

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

**BİLİŞİM ÇAĞINDA TOPLU GÖZETİM VE
YASAL MEVZUAT DÜZENLEMELERİ**

YÜKSEK LİSANS TEZİ

İsmail Cem BAKIR

Bilişim Uygulamaları Anabilim Dalı

Bilgi ve Haberleşme Mühendisliği Programı

Tez Danışmanı: Dr. Öğr. Üyesi Çiçek ERSOY

MART 2020

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

**BİLİŞİM ÇAĞINDA TOPLU GÖZETİM VE
YASAL MEVZUAT DÜZENLEMELERİ**

YÜKSEK LİSANS TEZİ

**İsmail Cem BAKIR
(708141008)**

Bilişim Uygulamaları Anabilim Dalı

Bilgi ve Haberleşme Mühendisliği Programı

Tez Danışmanı: Dr. Öğr. Üyesi Çiçek ERSOY

MART 2020

İTÜ, Bilişim Enstitüsü'nün 708141008 numaralı Yüksek Lisans Öğrencisi İsmail Cem BAKIR, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı “BİLİŞİM ÇAĞINDA TOPLU GÖZETİM VE YASAL MEVZUAT DÜZENLEMELERİ” başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı : **Dr. Öğr. Üyesi Çiçek ERSOY**
İstanbul Teknik Üniversitesi

Jüri Üyeleri : **Prof. Dr. Mustafa Aksu**
İstanbul Üniversitesi

Dr. Öğr. Üyesi. Sebahattin Eker
İstanbul Teknik Üniversitesi

Teslim Tarihi :
Savunma Tarihi :





Özgür günlere,



ÖNSÖZ

Bu çalışmada geçmişten beri gündemde olan fakat algoritmaların, yazılımın ve teknolojik kapasitenin büyük bir hızla gelişmesiyle gündelik hayatımızın bir parçası haline gelen ve toplanan verinin büyüklüğü ile artan, makine öğrenmesi ve yapay zeka ile kolaylaşan toplu gözetimi, felsefi altyapısını ve uygulamaları incelenmiştir. Özel hayatın gizliliğini, mahremiyeti, kişisel verilerini korumak ve bu gözetim düzenine bir sınır çekebilmek için insanlar hala hukukun gölgesine sığınmaktadır. Bu nedenle hukuki uyumsuzlıklara ve tartışmalara konu olan durumlar, Türkiye’de ve yurtdışında yapılan düzenlemeler ve gözetim bağlamında bireyin devlet karşısındaki konumu bu tezin bir parçası haline getirilmiştir.

Tezin teknolojinin bu baş döndürücü hızına yetişmekte zorlanan hukuk dünyasıyla, mevzuat konusunda gelişmiş bir bilgi birikimine ve duyarlılığa sahip olmadığını söyleyebileceğimiz yazılım dünyası arasındanaçizane bir köprü olarak görü lmesi bana mutluluk verecektir.

Bu çalışmayı yaparken her daim bana yol gösteren ve sürekli yanımda olan, onunla çalışmaktan büyük mutluluk duyduğum sayın hocam Dr. Öğr. Üyesi Çiçek ERSOY’a teşekkürlerimi sunarım.

Bugünlere gelmemdeki en büyük pay sahibi, emeklerinin karşılığını hayatım boyunca ödeyemeyeceğim, bu tezi ona armağan ederek bir nebze mutlu edeceğime inandığım çok sevdiğim anneme sonsuz teşekkürler ederim.

Mart 2020

İsmail Cem Bakır
Bilgisayar Mühendisi



İÇİNDEKİLER

ÖNSÖZ.....	vii
İÇİNDEKİLER	ix
KISALTMALAR.....	xi
ŞEKİL LİSTESİ	xiii
ÖZET.....	xv
SUMMARY	xvii
1. GİRİŞ.....	1
1.1 Akışkan Gözetim.....	4
1.2 Panaptikon Uygulamaları.....	5
1.3 Covid-19 Ve Toplu Gözetim.....	9
1.3.1 Hayat eve sığar mobil uygulaması.....	12
2. GÜVENLİK Mİ ÖZGÜRLÜK MÜ?	13
2.1 İnternetin Tarihi	13
2.1.1 İnterneti kim kontrol ediyor?.....	15
2.1.2 Temel bir insan hakkı olarak internet.....	17
2.2 Özel Hayatın Gizliliği	19
2.2.1 Ömek davaları.....	20
2.3 Türkiye’de Gözetim Uygulamaları ve Hak İhlalleri.....	24
2.4 Hukuki Çerçeve.....	27
2.4.1 Avrupa insan hakları sözleşmesi’nde özel hayatın gizliliği	28
2.4.2 Anayasamızda özel hayatın gizliliği.....	29
2.4.3 Türk hukukunda durum.....	30
3. PIPA, SOPA, ACTA, CISPA GÖZETİM VE SANSÜR KISKACINDA	
İNTERNET.....	33
3.1 PIPA (Protect Intellectual Property Act – Fikir Eserlerinin Mülkiyetinin	
Korunması Yasası).....	33
3.2 SOPA (Stop Online Piracy Act – Çevrimiçi Korsanlığı Durdurma Yasası) ...	34
3.3 ACTA(Anti Counter-Feiting Trade Aggrement – Sahteciliğe Karşı Ticaret	
Anlaşması).....	37
3.4 CISPA (Cyber Intelligence Sharing Protection Arc – Siber İstihbarat Paylaşımı	
ve Korunması Yasası)	38
4. SONUÇ	41
KAYNAKLAR.....	43
ÖZGEÇMİŞ	53

KISALTMALAR

İHA	: İnsansız Hava Aracı
IP	: İnternet Protokol
TCP	: Transmission Control Protocol
TT	: Trendy Topic





ŞEKİL LİSTESİ

Sayfa

Şekil 1.1 : Bentham'ın Panaptikon tasarımı.....	1
Şekil 1.2 : Diktatör Modelo tarafından 1926 yılında Küba'da inşa ettirilmiş bir Panaptikon hapishanesi	2
Şekil 1.3 : Ükelere göre 16-24 yaş aralığında aktif olarak sosyal medya kullanan genç nüfusun oranı	4
Şekil 1.4 : DeepFace Facebook'un yüz tanıma yazılımı.....	5
Şekil 1.5 : AnyVision'a ait yüz tanıma sistemi taraftarların tüm vücudunu tarayarak, maçlara biletsiz girebilmelerini sağlıyor	9
Şekil 2.2 : İnterneti Oluşturan Ağlar	12
Şekil 2.3 : İnternetin Yaratıcısı	13
Şekil 2.4 : Dünya Popülasyonunun İnternete Erişim Haritası	15
Şekil 2.5 : Hızlı İnternete Erişen İnsan Popülasyonu Yüzdesi	16
Şekil 2.6 : 2007-2018 Yılları Arası Erişime Engellenen Alan Adı Sayıları.....	22
Şekil 2.7 : Erişime Engellenen Web Sitelerinin Karar Veren Kurumlara Göre Dağılımı	23
Şekil 2.8 : 2012-2018 Twitter Şeffaflık Raporlarında Mahkeme Kararları Ve Diğer Çıkartma Talepleri	24
Şekil 2.9: 2012-2018 Twitter Raporlarında Çıkartılması Talep Edilen ve Çıkartılan Hesap Sayıları	24



BİLİŞİM ÇAĞINDA TOPLU GÖZETİM VE YASAL MEVZUAT DÜZENLEMELERİ

ÖZET

Gözetleme iktidarlar için geçmişten günümüze toplumları kontrol etmenin bir aracı olmuştur. Bir cezaevi tasarımı olarak ortaya çıkan panoptik gözetleme sistemlerinde görünmez bir gardiyan mahkumları izlerken, gözetlendiğini bilen mahkumlar otokontrol mekanizması geliştirmekte ve kendi davranışlarını kontrol etmeye başlamaktadır. Devletler de kitleleri toplu olarak gözetlerken, gözetlendiğini bilen toplumlar çizilen sınırların dışına çıkmayan, itiraz yerine itaat eden bir tebaaya dönüşmektedirler. Fakat her zaman bir gözetleyiciye ihtiyaç duyan bu maliyetli ve katı sistemlerin yerini giderek daha esnek ve akışkan gözetim sistemleri almaktadır. Zorlama yerine eğlence ve ödül vaat eden akışkan gözetim mekanizması ile, toplumlar her an ve her yerde gözetlenmeye başlamıştır. İnternet siteleri, cep telefonu uygulamaları, sosyal medya, akıllı evler ve internete bağlanabilen eşyalar, yüz tanıma sistemleri insanların gözetlenebilmesi için gerekli teknolojik altyapıyı sağlamaktadır. Üstelik sosyal medyada beğenilme arzusu ve göz önünde olma isteği, iş hayatında terfi ve ödül sisteminden pay kapma yarışı, günlük yaşamda güvenlik kaygıları sayesinde, akışkan gözetim kişilerin gözetim sistemine rızasını üretebilmektedir.

Teknoloji devleri daha fazla kar elde etmek için gözetim tabanlı iş modelini kullanmaktadır. Bu modele göre kişisel verilerimiz şirketler tarafından toplanmakta, saklanmakta ve işlenmektedir. Daha sonra bu veriler ile yapay zeka algoritmaları eğitilmektedir. Yapay zeka algoritmaları ticari amaçla müşteri profilinin çıkarılmasında, reklam servislerinin geliştirilmesinde ve hatta seçmen tercihlerinin değiştirilmesi için kullanılmaktadır. Gözetlenen birey bu iş modelinde ürünün kendisi haline gelmektedir.

Toplu gözetim sadece ticari amaçla şirketler tarafından yapılmamaktadır. Devletler insanları daha fazla kontrol altında tutmak, kategorize etmek ve kendi tanımlarına göre tehlikeli grupları fişlemek için gözetleme sistemlerini kullanmaktalar. Muhalif sosyal medya paylaşımlarının izlenmesi, böcek boyutlarındaki insansız hava araçlarının kullanılmaya başlanması, kamusal alanlarda insanları izleyen yüz tanıma sistemleri iktidarlar için gerekli verileri sağlamaktadır. Bu gözetim sistemleri azınlık grupların daha fazla ayrımcılığa uğramasına, insanların kişisel verilerinin izinsiz olarak toplanmasına ve özel hayatının gizliliğinin ihlal edilmesine neden olmaktadır.

Teknolojinin gelişmesine paralel olarak devletlerin vatandaşlarını gözetleme kapasitesinin artması, dinlenen ve izlenen kişi sayısında büyük bir artışa ve özel hayatının gizliliğinin çok daha sık şekilde ihlal edilmesine yol açmıştır. Bu ihlallerin önüne geçmek ve yurttaşların özel hayatlarının gizliliğini korumak için yasalarda yer alan bazı maddeler vardır. Avrupa İnsan Hakları Sözleşmesinin 8. maddesinde şu ilke yer almaktadır: “Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.”. Benzer şekilde anayasamızda özel yaşamın gizliliğine

hak olarak yer verilmiş ve düzenlenmiştir. Anayasamızın 20. maddesine göre “Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.”.

Gözetimin yanında devletin toplumu kontrol altında tutabilmesinin bir diğer yolu sansürdür. Türkiye’de erişime engellenen sitelerin sayısında son yıllarda yaşanan artış, Twitter ve Wikipedia’ya uygulanan sansür bu örnekler arasındadır. Türkiye’de 2018 yılı sonu itibarıyla 245.825 web sitesi ve alan adına erişimin engellendiği tespit edilmiştir. Yine interneti kontrol altına alma amacıyla ABD’de çıkarılan ve senatodan geçirilmeye çalışılan yasa tasarıları, web sitelerini sansürleme ve gerektiğinde engelleme olanağı getirmektedir. Bu yasa tasarıları toplumsal muhalefetin karşı mücadelesi sayesinde yasalaşamamıştır.

Sonuç olarak hem devletler hem şirketler eliyle yapılan toplu gözetim ile kişisel verilerimiz toplanmakta, birçok örnekte özel yaşamın gizliliği ihlal edilmektedir. Yine sansür ve yasaklarla toplumlar kontrol altında tutulmaya çalışılmaktadır. Bu sürecin aktif bir parçası olmanın ve gerektiğinde itirazlarımızı dile getirebilmenin yolu gözetim sistemlerinin nasıl işlediğini, hangi alanlarda ve hangi teknolojilerle hayata geçirildiğini anlamaktan ve yurttaş olarak mevzuatlarda yer alan haklarımızı bilmekten geçmektedir.

MASS SURVEILLANCE AND LEGISLATION ARRANGEMENTS IN THE INFORMATION AGE

SUMMARY

Surveillance has been a tool for governments to control societies from past to present. In panoptic surveillance systems that have emerged as prison design, an invisible prison officer watch prisoners knowing that they are being watched, develop auto control mechanisms, and begin to control their own behavior. While the states are watching the masses as a whole, the societies knowing that they are being watched become a subject who does not go beyond the drawn borders and obey instead of objection. But these costly and rigid systems, which always need a watchdog, are being replaced by more flexible and fluid surveillance systems. With the fluid surveillance mechanism that promises entertainment and reward instead of coercion, societies are being monitored at any time and anywhere. Internet sites, mobile phone applications, social media, smart homes, and articles that can be connected to the internet, face recognition systems provide the necessary technological infrastructure for people to be observed. Moreover, thanks to the desire to be liked and to be considered in social media, the race to get a share from the promotion and reward system in business life, and security concerns in daily life, fluid surveillance can produce people's consent to the surveillance system.

Technology giants use the surveillance-based business model to make more profit. According to this model, our personal data is collected, stored, and processed by companies. Then, artificial intelligence algorithms are trained with this data. Artificial intelligence algorithms are used for commercial purposes in the profile of the customer, in the development of advertising services, and even in changing voter preferences. The individual becomes the product itself in this business model.

Mass surveillance is not only carried out by companies for commercial purposes. States use surveillance systems to keep people more under control, categorize them, and blacklisting dangerous groups according to their own definition. The monitoring of opposition social media posts, the use of insect drones, facial recognition systems that monitor people in public spaces provide the necessary data for the rulers. These surveillance systems lead to greater discrimination of minority groups, the unauthorized collection of people's personal data, and a violation of their privacy.

The right to privacy, which was put forward in 1890 with the article "The Right to have privacy" written by Samuel Warren together with Louis D. Brandeis, has been the subject of many cases until now. It has been observed that there are disagreements between individuals and between individuals and government institutions, and in many cases, the right to privacy is violated. In parallel with the development of technology, the increase in the capacity of the states to watch over their citizens has led to a large increase in the number of people listened and watched, and a much more frequent violation of the right to privacy. There are some articles in the law to prevent these

violations and protect the privacy of citizens' private lives. "Unless there exists a decision duly given by a judge on one or several of the grounds of national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there exists a written order of an agency authorized by law, in cases where delay is prejudicial, again on the above-mentioned grounds, neither the person, nor the private papers, nor belongings of an individual shall be searched nor shall they be seized. The decision of the competent authority shall be submitted for the approval of the judge having jurisdiction within twenty-four hours. The judge shall announce his decision within forty-eight hours from the time of seizure; otherwise, seizure shall automatically be lifted."

Similarly, the right to privacy is included and regulated in our constitution. According to Article 20 of the Constitution, "Everyone has the right to demand respect for his / her private and family life. Privacy of private or family life shall not be violated." Situations, where the confidentiality of private life will be restricted, are subject to conditions such as national security, public interest, crime prevention and are included in the constitution as follows:

"Unless there exists a decision duly given by a judge on one or several of the grounds of national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there exists a written order of an agency authorized by law, in cases where delay is prejudicial, again on the above-mentioned grounds, neither the person, nor the private papers, nor belongings of an individual shall be searched nor shall they be seized. The decision of the competent authority shall be submitted for the approval of the judge having jurisdiction within twenty-four hours. The judge shall announce his decision within forty-eight hours from the time of seizure; otherwise, seizure shall automatically be lifted."

Except in constitutional article governing the right of privacy in Turkey, studies, regulations and issued laws in information technology law field are: Relevant Articles in the Turkish Penal Code (5237), relevant articles of the Criminal Procedure Code (5271), Law on Intellectual and Artistic Works (5846), Electronic Signature Law (5070), Law on Regulating of Publications on the Internet and Combating Crimes Committed By Means of Such Publication (5651), Personal Data Protection Law (6698).

