.org/wiki/Lizbon_Antla%C5%9Fmas%C4%B1 (Erişim tarihi: 10.12.2018).

http-55: https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf (Erişim tarihi: 17.12.2018).

http-56: https://iclg.com/practice-areas/data-protection-laws-and-regulations/germany (Erişim tarihi: 03.01.2019).

http-57: https://www.garanteprivacy.it/web/guest/home_en/italian-legislation (Erişim tarihi: 05.01.2019).

http-58: https://iclg.com/practice-areas/data-protection-laws-and-regulations/italy (Erişim tarihi: 06.01.2019).

http-59: https://www.law.cornell.edu/wex/fourth_amendment (Erişim tarihi: 10.01.2019).

http-60: https://withoutmyconsent.org/50state/234521616 (Erişim tarihi: 20.01.2019).

http-61: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 (Erişim tarihi: 21.01.2019).

http-62: https://www.law.cornell.edu/uscode/text/18/2701 (Erişim tarihi: 22.01.2019).

http-63: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (Erişim tarihi: 02.02.2019).

http-64: https://www.pdpjournals.com/docs/99007.pdf (Erişim tarihi: 02.02.2019).

http-65: https://justice.org.uk/regulation-investigatory-powers-act-2000/ (Erişim tarihi: 02.02.2019).

http-66: http://www.slaughterandmay.com/media/39127/controlling_employee_electronic_communications.pdf (Erişim Tarihi: 05.02.2019).

http-67: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf (Erişim tarihi: 05.02.2019).

http-68: https://www.gov.uk/government/publications/data-protection-law-eu-exit/amendments-to-uk-data-protection-law-in-the-event-the-uk-leaves-the-eu-without-a-deal-on-29-march-2019 (Erişim tarihi: 10.02.2019).

http-69: https://en.wikipedia.org/wiki/Data_Protection_Act_2018 (Erişim tarihi: 10.02.2019).

http-70: http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.16405&MevzuatIliski=0 (Erişim tarihi: 12.02.2019).

http-71: https://tr.wikipedia.org/wiki/Ceza_Muhakemesi_Kanunu (Erişim Tarihi: 15.02.2019).