Besides surveillance, another way for the state to keep society under control is censorship. The increase in recent years in the number of access blocked web sites in Turkey, censorship of Twitter and Wikipedia are among the examples. By the end of 2018 in Turkey, it was determined that 245.825 websites and domain name access are denied. According to data published by Twitter and is located in the Transparency Report, covering the period 2012-2018, 5099 decision to remove the content in the courts, with 1,979 blocked accounts Turkey is located on the world-leading position on this category. Again, draft laws issued in the USA to control the internet and tried to be passed through the senate provide the opportunity to censor and block websites when necessary. These draft laws could not be enacted thanks to the struggle of the public opposition.

As a result, our personal data is collected through mass surveillance by both states and companies, and in many instances, the privacy of life is violated. Societies are tried to be kept under control with censorship and bans. The way to be an active part of this process and to express our objections when necessary is through understanding how

surveillance systems work, in what areas and with what technologies, and knowing our rights as a citizen in the legislation.



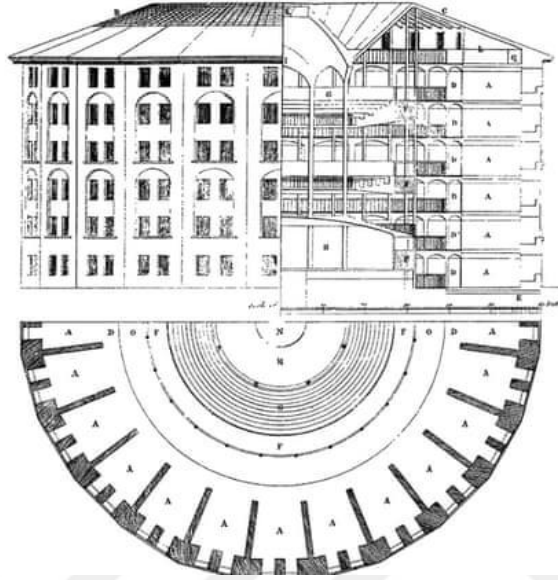


1. GİRİŞ

Katı ve sabit olagelmiş, duvarlara, sınırlara ve gözcülere ihtiyaç duyan gözetim günümüzde esnekleşmiş toplumsal hayata nüfuz etmiştir.

George Orwell ünlü romanı 1984'te totaliterleşen devlet yönetimlerini ve iktidarın vatandaşlarının günlük yaşamlarını Büyük Birader(Big Brother) uygulamalarıyla nasıl daha fazla kontrol altına aldığını anlatır. Bu tasarı günümüz toplumları için bir uyarı niteliği taşımaktadır. Panoptikon kavramı ise İngiliz hapishane reformcusu Jeremy Bentham tarafından üretilmiştir. Yunanca pan ve optikon kelimelerinden türetilmiştir ve her yeri gören yer anlamına gelmektedir (Dereli, 2015) . Michel Foucault, 1975 yılında yazdığı “Hapishanenin Doğuşu” adlı kitabında panaptikonu iktidar mekanizmasıyla özdeşleştirir (Elektrik Mühendisleri Odası, 2006, s.3) . Foucault yaptığı incelemede panoptikonu yalnızca bir hapishane modeli olmaktan çıkarır, felsefenin, toplumsal yaşamın ve iktidarın bir konusu haline getirir. Foucault panaptikonu şu şekilde değerlendirir. “Çevrede halka halinde bir bina, merkezde bir kule; bu kulenin halkanın iç cephesine bakan geniş pencereleri vardır. Çevre bina hücrelere bölünmüştür; bunlardan her biri binanın tüm kalınlığını kat etmektedir. Bunların biri içeri bakan ve kuleninkilere karşı gelen, diğer de dışarı bakan ve ışığın hücreye girmesine olanak veren ikişer pencereleri vardır. Bu durumda merkezi kulede tek bir gözetmen ve her bir hücreye tek bir deli, bir hasta, bir mahkûm, bir işçi veya bir ilkokul çocuğu kapatmak yeterlidir. Geriden gelen ışık sayesinde, çevre binaların içindeki küçük silüetleri olduğu gibi kavramak mümkündür. Ne kadar kafes varsa, o kadar küçük tiyatro vardır, bu tiyatrolarda her oyuncu tek başınadır, tamamen bireyselleşmiştir ve sürekli olarak görülebilir durumdadır. Görülmeden gözetim altında tutmaya olanak veren düzenleme, sürekli görmeye ve hemen tanımaya olanak veren mekânsal birimler oluşturmaktadır. Sonuç olarak, hücre ilkesi tersine döndürülmekte veya daha doğrusu onun üç işlevi kapatmak, ışıktan yoksun bırakmak ve saklamak- ters yüz edilmektedir; bunlardan yalnızca birincisi korunmakta ve diğer ikisi kaldırılmaktadır. Tam ışık altında olma ve bir gözetmenin bakışı, aslında koruyucu olan karanlıktan daha fazla yakalayıcıdır.” (Foucault, 1992, s. 251).

Merkezdeki otorite tüm hücreleri gözetlerken, gözetleyenler hiçbir zaman görünmez. Bu tek yönlü gözetleme sisteminde mahkumlar gardiyanları göremediği için her an gözetleniyormuş gibi hissetmekte, bir otokontrol mekanizması ile otoritenin sözünden çıkmayan tebaaya dönüşmektedir. Jeremy Bentham tarafından tasarlanan hapishane mimarisi Şekil 1.1’de görülmektedir. Şekil 1.2’de ise panaptikon modeli baz alınarak Küba’da inşa edilmiş gerçek bir hapishane binası gösterilmektedir.



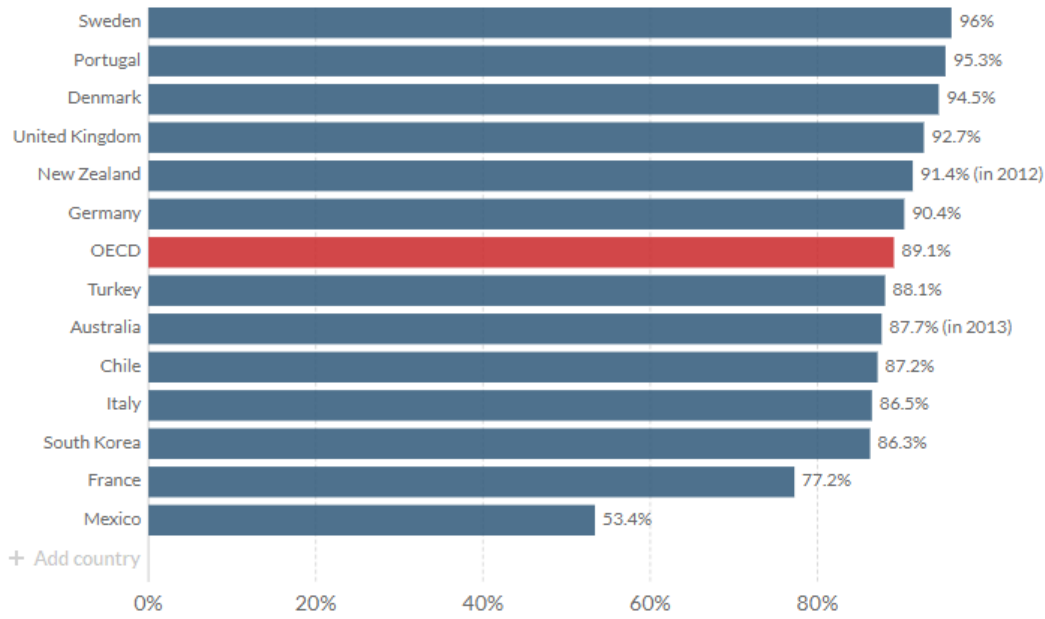
Şekil 1.1: Bentham’ın Panaptikon tasarımı (McMullan, 2017).



Şekil 1.2: Diktatör Modelo tarafından 1926 yılında Küba’da inşa ettirilmiş bir Panaptikon hapishanesi (McMullan, 2017).

Bauman'a göre günümüzün panaptikon sonrası dünyasında mahkumlar ve gardiyanların bağılılığı sona ermiştir. Çevrimiçi dünyada kullandığımız araçlar bir gözetleyiciye ihtiyaç bırakmaksızın bizi gözetlenen objeler haline dönüştürmüştür (Bauman, 2000, s.11) . Panaptikon yanındaki diğer gözetleme ve kontrol türleri esneklik ve eğlence sağlayarak kişilerin rızalarıyla gözetim yöntemlerini kabul etmesine fırsat vermektedir. Zorlama yerini ayartılan insana bırakıyor. Tehdit edilen, korkutulan insanın yerini gönüllü, iş birliğine hevesli insanın alması amaçlanmıştır. Üstelik gözetim sadece anı kontrol eden bir mekanizma olmaktan çıkarak veri işlemeye dayalı karar alma gibi dijital teknikler kullanılarak geleceğe dönük tahminlerin ve buna bağlı denetimlerin yapıldığı bir projeye dönüşmektedir. Dijital çağın yeni gözetim teknikleri veri işlemeye dayanmakta ve bu verilerin kaynağını biyometrik verilerinden günlük aktivitelerine kadar gözetlenen toplumlar oluşturmaktadır. İnsanlar gözetlenmekle kalmaz, bu veriler aracılığıyla incelenir, değerlendirilir ve yargılanır. Fakat bu gözetim katı bir şekilde yapılmaz. İnsanlar cep telefonlarını kullanarak, günlük internet sorgulamaları yaparak, kredi kartı harcamalarıyla, seyahatleriyle bu gözetim sistemine gönüllü olarak veri taşımaktadırlar. Yüz tanıma sistemleri Facebook'ta insanları etiketlemek için, cep telefonunun kilidini açmak ya da iş yerinizin kapılarını açmak için kullanılırken diğer yandan insanların toplu olarak gözetlenmesine yol açmaktadır. Bu sistem kişilerin yalnızca gizlilik ve mahremiyet kaybına uğramasına neden olmaz, bunun yanında toplumsal sınıflandırmaya maruz bırakılarak dijital ayrımcılığa uğramalarına sebep olur(Lyon, 2003) . Bu istatistik ve yazılım sürecinin içerisinde dezavantajlı gruplar daha fazla ayrımcılığa uğramaktadır. Örneğin Müslüman ve Arap yolcular havaalanlarında daha fazla rastgele incelemeye maruz kalabilmektedir. Panoptik sistemlerde kişide her an izleniyorum korkusu oluşturan gözetleme, günümüzde hayatın her anında uygulanmakta fakat bu kez kişide göz önünde olma, yalnız kalmama, sosyal ortamdan kopmama zevki yaşatmaktadır. İnsanların korkusu olan hapsedilmek yerini toplumdan dışlanmaya bıraktığı için gözetleme uygulamalarına maruz kalmak istenen ve haz verici bir duruma dönmüştür (Bauman ve Lyon, 2013, s. 42). Yapılan paylaşımlar, alınan beğeniler, takipçi sayıları toplumsal konumu göstermeye başlarken sosyal medyada olmamak ise toplumsal hayatta var olmamak ile eş anlama gelmeye başlamıştır. Sosyal medya insanlar için yalnızlıklarından kurtulabilecekleri bir araç olmuştur. Dünyadaki genç nüfusun sosyal medyayı aktif olarak kullanma verileri bu çıkarımları desteklemektedir. Şekil 1.3'te görülen verilere

göre OECD ülkeleri arasında 16-24 yaş aralığındaki genç nüfusun aktif olarak sosyal medya kullanma oranı yüzde 89'un üzerindedir.



Şekil 1.3 : Ülkelere göre 16-24 yaş aralığında aktif olarak sosyal medya kullanan genç nüfusun oranı, Url-1 'den alınmıştır.

Bunun dışında sosyal medya kullanmamak kişiler için dışlanmayı, suç işlediğinden şüphe duyulmayı beraberinde getirir. Enriquez bu durumu şu sözlerle ifade etmektedir: “Önceleri görünmez olanın -herkesin mahremiyeti, herkesin içsel yaşamı- şimdilerde kamusal sahnede (esasen TV ekranlarında ama aynı zamanda yazılı sahnede) ifşa edilmesi gerektiği hatırlanırsa, kendi görünmezliğini önemseyenlerin yadsınmaya, dışlanmaya veya bir suç işlediğinden kuşkulanılmaya mahkum olduğu anlaşılabilir. Fiziksel, sosyal ve ruhsal çıplaklık günün gereklilikleridir.” (Bauman ve Lyon, 2013, s. 43). Her şeyin şeffaf olması ve gözetim uygulamalarına tabii olmak toplumsal bir gereksinim haline gelmeye başlamıştır. İstekle ve zevkle dahil olunan bu platformlarda kullanıcılar aslında satılan ürüne dönüşmekte, pazarlanan ürün kişinin kendisi ve kişisel verisi olmaktadır. Daha çok takip edilen kişi toplumsal konum olarak üstte yer alır.

1.1 Akışkan Gözetim

Panoptik sistemlerin günümüzdeki evrimi herkesin kendi gözetleme sistemini yanında taşıyacak şekilde şartlanmış olmasıyla gerçekleşmektedir. Çalışanların cep

telefonlarını ya da bilgisayarlarını almadan tatile çıkmaları dahi mümkün değildir. Yöneticilerin bu durumda panoptik bir sistem kurma, onu düzgün şekilde işletme yükümlülükleri ve bu sistemin masrafı ortadan kalkmıştır.(Bauman & Lyon, 2013, s. 73) . Katı ve maliyetli olan panoptik gözetim yerini akışkan gözetime bırakmaktadır. Çalışanlar her an gözetleniyormuş hissi ile kendi öz disiplinlerini dış bir müdahale olmadan sağlamaktadırlar. Gönüllü olarak işleyen bu panoptik sistem sinoptikon olarak adlandırılır. Çalışanlara verilecek ödüllerle bu sistem içinde gönüllü yer almanın alt yapısı oluşturulmuş olur.

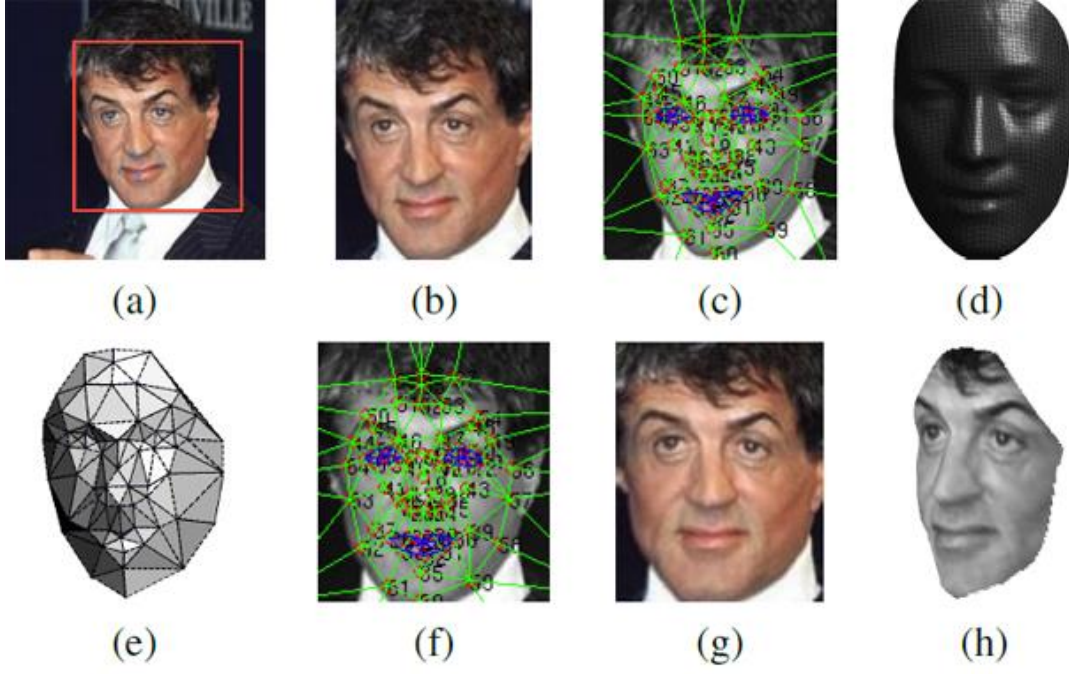
Panoptikonun şüphe duyulan, hor görülen ve istenmeyen azınlıkları gözetleme ve kontrol altında tutma gibi bir işlevi de bulunmaktadır. Bu sistemde dışlanmış gruplar geçmiş veriler ve profillemeye teknolojileri kullanılarak şüphe duyulacak ve gözetlenecek topluluk olarak belirlenir. Bu panoptik sistemin adı panoptikondur(Fierke, 2007, s.183) . Düşmanı gözetlemeye, işaretlemeye ve gerektiğinde yok etmeye programlanan askeri ihalar bu panoptik sistemin içine dahil edilmektedir.

1.2 Panaptikon Uygulamaları

Facebook'un geliştirmiş olduğu aynı insana ait iki farklı fotoğrafı eşleştirebilen yazılımı DeepFake %97.25 başarı oranı yakalamıştır. Bu oran ile insanların yapabildiği başarılı eşleştirme oranının(%97.53) arasında çok küçük bir fark bulunmaktadır(Chowdhry, 2014).

DeepFace'in çalışma mantığı iki ayaktan oluşmaktadır. İlk aşamada yüzün farklı açıdaki görüntüsü düzeltilerek düz bakan üç boyutlu bir model elde edilmekte, daha sonrasında ise derin öğrenme ile eğitilmiş bir yapay sinir ağı yüzün nümerik bir tanımını çıkarmaktadır. İki farklı görüntüden yeterli eşleşme oranı yakalanırsa yazılım burada görüntülerin aynı kişiye ait olduğu sonucunu çıkarır (Simone, 2014). Şekil 1.4'te DeepFace yazılımının yüzün farklı açılardaki görüntüleri için yaptığı modelleme örnekleri gösterilmiştir.

Makine öğrenmesi ve yapay zeka uygulamaları veriye ihtiyaç duyan algoritmalar ile çalışmaktadır. Bu algoritmaların daha kesin sonuçlar verebilmesi sürekli daha fazla veri seti ile eğitilmesi gerekmektedir. Buradaki soru ise ihtiyaç duyulan bu verinin kaynağı ve nasıl toplandığıdır.



Şekil 1.4 : DeepFace Facebook'un yüz tanıma yazılımı, Url-2'den alınmıştır.

Sistemlerini satarak daha fazla kar etmek isteyen şirketler bu veri açığını milyonlarca insanın kullandığı sosyal medya, internet siteleri ve cep telefonu uygulamaları ile karşılamaktadır.

Uluslararası Af Örgütü'nün raporuna göre teknoloji devleri Google ve Facebook gözetim tabanlı iş modeli uygulayarak servislerini kullanan kişilerin kişisel bilgilerini topluyorlar(Amnesty International, 2019, s.12). Facebook kendi sitesinde yer verdiği açıklamasında oturumunu kapatmış kullanıcılarının ve hatta Facebook kullanıcısı olmayan kişilerin, kendi servislerini kullanan farklı websitelerini ziyaret etmeleri durumundabilgilerinin toplandığını söylüyor (Baser, 2018). Bu bilgiden sonra şirketin yaptığı savunma da ilginç: "Twitter, Amazon, Google, LinkedIn gibi şirketler de bu verileri topluyor" (Baser, 2018). Yine Uluslararası Af Örgütü'nün raporuna göre Google ve Facebook şirketleri evlerimizde akıllı ev eşyalarımız aracılığı ve Nesnelerin İnterneti teknolojisini altyapısıyla, akıllı şehir tasarımlarıyla vakit geçirdiğimiz mekanları kişisel verilerin toplandığı bir alana dönüştürüyorlar(Amnesty International, 2019, s.12). Bu iki dev şirket pazarlarını daha da genişletmek için internete erişimi olmayan dünya popülasyonunun yarısına ulaşmayı hedefliyorlar (Reynolds, 2018). İnternet erişimi olmayan bölgelere internet alt yapısı sağlama konusundaki girişikleri yarışın sonucunda daha fazla insanın kişisel verilerine ulaşmayı hedefliyorlar.

IBM, ocak ayında fotoğraf paylaşma sitesi Flickr'dan çektiği bir milyona yakın kayıt olan veri koleksiyonunu araştırmacıların kullanımına açmıştı. Ancak bu fotoğraflar kullanıcılardan ya da fotoğrafçılardan izin alınmadan kullanılmıştır (Solon, 2019) . Başlarda ünlü isimlerin fotoğraflarıyla eğitilen algoritmaların veri açlığını doyumak için sıra sıradan insanların kişisel verilerine gelmiştir. Bireylerin tek tek rızalarını almanın zor olduğunu bilen şirketler, hukukun teknolojinin hızına yetişememesini ve yasadaki boşlukları ve gri alanları fırsat bilip kişisel verilerimizi kullanmaya devam etmektedir. Örneğin IBM yaptığı açıklamada kullanıcıların başvurması halinde fotoğraflarını veri tabanlarından kaldıracağını söylemiştir(Solon, 2019) . Fakat bunun için veri tabanından hangi fotoğraflarınızın kullanıldığını bulmanız gerekmektedir. Ek olarak, fotoğraflarının IBM tarafından kullanıldığından haberi dahi olmayan yüzbinlerce kullanıcıyı düşünürsek büyük şirketler karşısında toplumun zayıf bir konumda olduğunu söylemek mümkündür.

Yüz tanıma sistemleri sadece ticari amaçla değil devletler tarafından güvenlik amacıyla da kullanılmaktadır. Çin yüz tanıma sistemleriyle toplu gözetimi etkinleştiren ilk devletlerden biri oldu. Çin Devleti aranan suçluları bulabilmek için binlerce kişinin bir araya geldiği spor müsabakalarında vatandaşlarını gözetime tabii tutmaktadır (Schuppe, 2018) . Aynı uygulamalara insan haklarına daha saygılı olduğu düşünülen batı devletlerinde de rastlanmaktadır. 27 Ekim günü İngiltere'de oynanan Swansea City - Cardiff City maçında seyirciler üstünde yüz tanıma teknolojisini kullanan Güney Galler polisine karşı taraftar grupları maça cadı maskeleriyle katılma çağrısı yapmıştı(E&T editörü, 2019). Galler Futbol Taraftarları Birliği sözcüsü Vince Alm uygulamaya karşı çıkarken aralarında çocukların da bulunduğu hiç suç işlememiş binlerce masum taraftarın yüzlerinin taranmasının ve verilerinin toplanmasının tamamen gereksiz ve ölçüsüz olduğunu söylemişti. Gelen tepkiler üzerine açıklama yapan Güney Galler polisi taramanın bu maça özel olduğunu, futbol suçlarından mahkum edilen taraftarın karşılaşmaya katılımının önlenmesinin ve olası tehditlerin önüne geçmek için uygulandığını söyledi. Bundan önce dava konusu olan İngiltere polisinin güvenlik nedeniyle yüz tanıma teknolojisini kullanması yüksek mahkeme tarafından insan haklarına ve İngiltere'nin kişisel verileri koruma uygun bulunmuştu(Burgess, 2019) . 500 bin insanın yüzü yüz tanıma sistemlerinin deneme aşamasında Güney Galler Polisi tarafından toplanmış durumdadır. Ülke genelinde 20

milyon insanın yüzlerine ait fotoğrafların İngiltere polisinin veri tabanında bulunduğu bilinmektedir(Burgess, 2019) .

İsrail ordusu Batı Şeria’da yaşayan Filistinlileri sürekli olarak gözetleyebilmek için bölgeye binlerce kamera yerleştirmiştir ve bu kameraların sayısını gün geçtikçe arttırılmaktadır(Harel, 2017) . Masumiyet karinesine bakılmaksızın potansiyel birer suçlu görülen Filistinlilere karşı yapılan ayrımcılık kitlesel gözetimlerle daha da derinleşmiştir. Kameralardan alınan verileri ve yüz tanıma sistemlerini kullanarak Filistinlileri gözetleyen uygulamalar geliştiren AnyVision şirketine 2018 yılında büyük data kullanarak yüzlerce terör saldırısını önlediği gerekçesiyle İsrail devleti tarafından savunma ödülü verilmişti (Solon, 2019) . Bu şirket Microsoft’tan aldığı 74 milyon dolarlık yatırımla da tartışma konusu olmuştur. AnyVision’ın İsrail ile yaptığı iş birliği ile beraber 200bin insan potansiyel terörist olarak fişlenmiş ve gözetim bu insanlar üstünde yoğunlaştırılmıştır. Bu liste insanların İsrail’i eleştiren Facebook paylaşımları, Hamas’ın popüler olduğu köylerde yaşamaları gibi kriterlere göre hazırlanmıştır. Bireyin suç işlediği kanıtlanana kadar masum olduğu ilkesi açıkça ihlal edilmektedir. Diğer yandan devletlerin kendi terörist profiline göre eğittiği algoritmalar ezilen azınlıklara suçlu şüphesiyle yaklaşacak, veri toplama ve izleme işlemini bu topluluklar üzerinde yoğunlaştıracaktır. İsrail’de Filistinliler, ABD’de zenciler, Avrupa’da göçmenler ve mülteciler daha sıkı teknolojik takibin ve buna müteakip daha çok inceleme ve soruşturmanın konusu olacaklardır.

Aynı şirket yalnızca askeri çözümler değil sivil alan için de yüz tanıma teknolojileri geliştirmektedir. Bunlardan biri tüm vücudu tarayarak kişileri tanıyıp, taraftarların stadyumlara biletsiz girebilmelerini sağlayan yapay zeka tabanlı yüz tanıma sistemi(Blunden, 2018) . Bu yüz tanıma sistemine ait resim Şekil 1.5’te bulunabilir. Bu yazılımla birlikte maç, konser, festival gibi insan topluluklarının yoğun olarak katıldığı etkinliklerde turnike yönteminin kalkması ve insanların kuyruklarda vakit harcamasının önüne geçilmesi hedeflenmektedir.

Aynı şirketin geliştirmiş olduğu iki farklı yazılım dünyanın bir yerinde ezilenler için baskı aracına, diğer yanda insan hayatını kolaylaştıran bir teknolojiye dönüşmektedir. Marx’a göre gözetim emek ve sermaye arasındaki mücadelenin bir parçasıdır (Bozkurt, 2000). Sanayi devrimi ile atölyelere ve fabrikalara doldurulan işçilerin

ürettikleri artı değeri arttırmanın yolu işçilerin üretim sürecini gözetleyerek kontrol etmekten geçer.



Şekil 1.5 : AnyVision’a ait yüz tanıma sistemi taraftarların tüm vücudunu tarayarak, maçlara biletsiz girebilmelerini sağlıyor, Url-3’ten alınmıştır.

18. yüzyılın sonunda ve 19. yüzyıl boyunca işçiler yönetimin kişisel nezaretinde çalışmıştır. Günümüzde emeğin farklı üretim metotlarıyla birlikte farklı mekanlarda konumlanmasıyla bu gözetim metotları çeşitlenmiştir. Beyaz yakalı çalışanların bilgisayarlarının otomatik ekran görüntülerini alarak üstlerine ileten programlar ve girdikleri internet sitelerini kayıt altına alan loglama sistemleri emeğin disiplin altına alınmasını sağlamaktadır.

1.3 Covid-19 Ve Toplu Gözetim

Tüm dünyayı etkisi altına alan, ekonomileri durduran ve insanları evine hapseden Koronavirüs salgını için bundan sonra hiçbir şeyin bir daha eskisi gibi olmayacağı yorumları yapılıyor. Normalleşme sözcüğünün bile eskiye dönme değil ‘yeni normal’e uyum sağlamak anlamında güncellendiği bu pandemi sürecinin etkileriyle başa çıkabilmek ve yeni dalgalara karşı önlem alabilmek için devletler stratejilerini belirlemeye başladılar. İnsan sağlığı konusunda devletlerle tam bir uyum ve işbirliği içinde olması beklenen kamuoyundan ise getirilmekte olan bazı tedbirlere karşı muhalif sesler yükseliyor. Tartışmalara yol açan en ciddi başlık ise tanıdık: hastalığın

yayılımını sınırlandırmak için teknoloji yardımıyla insanları toplu olarak gözetlemek. Pandemi nedeniyle ortaya çıkan kamu sağlığının korunması ihtiyacının karşısında kişilerin mahremiyetinin korunması durmakta ve bu iki temel menfaat birbiri ile çatışmaktadır. İdeal olan bu çatışmayı en adil ve topluma en az zarar verecek şekilde dengeleyebilmektir. Kamu sağlığı ve toplum güvenliği lehine yapılacak bir tercih ilk bakışta pandemi ile mücadele açısından meşru görünse de, mahremiyet ve kişisel verilerin korunması konularında bireylerin aleyhine uygulamalar uzun vadede çok daha ciddi toplumsal sorunlara yol açabilecektir.

Yeni yeni kullanılmaya başlanan kişi takip uygulamalarında kişilerin konum verileriyle beraber açık kimliklerinin depolanabilmesi, depolanan bu verilerin ne amaçla ne kadar süreyle kullanılabileceği ve hangi kurum ya da kişilerle paylaşılabileceği soruları kişinin mahremiyeti konusunda bazı tartışmaları başlatmış durumda.

ABD’de kullanıcının GPS verilerini kullanarak bir takip uygulaması geliştirmeyi planlayan Phunware firması Donald Trump’ın içinde bulunduğu başkanlık yarışında lokasyon bazlı potansiyel seçmen çalışması yapan bir şirket olarak dikkat çekiyor (Biddle & Fang, 2020). Trump’ın başkan seçildiği 2016 kampanyası sonrası patlak veren ve milyonlarca Facebook kullanıcısının verilerinin kampanya için usulsüz şekilde kullanıldığı Cambridge Analytica – Facebook skandalı(Confessore, 2018) düşünüldüğünde, Phunware firmasının aldığı bu karar ilginç bir hal alıyor.

Çin’de Koronavirüs önlemleri kapsamında kullanılmaya başlanan kişi takip uygulaması kişinin konumunu ve kimlik numarasını otoriteye ait sunuculara gönderiyor ve bu veriler polis birimiyle de paylaşılıyor(Mentha, 2020). Norveç’te kişiye ait telefondan toplanan GPS ve Bluetooth verisi merkezi sisteme gönderilirken bu verilerin yalnızca pandemi ile mücadele için kullanılması ve 30 günlük süre sonunda silinmesi yasa ile karara bağlanmış durumda (DeVries, Krolik & Singer, 2020). Almanya ve Avusturya gibi bazı ülkeler ise Apple ve Google’ın geliştirdiği GPS yerine bluetooth teknolojisinin kullanıldığı, kişinin verilerinin merkezi bir sistemde toplanmadığı modeli tercih ettiler(Kelion, 2020). Bu sistemde kullanıcıdan toplanan verilerin azaltılması ve verilerin hükümetle paylaşılmaması kişinin mahremiyetini korumak için bir kalkan sağlamaktadır.

Farklı uygulamalarını gördüğümüz bu takip sistemleri için Avrupa Birliği'nin yayınladığı araç kutusunda pandemi ile savaşılmaları için teknolojiden yararlanmanın önemli olduğu vurgulanırken bunun mahremiyet ilkesinden vazgeçilmeden yapılabileceğini vurguluyor ("Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures", 2020). Araç kutusunda yer verilen ve üye devletlerin riayet etmesi istenen ilkeler ise şunlardan oluşuyor:

- Uygulamalar AB veri koruma ve mahremiyet ilkelerine uygun olmalı,
- Halk sağlığı otoriteleri ile koordinasyon halinde ve onların onayı alınarak geliştirilmeli,
- Gönüllü biçimde yüklenmeli ve ihtiyaç kalktığı an uygulamaların ömrü sona ermeli,
- Mahremiyetin korunması için uygun teknolojik çözümler kullanılmalı. Kişinin konum bilgisinin izlenmesi yerine Bluetooth teknolojileri baz alınmalı,
- Anonimleştirilmiş veri kullanılmalı. Hasta bireyle temas eden kişiler uyarılmalı fakat hasta bireyin kimlik bilgileri gizli tutulmalı,
- AB ülkeleri içinde uyumlu olmalı ve AB vatandaşları sınırlar dışında da korunmalı,
- Siber güvenlik alanında en iyi önlemler alınmalı,
- Güvenli ve efektif olmalıdır.

Konuya getirilen bir diğer yaklaşım ise bunun bir halk sağlığı problemi olduğu ve Koronavirüs ile daha etkili bir mücadele için toplumun genel çıkarının birey hak ve özgürlüklerinin önüne geçebileceği. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanı Ali Taha Koç yaptığı açıklamada şunları dile getirmişti:

"Kamu olarak ne kadar fazla veri toplanırsa risk analizini daha doğru yapabileceğimizi söyleyebilirim (...) Her gün yeni özellikler ekliyoruz. Yakında bir barkod uygulaması getireceğiz. Bu sayede Covid-19 pozitif tanısı olduğunda bu özellik sayesinde girilen yerler ve zamanları takip edilecek. Salgının yayılmasını önleme açısından kişi bazlı takip çok önemli." (Kasapoğlu, 2020).

Koronavirüs sonrası dünyanın sadece günlük yaşamımızda değil veri güvenliği ve kişi mahremiyeti konularında da yeni düzenlemelerle geleceğini şimdiden söyleyebiliriz.

1.3.1 Hayat eve sığar mobil uygulaması

Sağlık Bakanlığı tarafından yayınlanmış olan Hayat Eve Sığar mobil uygulamasına dair aydınlatma metni ‘Veri Sorumlusu Kimliği’ni belirleyerek başlar: “Bu uygulamada işlenen kişisel verileriniz bakımından veri sorumlusu T.C. Sağlık Bakanlığı’dır.” (“T.C. Sağlık Bakanlığı Filyasyon Ve İzolasyon Takip Sistemi(Fitas) Kullanıcı Sözleşmesi Ve Mahremiyet Politikası”, t.y). Veri sorumluluğu bireyin kendisinde değildir.

Kasapoğlu’nun haberinde, Hayat Eve Sığar uygulamasını kullanmak için kullanıcıdan alınan izinler şöyle sıralanıyor (2020): “GPS ve ağ tabanlı konum bilgilerine erişim, telefon rehberi, kamerada resim çekme ve görüntü kaydetme, kablosuz bağlantılar, tam ağ erişimi, Google hizmet yapılandırmasını okuma, Bluetooth ayarları, internetten veri alma.

Bunlara ek olarak hali hazırda kayıtlı olan e-devlet kimlik bilgileri, e-nabız sistemi ve Mernis (nüfus ve vatandaşlık işleri) verilerine de erişim sağlanıyor. Hayat Eve Sığar uygulaması Türkiye’de faaliyet gösteren üç GSM operatörüyle çalıştığı için cep telefonunun kayıtlı olduğu operatörle paylaşılan tüm veriler yine bu uygulama aracılığıyla devlet sistemlerine doğrudan erişim veriyor.”

Yine aynı habere göre Alternatif Bilişim Derneği Yönetim Kurulu Başkanı Avukat Faruk Çayır depolanan bu bilgiler ile anonimleştirmenin çok zor yapılacağını ve kişinin kimliğinin belirlenebileceğine dikkat çekiyor (Kasapoğlu, 2020): “Diğer veriler bir yana, konum verilerinin tamamen anonim hale dönüştürülmesi bile çok zor. Konum verileriyle birlikte 3 ya da 4 veriyi birleştirdiğinizde rahatlıkla kişileri tanımlanabilir hale getirebilirsiniz. Tek bir konum verisinin bile kaydedilmesi tehlikeliyken, 'Biz ne kadar çok veri toplarsak o kadar iyidir' anlayışı yanlıştır ve güvenliğinin ne kadar sağlanabileceğini de tartışmalı hale getirir.”

2. GÜVENLİK Mİ ÖZGÜRLÜK MÜ?

İnternet yapısı gereği açık, herkesin kullanabileceği, kullanıcıların eşit ve özgür olduğu, birbirlerine eşit koşullarda bağlanabildiği ortak bir ağıdır. Bu ağ küresel düzeyde birbirine bağlanan bilgisayar ağlarının belli bir protokol altında haberleşmesiyle meydana gelir. Çevrimiçi ağların haberleşme, teknoloji ve nihayetinde sosyal ağlarla günlük birey davranışlarında, toplumsal ilişkilerde meydana getirdiği büyük devinimi anlayabilmek için internetin nasıl ortaya çıktığını ve teknik altyapısını incelemek gerekmektedir. Bu bilgiler internetin mevcut durumunu anlamak ve günümüzdeki çevrimiçi ortamdaki gözetim, güvenlik, mahremiyet ve demokrasi tartışmalarını daha iyi anlayabilmek için bize kılavuz olacaktır.

2.1 İnternetin Tarihi

İnternetin temelleri ABD Savunma bakanlığının geliştirdiği bir proje olan ARPANET (Advanced Research Projects Agency Network) ile atılmıştır. Ülkenin yapacağı olası bir nükleer atak için gerekli hesapları yapmak için bu projeye başlanmıştır. Nükleer silahların yüklemelerini yapan ve dünyanın dört bir yanında bulunan bilgisayarları birbirine bağlayacak bir sistemin araştırmaları yapılırken 1969 yılında 4 bilgisayar arasında bir ağ oluşturulmuştur(Schneider, Evans, Pinard, 2010, s.6) . Bu ağ bilgisayarlar arasında paket alışverişini sağlamaktaydı.

Bilgisayarlar arasındaki iletişimin ilk kez gerçekleştiği bu tarihsel an California Üniversitesi'nin Stanford Araştırma Enstitüsü'yle kurduğu ağ ile gerçekleşmiştir. Bu diyalog tarih sayfalarına şu şekilde girmiştir (Gromov, t.y.) :

“Stanford’a telefon açtık ve L yazıp onlara sorduk:

“L’yi gördünüz mü?”

“Evet L’yi gördük.” diye cevap geldi.

O yazdık ve sorduk, “O’yu gördünüz mü?”

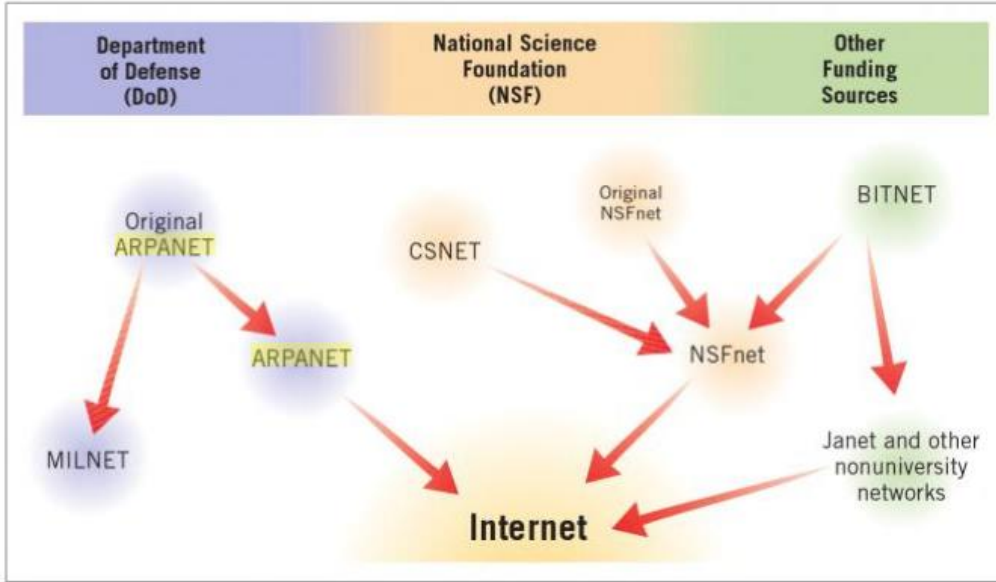
“Evet O’yu gördük.”

Sonra G yazdık ve sistem çöktü.

Fakat devrim başlamıştı.”

Bu ağın paket gönderimi esnasında transfer kuralları belirlemek için TCP/IP transfer protokolü oluşturuldu. TCP(Transmission Control Protocol) bir bilgisayarın bir ağda bağlantı kurması ve bu bağlantıyı kapatması için gerekli kuralları içeren protokoldür. IP(İnternet Protocol) transfer edilen paketlerin yönlendirme kurallarını içeren protokol olarak görev yapmaktadır. TCP/IP protokolü birlikte bir bilgisayarın bir ağa paket göndermesi ya da alabilmesi için gerekli olan kurallar bütünü oluşturur.

1981 yılına gelindiğinde INTRANET alt yapısını 200 bilgisayar kullanmaya başlamıştı. Genişleyen ve trafiği artan ARPANET ikiye bölündü. (Schneider, Evans, Pinard, 2010, s.6) . ARPANET araştırma etkinlikleri için devam ederken yeni oluşturulan MILNET(Military Network) askeri araştırmalar için yüksek güvenli bir ağ olarak rezerve edilmişti. 1987 yılında Ulusal Bilim Kuruluşu(National Science Foundation) tarafından kurulan NSFnet ve ARPANET daha fazla ağ trafiği yönetebilmek için birleştiler ve günümüzdeki internetin temelleri atılmış oldu. İnterneti oluşturan ağlar şekil 2.2’de verilmiştir.



Şekil 2.2: İnterneti Oluşturan Ağlar (Schneider, Evans & Pinard, 2010)

Bildiğimiz anlamda internetin ya da diğer bir deyişle world wide web'in ortaya çıkışı ise 1990 yılının Kasım ayında İngiliz bilim insanı Tim Berners-Lee'nin yazdığı makale

ile olmuştur. 1990 yılının sonunda Tim Berners-Lee makalesinde açıkladığı fikirleri hayata geçirmiş ilk internet sunucusu ve tarayıcısı CERN’de çalışmaya başlamıştır. Şekil 2.3’te tarihteki ilk web sitesi ve onun kurucusu Tim Berners-Lee görülmektedir. Kod geliştirerek internet sunucusunu kurduğu bilgisayarın yanlışlıkla kapatılmasını engellemek için üstüne kırmızı kalemle yazılmış şu uyarı notunu bırakmıştır: “Bu makine bir sunucudur. LÜTFEN KAPATMAYIN” (“Where the Web was Born”, t.y.). Tim Berners-Lee’nin oluşturduğu dünyanın ilk internet sitesi hala <http://info.cern.ch/> adresinde yayındadır.



Şekil 2.3: İnternetin Yaratıcısı, Url-4’ten alınmıştır.

2.1.1 İnterneti kim kontrol ediyor?

İnterneti yöneten kurumlardan ya da merkezi bir yapıdan bahsetmek mümkün değildir. Bugüne kadar merkezsiz, hiyerarşinin olmadığı, dağıtık bir yapıda olan internet için kontrolün de bir grubun elinde olduğundan bahsedilememektedir. Fakat internet servis sağlayıcıları kendi ağları üstünden veri alış verişi yapan trafikleri izleyebilmekte, büyük şirketler kişilerin bilgilerini depolamaktalar. Bu açıdan internetin mimarisi değişmeye ve iletişim kontrol altında tutulmaya başlanmıştır. Bahsedilen servis ve içerik sağlayıcılarının yanında internetteki standartları belirleyen uluslararası kurumlar bulunmaktadır (Dursun, “İnternet Üzerine Güncel Bir Panorama”, 2014).

- IETF (Internet Engineering Task Force): Uluslararası gönüllü bir topluluk olan IETF internet standartları için teknik ve teknolojik katkılar yapmaktadır. TCP/IP protokollerinin de içinde olduğu protokollerin yönetilmesinden ve geliştirilmesinden sorumludur.
- W3C (The World Wide Web Consortium): İnternetin teknik standartlarını belirleyen uluslararası bir kurumdur. Web site sahipleri ve şirketler uymak zorunda olmasalar da, bu sertifika sitelerin uygun teknolojilerle çalıştığını belgeler. Kendi sitelerinde yazdıklarına göre W3C'nin ana amacı internetin faydalarından coğrafya, dil, kültür, sahip oldukları yazılım, donanım ya da ağ alt yapısı ne olursa olsun tüm toplulukların ve insanların yararlanabilmesine imkan sağlamaktır.
- ISOC(Internet Society): 1992 yılında ABD'de kurulmuş kar amacı gütmeyen bir kurumdur. Amacını dünyanın her yerindeki insanlara internet erişiminin sağlanması olarak açıklar. IETF ile internet standartlarının geliştirilmesi için ortak olarak çalışır.
- WIPO(World Intellectual Property Organization): Birleşmiş Milletler bünyesinde kurulmuş telif haklarının ve fikri mülkiyet haklarının korunması için uluslararası standartların geliştirilmesini hedefleyen organizasyondur.
- ICANN(The Internet Corporation for Assigned Names and Numbers): ABD hükümeti bünyesinde kurulmuş fakat şu an bağımsız ve kar amacı gütmeyen bir kurum olarak çalışan ICANN internetin alt yapısıyla ilgili kritik bir rol oynamaktadır. ICANN Alan adı(domain name) ve .com, .info gibi alan adı uzantılarını düzenler, alan adı satan şirketlerin standartlarını belirler.
- IANA(Internet Assign Numbers Authority): ICANN'nin bir parçası olan IANA alan adlarıyla çalışan IP adreslerinin (Internet Protocol) dağıtılması ve paylaştırılmasını sağlayan uluslararası kurumdur.

Görüldüğü üzere internet standartları, kuralları ve protokollerini belirleyen kurumlar kar amacı gütmeyen, devletlerin ya da şirketlerin kontrolü altında olmayan organizasyonlardır. Hala internetin demokratik yapısından bahsedebiliyorsak bu hiyerarşisiz mimarinin bunda büyük payı vardır.

2.1.2 Temel bir insan hakkı olarak internet

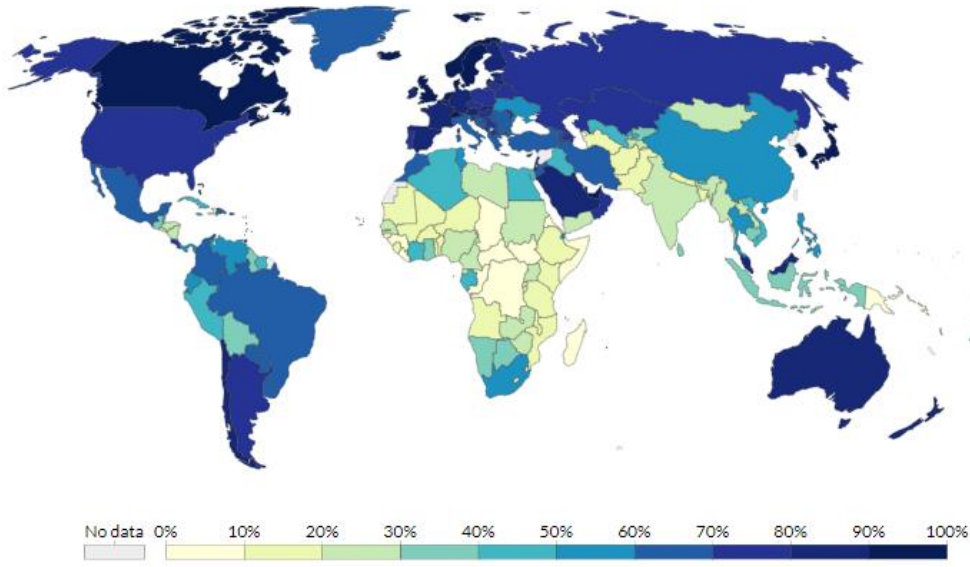
Devletlerin ve şirketlerin panoptik gözetimiyle bireylerin özel hayatın gizliliği ilkesi kitlesel şekilde ihlal edilirken, yargının mahkeme kararlarıyla, yasa koyucuların yeni mevzuatlarla teknolojinin bu baş döndürücü hızına yetişme çabalarına hepimiz tanık oluyoruz. Yasaların bizi koruyup korumadığına, yapılan düzenlemelerin toplumun mu yoksa dev şirketlerin mi yararına olduğunu incelemeden önce bugün bu konuları tartışmamıza vesile olan o büyük ağı, yani interneti, temel bir insan hakkı olarak değerlendirip bu haktan dünya nüfusunun hangi şartlarda ne kadar yararlanabildiğini incelemek yararlı olacaktır.

Birleşmiş Milletler İnsan Hakları Konseyi interneti temel insan haklarından biri olarak kabul etti (“BM interneti "temel insan hakkı" olarak kabul etti”, 2016). Bu karardan önce Estonya, Finlandiya, İsveç, Fransa yalnızca interneti değil geniş bant erişimini de insan hakları olarak tanımıştı (Öymen, 2016). İnternet temel bir insan hakkı olmasının yanında Anayasa ve Avrupa İnsan Hakları Sözleşmesi ile garanti altına alınmış olan ifade ve haber alma ve iletişim özgürlüğünün görünümü olarak da değerlendirmek doğru olur. İnternet erişiminin tüm insanlara sağlanması gereken dünyamızda diğer tüm alanlarda olduğu gibi burada da adaletsiz ve çarpık bir dağılım bulunmaktadır.

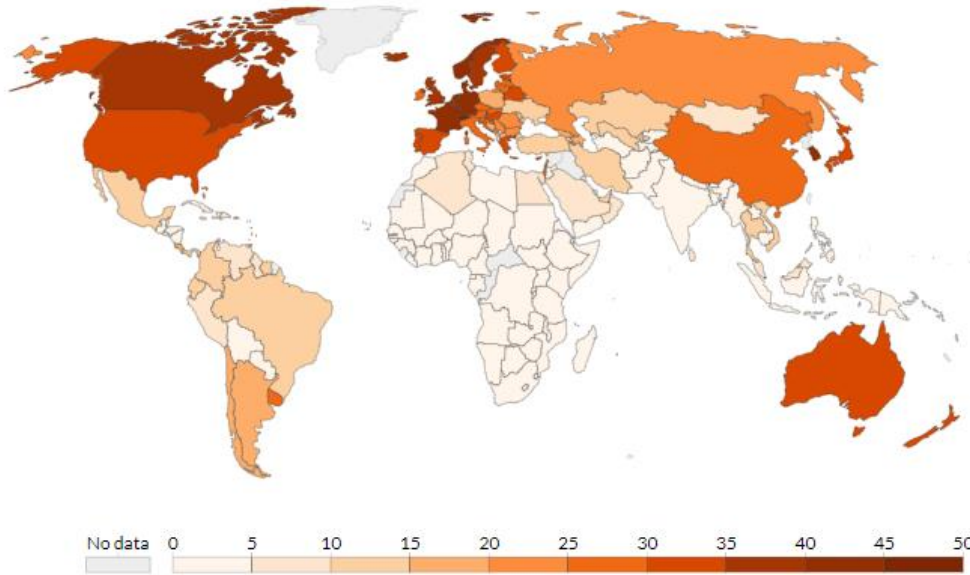
Şekil 2.4’te görselleştirilmiş hali bulunan 2016 yılı istatistiklerine göre ABD nüfusunun yüzde 76’sı, Malezya’nın yüzde 79’u, İspanya ve Singapur’un yüzde 81’i, Fransa nüfusunun yüzde 86’sı, Güney Kore ve Japonya nüfuslarının yüzde 93’ü, Danimarka ve Norveç nüfuslarının yüzde 97’si ve listenin en başında olan İzlanda halkının yüzde 98’si internet erişimine sahip. Diğer yandan en fakir ülkeler arasında bulunan Eritre, Somali, Gine Bissau, Orta Afrika Cumhuriyeti, Nijer ve Madagaskar halklarının yüzde 5’ten azı internete ulaşma imkanına sahip.

Benzer sonuçlar Şekil 2.5’te görselleştirilmiş olan 256 kbit/s ve üstündeki hızlarda internet bağlantısına erişebilen insan popülasyonunun dünyadaki dağılımını gösteren haritaya bakarak çıkarılabilir.

Temel bir insan hakkı olarak tanımlanmasına rağmen gelişmiş ülke vatandaşlarının yüksek hızda internet erişimine sahipken, gelişmemiş ülkelerde insanların temel bir internet erişimini bulmakta dahi zorlanması tüm insanların doğuştan aynı haklara sahip olmadığını gösteren çarpıcı bir örnektir.



Şekil 2.4 : Dünya Popülasyonunun İnternete Erişim Haritası, Url-5'ten alınmıştır.



Şekil 2.5 :Kişi başına düşen hızlı internete ulaşım oranı, Url-6'dan alınmıştır.

Diğer yandan panoptik gözetim ile takip edilen, verileri toplanan, bir yandan müşteri bir yandan şüpheli olarak sınıflanan insanlar yoğunlukla bu imtiyazdan yararlanabilen zengin ve 'demokratik' ülkelerin vatandaşları olmaktadır. Bundan sonra incelenecek hukuki düzenlemeler de bu bölümde bahsettiğimiz hızlı bir internet altyapısı olan bu ülkelerde tartışılmakta ve hukuki sınırlar çizilmeye çalışılmaktadır.

2.2 Özel Hayatın Gizliliği

Özel hayatın gizliliğinin dünyada ilk olarak gündeme gelmesi ABD’li avukat Samuel Warren’in kızının düğünü hakkında çıkan bir magazin haberine sinirlenmesiyle olur. Durumdan rahatsız olan avukat partneri Louis D. Brandeis ile birlikte özel hayatın gizliliğine dair dünya hukuk literatüründe ilk kez dillendirilecek ve ABD hukuk çevrelerini ve giderek dünya hukukunu etkileyecek olan, The Right to Privacy makalesini yazarlar (Proser, 1960). Makale zamanın hukuk profesörlerinden Melville B. Nimmer tarafından “Belki de şu ana dek hukuk alanında yazılmış en etkileyici ve en ünlü makale” diyerek bahsedilir(1954, s.203). Makale kişinin özel yaşamında ve mülkiyet alanında tam bir koruma altında olması gerektiğini söyleyerek başlar. Warren and Brandeis amaçlarının var olan yasaların kişinin gizliliğinin korunması için yeterli olup olmadığını ve bu korumanın ne derecede olduğunu tartışmak olduğunu belirtirler. Ek olarak o günkü yasalarda yer almayan fiziksel anlamda bireyin yalnız kalma hakkının olması gerektiğini öne sürerler. Bireyin yalnız kalma hakkı kişinin kendi eylemleri üstünde belirleyici olarak özel yaşamını ve ilişkilerini belirlemesi hakkına atıfta bulunmaktadır. Yazarlar özel yaşamı sınırsız ve müdahale edilmeyecek bir alan olarak görme eğiliminde değildir. Özel hayatın gizliliği için 6 adet kısıtlayıcı madde önermişlerdir (Brandeis & Warren, 1890).

- I. Özel hayatın gizliliği kamu ve toplumun ortak çıkarlarının önüne geçemez.
- II. Özel hayatın gizliliği kamu kuruluşlarında yasal olarak yapılan iletişimin önüne geçemez.
- III. Sözlü iletişim diğer yasalara uygun olması koşuluyla özel hayatın gizliliği ilkesini ihlal etmez, yazılı yayınlardan bu yönüyle farklı değerlendirilirler.
- IV. Kişinin kendisi tarafından ya da kendi rızasıyla yapılan yayınlarda özel hayatın gizliliği ilkesine uygunluğu aranmaz.
- V. Yayımlanan konunun gerçeklikle ilişkisi ilkenin ihlali durumunda karşı tarafa bir savunma hakkı vermez. Gerçek olmayan yayın zaten iftira suçu kapsamında değerlendirilir.
- VI. Yayıncının(bu durumda ilkeyi ihlal eden kişi ya da kurum) kastının olmaması özel hayatın gizliliğinin ihlali durumunda bir savunma hakkı sağlamaz.

Bu makaleyle gündeme giren özel yaşamın gizliliği ilkesi yıllar içinde çeşitli davalara ve yasalara konu olmuştur.

2.2.1 Örnek davalar

ABD’de 1960’lardan sonra kişilik hakkının bir parçası olan özel hayatın gizliliği, Amerikan mahkemeleri önündeki davalarda daha fazla tartışılmaya başlanmıştır. 1965’teki Griswold v. Connecticut davasında mahkeme Comstock yasası olarak adlandırılan ve çeşitli ilaç ya da araçlarla gebe olmayı engellemeyi yasaklayan yasayı anayasaya aykırı bulmuştur. Yediye karşı iki oyla alınan kararda yasanın bireylerin evlilik mahremiyetine ve özel yaşamın gizliliğine aykırı olduğu belirtilmiştir (“Griswold v. Connecticut, 381 U.S. 479 (1965)”, t.y.).

1967 Katz v. Abd davasının FBI’ın gerekli yasal izinler olmadan yaptığı telefon dinlemesini konu alır. İzinsiz olarak alınan bu kayıtlar bu dava bireye karşı kanıt olarak mahkemede kullanılmıştır. Yüksek mahkeme ise bu uygulamanın yasa dışı olduğu kararını alarak, izin çıkarılmadan yapılan dinlemenin delil olarak kullanılamayacağını ve anayasayı ihlal ettiğini belirtir. Mahkemeye göre bu dinleme topluma açık olan bir mekan da, telefon kulübesinde bile yapılmış olsa özel yaşamın gizliliği ilkesinin ihlal edilmediği sonucuna varılmaz (“Katz v. United States, 389 U.S. 347 (1967)”, t.y.).

1969’da Stanley ve Georgia davasında hakim Marshall devletin porno dahi olsa devletin bir bireyin evinde ne izleyeceğine karışamayacağına karar vermiştir. Bu kararını anayasal mirasın devletin insanların zihinlerini kontrol etme fikrine isyan edeceğine dayandırarak almıştır (“The Right of Privacy The Issue: Does the Constitution protect the right of privacy? If so, what aspects of privacy receive protection?”, t.y.).

1970’lerin Adil Kredi Raporlama Yasası, ABD’de bir bireyin finansal verilerini korumak için kabul edilen ilk yasa idi. Kredi raporlama kurumları tarafından toplanan kişisel bilgilerin korunması yanında, bu bilgilere erişim hakkını da düzenliyordu. Ek olarak, kullanıcıların kendilerine ait bilgilere talep etmeleri halinde istedikleri zaman erişimlerinin sağlanmasını garanti altına alıyordu. 1999 tarihli Finansal Para Kazanma Yasası, bu yasayı baz alarak finansal kurumların müşterilere ne tür bilgilerin toplandığını ve nasıl kullanıldığını açıklayan bir gizlilik politikası sunmasını gerekli kılmıştır. Bu yasaya göre finansal kurumlar, toplanan verileri korumak için yeterli güvenlik önlemlerini almakla yükümlü tutulmuşlardır (Head, 2019).

1973 Miller v. Abd davası FBI tarafından gerçek bir kişiye ait finansal kayıt ve bilgilerin usulsüz ve izinsiz olarak toplanması nedeniyle mağdur olan birey tarafından devlete karşı açılmıştır. Mahkeme finansal bilgilerin halihazırda banka ve banka çalışanlarıyla paylaşıldığını söyleyerek bu bilgilerin kişinin mahremiyetini ihlal etmediğine karar verir (Brown, 2001).

1987 yılında görülen Leander v. İsveç davasında üst düzey bir kamu görevine başvuran yurttaşın iş başvurusunun değerlendirilmesi için istihbarat polisinin kişinin özel yaşamını da içeren istihbarat raporları kullanılmıştır (“Leander v. Sweden, 26 March 1987, 9 EHRR 433, para. 74”, t.y.). Kişiye talep etmesine rağmen bu dosyaların kendisine verilmesi reddedilmiştir. Mahkeme bu davayı Avrupa İnsan Hakları Sözleşmesi’nin özel yaşamın gizliliği ilkesini düzenleyen 8. Madde yönünden incelenmesi talebini kabul etmiş, fakat bu işe alma işleminin bu hakkın kısıtlanabileceği ulusal güvenlik ve kamu güvenliği şartları ile ilişkili olduğu tespitini yaparak bunun özel yaşamın gizliliğini ihlal olarak değerlendiremeyeceği kararını vermiştir.

1997 yılındaki Z v. Finlandiya davasında evli olduğu kişiye Hiv virüsü bulaştıran sanık virüsü kasten bulaştırmakla ve taksirle insan öldürmek suçlarından yargılanmaktadır (“Z v Finland: ECHR 25 Feb 1997”, 2019). Soruşturma esnasında rızası olmamasına rağmen medikal kayıtlarının polis tarafından hastaneden elde edilmesine karşı dava açan sanık özel hayatının gizliliğinin ihlal edildiğini savunmuştur. AIHM bu davada kişisel verilerin korunmasının yanında hasta mahremiyetine saygı duymanın, tıp mesleğine ve genel olarak sağlık hizmetlerine duyulan güvenin önemini vurgulamış, sağlık verilerinin ifşa edilmesinin söz konusu olamayacağını ve yerel yasaların özel hayatın gizliliğini koruyan 8. madde ile uyumlu hale getirilmesi gerektiğine karar vermiştir.

2000 yılında görülen Rotaru v. Romanya davasının konusu Romanya istihbarat servisinin bir vatandaşın kişisel bilgilerini kaydedip kullanmasının hukuka aykırı olup olmadığıdır (“Rotaru V Romania: Echr 4 May 2000”, 2019). 50 yıldan uzun bir süre önce katıldığı bir eylemin ve yazdığı iki mektubun kayıt altında bulundurulmasının özel hayatının gizliliğinin ihlal edilmesi anlamına geldiğini savunan davacıyı mahkeme haklı bulmuştur. 1987 Leander v. İsveç davasına ve özel hayatın gizliliği ilkesinin kısıtlanabileceği ulusal ve kamusal güvenliğin korunması şartlarına atıf yapılırken diğer yandan devlet kurumları tarafından sistematik şekilde bilgi

toplanması ve bunun saklanması, bilgilerin tutulduğu uzun süre de göz önüne alındığında özel hayatın gizliliğinin ihlal edildiği sonucuna varılmıştır.

2009 Wood v. Metropolis Polis Müdürlüğü davasında halka açık bir alanda fotoğrafları çekilen birey polis teşkilatının özel hayatını ihlal ettiğini iddia etmiştir (“Surveillance of Protests and the Right to Privacy”, 2009). Polis teşkilatı fotoğrafların halka açık bir alanda çekildiğini, bunu sokaktan geçen herhangi bir kişinin yapabileceğini, bu durumun özel hayata müdahale anlamına gelmediğini savunmuştur. Mahkeme kamusal alanda fotoğraf çekmenin tek başına özel hayatı ihlal anlamına gelmeyeceğini belirtmiş fakat bunu polis teşkilatının yapması fotoğrafın saklanıp kullanılacağı anlamına geldiğini söylemiştir. Polis bu eylemi suçun önlenmesi ve kamu güvenliği yararını gözetmek için yaptığını gerekçelendirememiş, bu nedenle mahkeme davacıyı haklı bularak özel yaşamın gizliliğinin ihlal edildiğine karar vermiştir. 2002 Pretty v. Birleşik Krallık davasında katlanılmaz acılar çektiği hastalığından kurtulmak için eşinin yardımıyla hayatına son vermek isteyen başvurucunun kendisine engel olan ulusal mevzuata karşı bu isteğinin özel hayatının bir parçası olarak değerlendirilmesi talebi vardır (Roagna, 2012). Mahkeme bu isteği hukuki açıdan tartışmış ve kararında şu ifadeleri kullanmıştır: “Sözleşme’nin özünü insan onuruna ve insan özgürlüğüne saygı duymak oluşturur. Mahkeme, Sözleşme tarafından korunmakta olan insan hayatının kutsallığını hiçbir şekilde yadsımadan, yaşam kalitesi kavramının 8. Madde kapsamında anlam kazandığı görüşündedir. Uzayan ortalama yaşam süresinin artan tıbbi gelişmelerle birleştiği bir dönemde, pek çok kişi, herkes tarafından kuvvetli bir şekilde benimsenmiş öz ve kişisel kimlik düşünceleriyle çelişen, ileri yaşta hayatını idame etmeye veya ilerlemiş fiziksel ve zihinsel zayıflık durumlarında yaşamaya zorlanmaları hususunda kaygı duymaktadır. Bu davada başvuru, hayatına onursuz ve stres verici bir şekilde son verme olarak düşündüğü halden kaçınma tercihini kullanması hukuken engellenmiştir. Mahkeme henüz, bu durumun Sözleşme’nin 8. Madde’sinde korunan özel hayata saygı hakkına bir müdahale oluşturmadığını kabul etmeye hazır değildir.”

Strasbourg’da görülen Van Kück v. Almanya davasında konu cinsiyet değiştirmenin özel hayatın gizliliğinin bir parçası olup olamayacağıdır (“Van Kück v. Germany”, 2003). Davacı tarafın karşısında cinsiyet değiştirme tedavi ve ameliyat masraflarını karşılamak istemeyen sağlık sigortası kurumu vardır. Kurum cinsiyet değiştirmenin gerekli bir tedavi olarak görülemeyeceğini söylemiş ve mahkeme tarafından haklı

bulunmuştur. Kararı AİHM'ye götüren davacı 2003'te Strasburg'da görülen davada isim ve cinsiyet değiştirmenin özel hayatın gizliliğine saygı kapsamında değerlendirilmesi gerektiği gerekçisiyle haklı bulunmuş ve gerekli davacının talep ettiği belgelerin düzenlenmesine karar verilmiştir.

2004 Von Hannover v. Almanya davasında Monaco kraliyet ailesinin üyesi olan Prenses Caroline'nin yaptığı tatil esnasında magazin muhabirleri tarafından çekilen fotoğraflarının yayınlanması, başvuru tarafından resmi bir görevde olmadığı düşünüldüğünde özel hayatın gizliliği ilkesinin ihlali anlamına geldiği savunularak dava açılmıştır ("Von Hannover v Germany: Echr 24 Jun 2004", 2020). Mahkeme kişinin tanınmış biri olmasına ve kamusal alanda bulunmasına rağmen 8. Madde kapsamında özel yaşamına saygı duyulmasını beklemek konusunda haklı olduğu kararlaştırılmış ve fotoğrafları özel hayata ölçüsüz bir müdahale olarak değerlendirmiştir.

2009 Gardel v. Fransa davasında mahkeme, tecavüz suçundan hükümlü olan mahkumun kişisel verilerinin ulusal veritabanında saklanıp işlenmesine ve bu verilerin silinmesine dair başvurunun yaptığı başvuruyu işlenen suç ve kamu çıkarlarını göz önünde bulundurarak reddetmiş ve davanın kapsamının özel yaşamın gizliliği ilkesinin uygulanmayacağı istisnai durumlardan olduğu kararına varmıştır ("Inclusion in National Sex Offender Database Did Not Infringe The Right To Respect For Private Life", 2009).

2009'da görülen Reklos ve Davourlis v. Yunanistan davasında davacı tarafın bebeklerinin doğumu esnasında kendilerinden izin alınmadan fotoğraflarının çekilmesinin özel yaşamlarının gizliliğinin ihlal edildiği savıyla açtıkları davada mahkeme tarafından haklı bulunmuşlardır ("Case of Reklos and Davourlis v. Greece", 2009).

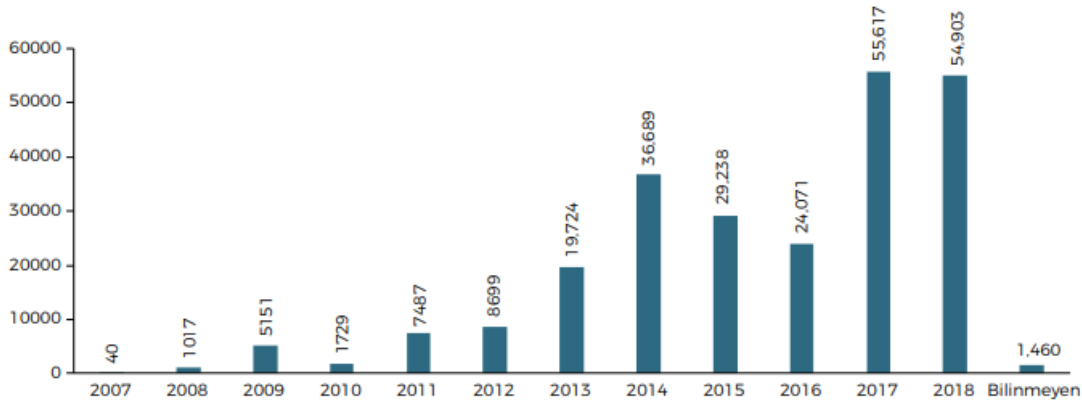
1978 yılında çıkarılan Yabancı İstihbarat Denetimi Kanunu (Foreign Intelligence Surveillance Act), FISA, ABD vatandaşlarının ülke içindeki iletişimlerinin izlenmesini düzenlemektedir. Bu iletişim kanalları telefon ya da radyo olarak belirlenmiştir. Kişilerin dinlenmesi için terör suçundan şüpheli bulunması gerekmektedir, bunun dışında hakim kararının alınması şartı aranmıştır. Başlangıçta az sayıda alınan bu karar (yılda ortalama beş yüz), 1995 yılında ortalama sekiz bin kere alınmaya başlamıştır. 1968 yılında ortalama 400 bin civarında olan dinlenen

konuşma sayısı 1994 yılında 1137 yargıç kararıyla verilen izin 2.35 milyon konuşmanın dinlenmesiyle sonuçlanmıştır(Yüksel, 2012, s.48).

2.3 Türkiye’de Gözetim Uygulamaları ve Hak İhlalleri

İfade Özgürlüğü Derneği’nin bünyesinde Prof. Dr. Yaman Akdeniz ve araştırmacı Ozan Güven tarafından hazırlanan Türkiye’den Erişime Engellenen Web Siteleri, Haber ve Sosyal Medya İçeriklerinin Analiz Raporu Türkiye’deki internet sansürü uygulamalarını değerlendirmektedir(Akdeniz & Güven, 2019, s.1).

Türkiye’den 2018 yılı sonu itibarıyla 245.825 web sitesi ve alan adına erişimin engellendiği tespit edilmiştir (Akdeniz & Güven, 2019, s.36). Erişime engellenen alan adlarının yıllara göre dağılımı Şekil 2.6’da şu şekilde gösterilmiştir:



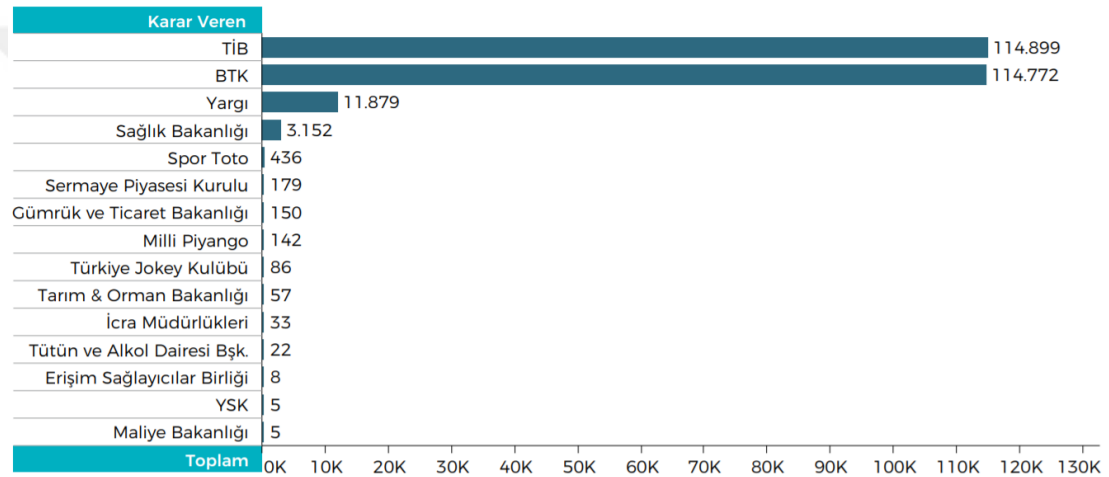
Şekil 2.6: 2007-2018 Yılları Arası Erişime Engellenen Alan Adı Sayıları (Akdeniz & Güven, 2019, s.36).

Türkiye’de artan gözetim uygulamaları ve erişime engellenen web sitelerinin sayılarından çıkarılabilecek sonuç, devletin giderek iletişim özgürlüğünü kısıtlama eğilimde olduğudur. 2013 yılına kadar bu sayı on binin altında iken günümüzde elli binin üstüne çıkmıştır.

Şekil 2018 öncesinde erişime engellenen 190.922 web sitesinden 177.515 tanesi TİB ve sonrasında BTK Başkanı tarafından 9227 alan adı ve web sitesi sulh ceza hakimlikleri, savcılıklar ve mahkemeler tarafından erişim engellenmiştir (Akdeniz & Güven, 2019, s.2). Şekil 2.7’de engellenen alan adlarının engelleme karara veren kurumlara dağılımı verilmektedir. 5651 nolu Kanun kapsamında BTK başkanı tarafından alınabilmesi sansür uygulamasının kurumsallaşmasına neden olmuştur. 671

nolu KHK ile kapatılmadan önce TİB'in ve sonrasında onun yerini alan BTK'nın başına Cumhurbaşkanlığı tarafından atama yapıldığı düşünüldüğünde internet üzerinde geniş yetkilere sahip bu idari kurumların yetkilerini siyasi saiklerle, gözetim ve sansür uygulamaları için kullanmaları eşyanın tabiatına aykırı olmayacaktır.

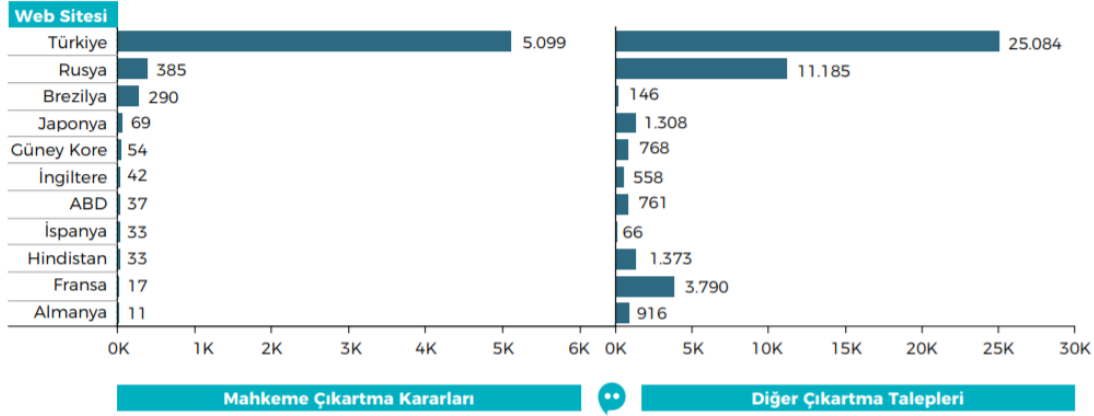
Ülke içinde engellenen alan adlarının yanında engellenmesi uluslararası kamuoyunda tepkilere neden olacak ünlü web sitelerine içerik çıkarma talebi gönderilmektedir. Bu içerik çıkarma taleplerine olumlu yanıt vermeyen Twitter 20 Mart 2014 tarihinde ülke çapında topyekün olarak engellenmiş, yapılan bir dizi görüşmenin ardından Twitter ülke bazlı içerik gizleme politikasını ('country withheld content policy') Türkiye'de devreye sokmuştur (Akdeniz, 2015).



Şekil 2.7: Erişime Engellenen Web Sitelerinin Karar Veren Kurumlara Göre Dağılımı (Akdeniz & Güven, 2019, s.2).

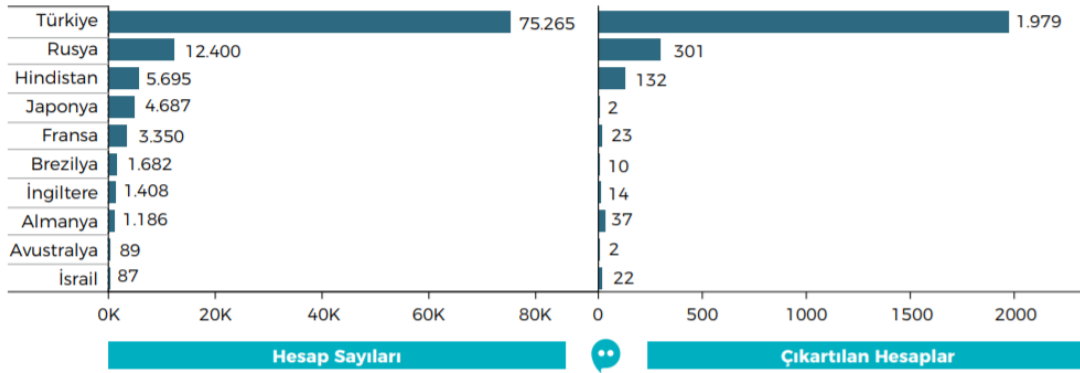
Twitter'ın engellenmesinin hemen sonrasında sms ve vpn gibi araçları kullanan kullanıcılar yasağı ve sansürü delmiş 1 saat içinde beş yüz binin üzerinde tweet atarak #twitterblockedturkey etiketi dünya çapında TT olmuştur (Johnson, 2014). Anayasa mahkemesi 2 Nisan 2014 tarihinde Twitter'ın tamamen yasaklanmasının anayasanın 26. Maddesi uyarınca ifade özgürlüğüne aykırı olduğuna karar vermiş ve erişim engelini kaldırmıştır ("Twitter yasağı kalktı", 2014).

Twitter tekrar toplu bir engellemeye uğramasa da Twitter tarafından yayınlanan şeffaflık raporunda yer alan ve Şekil 2.8'de görülen dramatik tablo site üzerindeki sansür isteğinin kalkmadığını göstermektedir. Dünya genelinde yapılan bu değerlendirmede Türkiye açık ara lider pozisyonundadır.



Şekil 2.8: 2012-2018 Twitter Şeffaflık Raporlarında Mahkeme Kararları Ve Diğer Çıkartma Talepleri (Akdeniz & Güven, 2019, s.25).

Şekil 2.9’da gördüğümüz veriler ise Türkiye’den Twitter’a iletilen engellenmesi istenen hesap sayılarına aittir. Toplam 75.265 engelleme isteğine Twitter’ın cevabı bunların yalnızca 1979’unu Türkiye’de engellemek olmuştur.



Şekil 2.9: 2012-2018 Twitter Raporlarında Çıkarılması Talep Edilen ve Çıkarılan Hesap Sayıları(Akdeniz & Güven, 2019, s.25).

Ulusal ve uluslararası kamuoyunda çokça tartışılan bir diğer sansür uygulaması ise Wikipedia’nın erişime kapatılması olmuştur. 29 Nisan 2017’de alınan kararla Wikipedia’ya Türkiye’den erişim engellendi (“Wikipedia engellendi”, 2017). Diğer pek çoğu gibi bu karar da yargı yoluyla değil BTK’nın idari tedbiriyle alınmıştı. BTK’nın web sitesinde yaptığı açıklama şu şekildeydi: “5651 sayılı Kanun uyarınca yapılan teknik inceleme ve hukuki değerlendirme sonucunda bu İnternet sitesi (wikipedia.org) hakkındaki Bilgi Teknolojileri ve İletişim Kurumu’nun 29/04/2017 tarih ve 490.05.01.2017.-182198 sayılı kararına istinaden Bilgi Teknolojileri ve İletişim Kurumu tarafından İDARİ TEDBİR uygulanmaktadır.” (“Mahkeme kararı olmaksızın: Wikipedia’ya ‘imaj’ gerekçeli erişim engeli geldi”, 2017). Böylece her

kullanıcının makaleleri düzenleyip katkıda bulunabildiği dünyanın en büyük açık ansiklopedisi olan Wikipedia “bazı terör örgütleriyle Ankara'yı ilişkilendiren içerikler” nedeniyle kapatılmış oluyordu (“Wikipedia erişim yasağı AİHM’de: Türkiye’nin uyguladığı yasağın nedeni ne, hangi adımlar atıldı?”, 2019). Yaklaşık 2.5 yıllık bir sansürün ardından Anayasa Mahkemesi’nin 26 Aralık 2019 tarihli kararının 15 Ocak 2020 tarihinde Resmi Gazete’de yayınlanması sonucu erişim yasağı kalkmış oldu (“Wikipedia’ya erişim açıldı”, 2020). Anayasa mahkemesi kararını gerekçelendirirken “Demokratik Toplum Düzeninin Gereklerine Uygunluk” ilkesine vurgu yapmış ve şu açıklamayı paylaşmıştır:

“Wikipedia; dünya üzerinde milyonlarca kullanıcısı olan ve sistemde yer alan içeriklerin kullanıcılar tarafından oluşturulduğu bir internet platformudur. Wikipedia’ya yeni bir içerik eklenmesi veya var olan içeriğin zenginleştirilmesi, içeriklerde bulunan bazı bilgilerin güncellenmesi, bazılarının silinmesi gibi değişiklikler sistemde kayıtlı, editör olarak adlandırılan kullanıcılar tarafından yapılmaktadır. Çevrim içi ansiklopedi olarak nitelendirilen ve her alanda önemli miktarda bilgi barındıran Wikipedia, her gün milyonlarca kişi tarafından ziyaret edilmektedir. Sitede yer alan arama butonu sayesinde bilgi edinilmek istenen konu hakkındaki içerikler kısa sürede bulunabilmekte, iç bağlantılar aracılığıyla da aranılan konu ile alakalı daha fazla bilgiye erişilebilmektedir. Böyle bir platformun bilginin herkes tarafından ulaşılabilir olmasına sağladığı katkı tartışmasızdır. Dolayısıyla bilgi alma ve verme özgürlüğüne hanel gelmemesi için Wikipedia’da yer alan içeriğe erişimin engellenmesi yoluyla yapılacak bir müdahalenin demokratik toplumda gerekli olduğu ilgili ve yeterli bir gerekçe ile ortaya konulmalıdır” (Vikipedi, 2020).

2.4 Hukuki Çerçeve

İletişim (Latince communicare’den "paylaşmak" anlamına gelir), karşılıklı olarak anlaşılan işaretler, semboller ve gösterge bilimsel kurallar kullanılarak anlamların bir varlık veya gruptan diğerine aktarılması eylemidir (Yüksel, 2012).

Sözsüz iletişim, bilginin dilsel olmayan temsiller biçiminde iletirme süreçlerini tanımlar. Sözsüz iletişim örnekleri arasında dokunsal iletişim, kronolojik iletişim, jestler, vücut dili, yüz ifadeleri, göz teması gibi iletişimler vardır. Sözsüz iletişim aynı zamanda bir mesajın niyeti ile de ilgilidir. Niyet örnekleri, el sallama veya göz kırpması

gibi gönüllü ve kasıtlı hareketlerin yanı sıra terleme gibi istem dışı hareketlerdir (“Types of Body Language”, 2007).

Sözlü iletişim, bir mesajın sözlü veya yazılı iletimidir. İnsan dili, sembollerin işlendiği bir semboller sistemi ve gramerler (kurallar) olarak tanımlanabilir. Dil kelimesi ayrıca dillerin ortak özelliklerini ifade eder.

Her türlü sinyal, sembol, ses ve görüntü iletimi ve iletme araçları hukuki bir çerçeve altında incelenmektedir.

2.4.1 Avrupa insan hakları sözleşmesi’nde özel hayatın gizliliği

Avrupa İnsan Hakları Sözleşmesi Madde 8’de özel yaşamın gizliliğine dair şu madde yer alır: “Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.” (“Avrupa İnsan Hakları Sözleşmesi”, 2010). Bu hakkın kısıtlanabileceği durumlar ulusal ve kamusal güvenliğin, suç işlenmesinin önlenmesi gibi şartlardır: “Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.” (“Avrupa İnsan Hakları Sözleşmesi”, 2010).

İstisna maddelerinin kapsamı dışında kalan mahkeme kararlarınca oluşturulmuş içtihatlarla göre kişinin özel ve aile yaşamına, konuta ve haberleşme gizliliğine müdahale olarak değerlendirilen durumlar şunlardır (Roagna, 2012): “

- Çocukların ailelerinden alınması ve devlet veya koruyucu aile bakımının altına alınması
- Üst ve ev araması
- Telefon dinleme ve genel olarak, kullanılan araca bakılmaksızın, haberleşmenin izlenmesi
- Yerlerinden edilen kişilerin evlerine dönmelerine izin verilmemesi
- Tutukluların haberleşmesinin durdurulması veya denetlenmesi
- Bireyler hakkında bilgi toplama ve saklama
- İmar planı kararları

- İhraç etme kararları
- Şikâyetçinin özel hayatına müdahale teşkil eden belirli bir kanuni rejimin yürürlükte kalması
- Saldırgan bir kişiye karşı koruma sağlamayı amaçlayan mahkeme kararının uygulanmaması
- Bir işçinin özel hayatıyla ilgili sebeplerle işten çıkartılması
- Mahkûm edilen bir kişinin, polisin izniyle görüntülerinin yayınlanması
- Mahkûmun bulunduğu hücrenin civarında, atık alanından yayılan şiddetli bir kokunun olması
- Yeni doğan bir bebeğin, ebeveyninin izni olmadan fotoğraflarının çekilmesi ve negatiflerinin elde bulundurulması
- Devlet hastanelerinde tıbbî hata sonucu ortaya çıkan bedensel zararların tazminini sağlayacak bir yolun bulunmaması
- Gizli servis tarafından tutulan kişisel dosyalara erişim sağlayan prosedürün etkin olmaması
- Başvurucunun rızası olmadan veya karşıt kültürel inanışlarına rağmen, etnik kökeninden ötürü kendisine zorla tıbbî tedavi uygulanması
- Tıbbî bilgiler dâhil, kişisel verilere izinsiz erişim
- İflas siciline bir isim girme
- Belli bir yerde daimi olarak ikamet edenlerin bulunduğu listeden kişinin isminin iptalini elde etmesinin imkânsızlığı
- Bir kişinin kimlik belgelerinin yenilenmesi veya iade edilmesi talebinin reddi
- Yerleşik bir göçmenin sınır dışı edilmesi”

2.4.2 Anayasamızda özel hayatın gizliliği

Anayasamızda özel yaşamın gizliliğine hak olarak yer verilmiş ve düzenlenmiştir. Anayasanın 20. maddesine göre “Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.” (“Türkiye Cumhuriyeti Anayasası”, 1982). Özel yaşamın gizliliğinin kısıtlanacağı durumlar milli güvenlik, kamu yararı, suç önlenmesi gibi şartlara

bağlanmış ve anayasada şu şekilde yer almıştır: “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 üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırk sekiz saat içinde açıklar; aksi hâlde, el koyma kendiliğinden kalkar.” (“Türkiye Cumhuriyeti Anayasası”, 1982).

2.4.3 Türk hukukunda durum

Dünyada yaşanan teknolojik gelişmeler sonucu bilgisayar, telefon gibi araçların internet kullanımıyla beraber günlük yaşamın bir parçası haline gelmesi ve bilişim alanındaki suçların yaygınlaşmasıyla kanun ve yasalarda değişiklik ihtiyacı doğmuş ve bu doğrultuda TCK ve çeşitli kanunlarda düzenlemeler yapılmıştır. Bilişim hukuku alanında ve toplu gözetimle ilgili olabilecek Türkiye’de çıkarılan kanunlar aşağıda sıralanmıştır (Adalı, 2016, s.262): “

- Türk Ceza Kanunundaki ilgili maddeler (5237 sayılı)
- Ceza Muhakemesi Kanunundaki ilgili maddeler (5271 sayılı)
- Fikir ve Sanat Eserleri Kanunu (5846 sayılı)
- Elektronik İmza Kanunu (5070 sayılı)
- İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hk. Kanun (5651 sayılı)
- Kişisel Verilerin Korunması Kanunu (6698 sayılı)”

Bu kanunlar içinde bireyleri toplu gözetime karşı korumaya en uygun araçlar TCK’nun bilişim suçları altında düzenlenen maddeleri (TCK m. 132 vd) ve Kişisel Verilerin Korunması Kanunu’dur.

Kişilerin Verilerin Korunması Kanunu (KVKK) kapsamında kişisel veri “Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlanmaktadır (“Kişisel Verilerin Korunması Kanunu”, 2016, s.1). Bu bilgiye göre kişinin adı, adresi, doğum tarihi, medeni hali, tabiiyeti, mesleği, görüntüsü, kanaatleri, fotoğrafı,

elektronik posta adresi, banka bilgileri, bilgisayarının IP adresi, kimlik, emeklilik, kurum sicili ve vergi numarası, parmak izi, eğitim bilgileri, sağlık verileri, telefon mesajları, telefon rehberi, mail, facebook, twitter gibi sosyal paylaşım sitelerinde yazdığı veya paylaştığı yazı, fotoğraf, ses ve görüntü kayıtları “kişisel verisi” olarak belirtilebilir (Dağsalı, t.y.). Kişisel verilerin korunması Anayasasının özel hayatın gizliliğini düzenleyen 20. Maddesinde de şu şekilde düzenlenmiş ve anayasal bir hak olarak kabul edilmiştir (“100 Soruda Kişisel Verilerin Korunması Kanunu”, 2018, s.10):

“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel verileri 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.”

Kişisel Verilerin Korunması Kanunu’nun temel ilkeleri şunlardır: “Hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.” (Kişisel Verileri Koruma Kurumu, t.y., s.1).

Bu ilkeler doğrultusunda kişisel verilerin işlenebilmesinin şartları açık şekilde tanımlanmış, bu şartlardan herhangi bir tanesinin sağlanması durumunda kişisel verinin işlenebileceği belirtilmiştir (“100 Soruda Kişisel Verilerin Korunması Kanunu”, 2018, s.41): “

1. İlgili kişinin açık rızasının varlığı
2. Kanunlarda açıkça öngörülmesi,
3. 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,
4. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

5. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
6. İlgili kişinin kendisi tarafından alenileştirilmiş olması,
7. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
8. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.”

KVKK kapsamında kullanımı bu ilkelere ve şartlara bağlanan kişisel veri üzerinde birey çok daha geniş kontrol imkanına kavuşmuştur. Kişisel verinin kapsamı genişletilmiş, verinin kullanabileceği şartlar netleştirilmiş, devlet ve şirketlerin gözetimine karşı bireye ciddi bir hukuki koruma sağlanmıştır.

3. PIPA, SOPA, ACTA, CISPA GÖZETİM VE SANSÜR KISKACINDA İNTERNET

İnternetin gözetim ve sansür uygulamalarıyla kontrol altına alınmaya çalışılması yalnızca ülkemize özgü bir durum değildir. Çeşitli ulusal ve uluslararası yasalar ve anlaşmalarla internet üzerindeki gözetim ve sansür kalıcı hale getirilmeye çalışılmaktadır. Amerika Birleşik Devletleri bu alandaki girişimleriyle öne çıkmaktadır.

3.1 PIPA (Protect Intellectual Property Act – Fikir Eserlerinin Mülkiyetinin Korunması Yasası)

Senatörler Patrick Leahy, Orrin Hatch ve Chuck Grassley tarafından 12 Mayıs 2011 tarihinde ABD senatosuna sunulmuştur (Carle, 2011). Yasa tasarısı yasaya karşı yapılan eleştirilerin ve eylemlerin sonucunda oylama yapılmadan ertelenmiştir.

PIPA interneti düzenleyen ve sansürün önünü açacak önemli maddeler getirmekteydi. ABD şirketleri ve ABD hükümeti tarafından telif hakkını ihlal ettiği şikayetinde bulunan internet sitesi ABD’de bulunmasa dahi ABD mahkemelerinden alınan kararla siteye erişim kapatılabilecekti (Strickland, 2012).

ABD mahkemelerinden çıkan kararla sitenin ABD’den elde ettiği gelir kesilebilecekti (Strickland, 2012). Yasayla sitelerin üzerinde ekonomik bir kıskaç oluşturulmak isteniyordu.

Blog sayfaları, arama motorları, web siteleri telif hakkı ihlali yapıldığı söylenen içerikten mesul olacak ve bu içerikleri engellemeleri gerekecekti (Carle, 2011).

İnternet servis sağlayıcıları belirtilen internet sitesine uygulanacak olan erişime kısıtlama, erişime kapatma gibi önlemleri hızlı bir şekilde yapabilmek adına gerekli teknik altyapıyı oluşturmakla yükümlü olacaklardı. Ek olarak site sahipleri ilgili siteye yönlendirmede bulunan linkleri kaldırmak zorunda kalacaklardı (“PIPA Law”, 2011).

Yasa internetin paylaşımcı ve demokratik yapısına karşı özel şirketlere büyük bir sansür gücü veriyor ve bunu sağlarken yasal prosedürü işlevsizleştiriyordu. Reddit, Twitter, Facebook, Youtube, Ekşi Sözlük gibi kullanıcı paylaşımlarıyla değer kazanmış ve işlemekte olan siteler tekil kullanıcıların paylaşımlarından sorumlu tutulacak ve bu sitelerin kapanmasına varan sonuçlar doğurabilecekti. Bu yolla devlete kısıtlamanın ötesinde bir sansür hakkı tanınıyor, devlet makamları ve büyük şirketler hukuk aracılığıyla internet servis sağlayıcılarının, site sahiplerinin ve en önemlisi tekil kullanıcıların haklarını tırpanlayacak bir güç elde ediyordu.

3.2 SOPA (Stop Online Piracy Act – Çevrimiçi Korsanlığı Durdurma Yasası)

Senatör Lamar Smith tarafından 26 Ekim 2011 tarihinde ABD temsilciler meclisine sunulmuştur (Kang, 2011). Çevrimiçi Korsanlığı Durdurma Yasası ve Fikir Eserlerinin Mülkiyetinin Korunması Yasası birbirini tamamlayacak iki yasa tasarısı olarak hazırlanmıştı. Yasanın destekçileri ve karşı çıkanlar iki ayrı kampa ayrılmışlardı. Yasayı destekleyenler Microsoft, Sony, Universal Music gibi telif hakkından büyük gelirler elde eden şirketlerdi. Yasanın karşısında yer alanlar ise telif hakları sorunlarıyla karşı karşıya kalabilecek olan Google, Twitter, Facebook, Yahoo gibi büyük şirketlerdi. Fakat ne SOPA'yı savunanların gerçekten eser sahibi çıkarlarını savunduğunu, ne de yasaya karşı çıkanların ifade özgürlüğünü, demokrasiyi ve internetin çoğulcu yapısını savunma gibi bir amaçlarının olduğunu görürüz. Her iki grup da kendi ekonomik çıkarları doğrultusunda tavır almıştır. Bunun yanında yasaya karşı çıkan toplumsal muhalefet de eylemliliğe başlayarak önemli bir kamuoyu baskısı oluşturdu. 18 Ocak 2012 tarihinde Wikipedia İngilizce yayın yapan sitesine 24 saatlik bir karartma uyguladı ("Websites blackout in SOPA anti-piracy protest", 2012). Wikimedia vakfının yöneticisi Sue Gardner (2012) tarafından yapılan yazılı açıklamada şu ifadeler yer verildi: "Karartma ABD senatosunda görüşülen PIPA ve kongredeki SOPA yasalarına karşı bir eylemdir. Eğer bu yasalar kabul edilirse özgür ve açık internete, Wikipedia da dahil ciddi bir zarar verecektir. Biz herkesin düşünce özgürlüğü ve ifade özgürlüğü hakkını destekliyoruz. Bunun için ödeme yapmasalar bile herkesin çok çeşitli konularda eğitim materyallerine erişimi olması gerektiğini düşünüyoruz. Bilginin engellemeden paylaşılacağı özgür ve açık bir İnternete inanıyoruz. SOPA ve PIPA gibi önerilen yeni kanunların ve ABD içinde ve dışında tartışılan diğer benzer yasaların, genel halkın çıkarlarını ilerletmediğine inanıyoruz.

Bu neden sadece ABD’den ziyade küresel bir eylem? Gerçek şu ki, SOPA’nın gittiğini düşünmüyoruz ve PIPA hala oldukça aktif. Dahası, SOPA ve PIPA sadece daha geniş bir sorunun göstergesidir. Tüm dünyada, çevrimiçi korsanlıkla mücadele etmek ve İnternet’i çevrimiçi özgürlüklere zarar veren başka şekillerde düzenlemek için tasarlanan mevzuatın gelişimini görüyoruz. Endişemiz SOPA ve PIPA’nın ötesine uzanıyor: bunlar sadece sorunun bir parçası. İnternet’in her yerde, herkes için özgür ve açık kalmasını istiyoruz.”

Bu eyleme Wikipedia’nın yanında binlerce internet sitesi de sayfalarını karartarak destek vermiştir.

İnternetin dahi çocuğu olarak adlandırılan Aaron Swartz SOPA yasa tasarısına karşı yürütülen mücadelede aktif olarak rol alıyordu. MIT’nin veri tabanını hackleyerek akademik makaleleri ücretsiz olarak halka açan ve bu nedenle 1 milyon dolar para, 35 yıl hapis cezasıyla yargılanırken trajik şekilde hayatına son veren Aaron Swartz SOPA’ya karşı nasıl mücadele verildiğini ve yasanın nasıl geri çekildiğini kendi kaleminden şöyle yazmıştı(Assange, Appelbaum, Müler-Maguhn & Zimmermann, 2013, s. 120): “Hükümetin gidip birisine yasadışı bir materyali kaldırmasını söylemesi değildi mevzu, internet sitelerinin tümüyle kapatılması söz konusuydu. Kısacası, Amerikan vatandaşlarının kimi gruplarla iletişim kurması tümüyle engelleniyordu”

Swartz yasanın devlet eliyle nasıl sansür için kullanabileceğini çarpıcı bir biçimde şöyle dile getiriyor (Assange, Appelbaum, Müler-Maguhn & Zimmermann, 2013, s. 121): “İşin ürkütücü yanı tam da buradaydı, çünkü bildiğiniz gibi, telif hakkı her yeri kuşatmış durumda. WikiLeaks’i kapatmak mı istiyorsunuz, buna gerekçe olarak sitede çok fazla pornografi bulunuyor diyemezsiniz, ama WikiLeaks’in telif haklarını ihlal ettiğini ileri sürerseniz işiniz kolaylaşır, çünkü her şey telif hakkıyla donatılmış durumdadır. Bu konuşma, yani şu an size yaptığım bu konuşma, ağzımdan çıkan şu sözler bile telif hakkına tabi. Günümüzde bir şeyi yanlışlıkla kopyalamak ise işten bile değil. Nitekim COICA yasasının en önde gelen destekçilerinden Cumhuriyetçi senatör Orrin Hatch, kendisine ait Senato sayfasına yasaya aykırı biçimde bir dizi kod kopyalamış. Öyleyse, Orrin Hatch’in Senato sayfasının bile telif yasasını ihlal ettiği ortaya çıkıyorsa, içimizden birine kancayı takacak bir şeyler bulmaları ihtimalinin ne olduğunu siz tahmin edin!”

Swartz verilecek geniş yetkilerin yalnızca ABD hükümetine değil dev şirketlere verileceğini de ifade ediyor: “İlk haliyle yasa, internet sitelerini kapatma yetkisini yalnızca hükümete veriyordu, oysa bu senatörler dünya üzerindeki herhangi bir şirketin de bir internet sitesini kapatma yetkisine sahip olmasını talep ediyorlardı” (Assange, Appelbaum, Müler-Maguhn & Zimmermann, 2013, s. 123)

Schwartz Sopa’ya karşı verilen toplu mücadeleyi ise şöyle anlatıyor (Assange, Appelbaum, Müler-Maguhn & Zimmermann, 2013, s. 128): “Wikipedia karartma uyguladı. Reddit karartma uyguladı. Craigslist karartma uyguladı. Washington’daki meclis binasının telefon hatları resmen telefon yağmuruna tutuldu. Meclis üyeleri daha birkaç gün öncesine kadar savunmakta oldukları yasadan desteklerini çektiklerini açıklamak için birbirleriyle yarışa girdiler. Olanlar düpedüz saçmalıktı. O dönem yayınlanan bir tablo durumu gayet iyi özetliyor. Bir tarafında “14 Ocak “yazılı ve altında yasayı destekleyenlerin isimlerinden oluşan upuzun bir liste var ve yalnızca bir-iki kişi yasaya karşı; diğer tarafta ise “15 Ocak” yazılı ve burada resim tersine dönmüş durumda — herkes yasaya karşı çıkıyor, yalnızca bir-iki isim desteğinde hâlâ ısrar ediyor.”

Yasa ABD de çıkmasına rağmen çeşitli şekillerde yorumlanarak ABD dışındaki ülkelerdeki kullanıcıları da etkileyebilecek; bu uluslararası hukukta kabul edilemeyecek bir durum olsa da söz konusu ülke ABD ve büyük, şirketlerin çıkarları olduğunda uluslararası hukukun nasıl bertaraf edilebileceğini gösteren bir örnektir.

SOPA yasa taslağında sunulan değişikliklere göre telif hakkı ihlali yaptığı söylenen siteler yanında bu siteleri barındıran servis sağlayıcılar da sorumlu hale geliyordu. Servis sağlayıcılar bu sitelerin IP adreslerini engellemekle yükümlü olacaklardı. Arama motorlarının telif hakkı ihlali yapan siteleri arama sonuçlarından çıkarmaları yasal bir yükümlülük olacaktı. Online ödeme sistemleri ABD vatandaşlarının bu sitelerde ödeme işlemi yapmasını önleyecek, reklam şirketleri reklamlarını bu siteden kaldırmak zorunda kalacaklardı (“Tribe Legis Memo on SOPA”, 2011). Görüldüğü üzere bu önlemler yalnızca ihlali yapan siteleri değil diğer birçok hizmet sağlayıcıyı da yasal yükümlülük altına sokuyordu. Hak ihlali yapan bir siteyi arama sonuçlarında gösteren Google’a erişim kısıtlanabilirdi. Twitter, Ekşi Sözlük gibi sosyal paylaşım sitelerinde paylaşımda bulunan kullanıcıların telif hakkı olan bir esere dair yaptıkları paylaşımlar tüm sitenin sansüre uğramasına, Youtube’a yüklenen bir video yine sitenin kapanmasına neden olabilirdi. Yasa bunların yanında açık kaynak kodlu, özgür

yazılım dünyasını da hedef haline getiriyordu (Mcsherry & Eckersley, 2011). Yazılımını geliştirdiğiniz ve ücretsiz şekilde tüm dünyadaki kullanıcıların kullanımına sunduğunuz ürünler kolay bir şekilde hali hazırda büyük şirketlerce parselenmiş olan telif haklarının ihlali kapsamında değerlendirilebilirdi.

3.3 ACTA(Anti Counter-Feiting Trade Aggrement – Sahteciliğe Karşı Ticaret Anlaşması)

ACTA, telif ve patent hakkı içeren eserlerin korsan yollarla satışı üretimi ve tüketimi halinde yeni yasal düzenlemeler getiren uluslararası çok taraflı bir sözleşmedir (Solon, 2012).

Sahteciliğe Karşı Ticaret Anlaşması'nın önemi fikri mülkiyet ihlallerinin dijital ortamda da diğer alandaki mülkiyet hakkı ihlalleri ile eş değer tutulması ve bunun uluslararası bir konsensüs ile kabul edilmesidir. Anlaşma ile SOPA ve PIPA yasalarındakine benzer olarak servis sağlayıcılara yükümlülükler getirilmektedir. Anlaşmayı savunanlar korsanla mücadele için devletler arası bir iş birliğinin ve uluslararası mücadelenin şart olduğunu belirtirken, karşı cephe anlaşmayla özgür yazılımın sekteye uğratılacağını, kaybedenin bilim, teknoloji ve toplum, kazananın büyük şirketler olacağını söylüyordu. Kendilerini özgür yazılım felsefesini kucaklayan ve bu felsefeye uyan tüm ürün, teknoloji, oluşum ve platformlara destek olmayı hedefleyen bir topluluk olarak tanımlayan ("Linux Kullanıcıları Derneği", t.y.) Linux Kullanıcıları Derneği tarafından yapılan açıklamada ACTA ile ilgili şu ifadeler yer verilmiştir ("ACTA Tehdidi", 2011):

"ACTA (The Anti-Counterfeiting Trade Agreement), yani "Ticarette Sahteciliğin Önlenmesi Sözleşmesi", 2007 yılından bu yana başta Müzik ve Film endüstrisinin devleri olmak üzere tüm telif hakkı lobilerinin zorlamasıyla ABD'nin uluslararası platforma taşıdığı bir anlaşmadır. ACTA internet, dolayısıyla dijital ortamda kullanıcılara ve servis sağlayıcılara ise birçok kısıtlama ve sorumluluk getirmektedir. Tüm kullanıcıları potansiyel "sahteci" yerine koyan anlaşma "bu potansiyele karşı" her türlü önlem ve cezaya uluslararası ölçekte hukuki zemin hazırlamakta. Öte yandan ACTA sadece interneti kısıtlamıyor. Çok temel/gündelik kullanılan jenerik ilaçlar, temel besin üretimi için gerekli tohumlar bile ACTA'nın getireceği düzenlemelerle rahatça dolaşamayacak, yasaklanabilecek.

İnternet kullanıcılarına sahip oldukları dijital donanım, yazılım ya da içerikler için her türlü tedbiri alma yükümlülüğü getirilmektedir. Servis sağlayıcılar için altyapılan üzerinden gerçekleşen ihlalleri ve ihlali gerçekleştiren kullanıcıları ilgili makamlara bildirme zorunluluğu öngörülmektedir. Bu da ancak içerik dahil tüm trafiğimizin gözetlenmesi ve takip edilmesi ile mümkündür. Kullanıcıların kişisel verileri ve özel yaşamlarının gizliliği büyük tehdit altındadır.

2010 yılından gizlice yürütülen müzakereler sonucunda ilk olarak ABD, Japonya, Kanada, Yeni Zelanda, Singapur ve Güney Kore, ACTA anlaşmasını imzalamıştır. Geçtiğimiz Ocak ayında da Avrupa Parlamentosu'nda yapılan gizli oylama ile 27 Avrupa Birliği ülkesinin 22'si bu anlaşmayı kabul etmiştir.

İnternet temel bir insan hakkıdır. İnternete müdahale, temel hak ve özgürlüklerimize müdahaledir. Kabul edilemez. Bu müdahaleyi bir günlük geçici karartmayla protesto ediyoruz.. İnternet yaşamdır, Sansürlenemez !”

Birçok AB ülkesinde protestolara neden olan yasa karşısında üye ülkeler geri adım atmış ve yasa Temmuz 2012’de Avrupa Parlamentosu’nun büyük çoğunluğu tarafından reddedilmiştir (39’a karşı 478 ret, 165 çekimser) (Whittaker, 2012).

3.4 CISPA (Cyber Intelligence Sharing Protection Arc – Siber İstihbarat Paylaşımı ve Korunması Yasası)

30 Kasım 2011 tarihinde Micheal Rogers tarafından senatoya sunulmuş yasa tasarısıdır (“H.R.3523 - Cyber Intelligence Sharing and Protection Act”, 2012) .

ABD’de her iki partiden yasaya karşı çıkışlar olmuştur. Cumhuriyetçi Ron Paul Silikon Vadisi’nde yaptığı açıklamada tarafından yasa teklifi özgür internete yapılan son saldırı ve Büyük Birader yasası olarak nitelendirilmiş, SOPA’ya karşı örgütlenen toplumsal muhalefetin bu yasa için de gerekli cevabı vereceğini umduğunu söylemiştir (McCullagh, 2012). Akademisyenler ve deneyimli mühendislerden oluşan bir grup aktivist kongreye yazdıkları açık mektupta yasaya karşı olduklarını şu ifadelerle açıklamışlardır:

“Bizler güvenliği son derece ciddiye alıyoruz, fakat şuna gerçekten inanıyoruz ki, güçlü bir bilgisayar ve ağ güvenliği için internet kullanıcılarının gizliliğini ve yurttaşların haklarını kurban etmeniz gerekmez. Sizlerden teklifin yasalaşmasını reddetmenizi bekliyoruz:

- Ağ güvenliği saldırılarını, tehdit göstergelerini ve karşı önlemleri tanımlamak için belirsiz bir dil kullanılması, zararlı olmayan çevrimiçi etkinliklerin siber güvenlik tehdidi olarak yorumlanmasına neden olur.
- Siber güvenlik aksiyonları, bireyin haklarını koruyan İletişimin Gizliği Yasası(the Wiretap Act), İletişimin Saklanması Yasası(the Stored Communications Act), Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Yasası'ndan (Computer Fraud and Abuse Act) muafır.
- Bireylerin mahremiyetini ihlal etseler bile şirketlere karşı yasal sorumluluk verilmemektedir.
- Siber güvenlik için toplanmasına rağmen, toplanan veri ilgisi olmayan suçların araştırılmasında kullanılabilecektir.

Ağlarımızı daha güvenli yapma çabanızı takdir ediyoruz, fakat üstte saydığımız nedenlerle bu taslak bizi daha güvenli hale getirmek için atılan bir adım olmaktan ziyade mahremiyete ve sivil özgürlüklere zarar verecek büyük bir hata olacaktır” (Open Letter, t.y.).

Aktivist Reitman'ın yaptığı değerlendirmeye göre (2012) tasarı yasalaşırsa şirketler elektronik iletişimimizi gözetleyebilecek, milyonlarca internet kullanıcısının hassas bilgilerini, herhangi bir yasal form ya da denetim olmaksızın hükümet ile paylaşabilecekti. Hükümet de bu bilgileri kendi kurumları arasında paylaşabilecek ve siber güvenlikle ilgili olmayan soruşturmalarda kullanabilecekti. Reitman taslak hakkında şu çarpıcı örneği paylaşıyor. Şirketler e-postalarınızı okuyabilecek, hangi siteleri ziyaret ettiğinizi izleyecek, hangi dosyaları indirdiğinizi takip edecek, bu verileri hükümetle paylaşacak ve bir yasal sorumluluk altına girmeyecekti.

Beyaz Saray da yaptığı açıklamayla “Yurttaşlarımızın mahremiyetinin güvenlik adına kurban edilmesine karşı duruyoruz.” demiş ve tasarının karşısında durmuştur.

Yasa tasarısı kamuoyunun tepkisi sonucunda senatodan geçememiştir.



4. SONUÇ

Yaşadığımız çağ bir distopya çağıdır, gelmesi uzun süredir beklenen bir distopya. İnsanların peşinde koşan gizli teşkilatlara, ajanlara, iz süren dedektiflere gerek yok. Makineler bunu bizim yerimize yapmaya başladılar bile. Bilgi edinmek için girdiğimiz internet siteleri, arkadaşlarımıza yakın olmak için kullandığımız sosyal medya hesapları, eğlenmek için kullandığımız telefon uygulamaları, güvenliğimizi sağladıklarını düşündüğümüz kameralar, böcekten farksız penceremizin önünde bizi izleyen makineler, tweetlerimizi okuyan, depolayan ve değerlendiren yapay zeka uygulamaları, hayatımızı kredi ödemelerimizden, maaşımızdan, borçlarımızdan yani ekonomik veriden ibaret gören, bizi skorlayan, profilimizi çıkaran ve bu profile göre bize yapılacak muameleyi belirleyen banka yazılımları, doğumumuzdan itibaren verilerimizin dijital ortamda depolandığı, geçmişimizden kurtulamadığımız bir çağ. Bu geçmiş ki algoritmaların geleceği tahmin etmek için kullandıkları rakamsal veriler sadece. Gerçekleşmeyen eylemlerimizden sorumlu tutulacağımız, eylememize gerek kalmayacak bir çağ. Masumlüğümüz kanıtlanana kadar herkesin suçlu olduğu, gözetlemenin yaşamımızın her anına yayıldığı bu sistemde güç dengesi ezilenlerin aleyhine bozulmaya devam ediyor. Bu kuralları herkesin olduğu gibi kabul ettiği ise söylenemez. Bir yandan bireyler haklarını davalarla, hukuki mücadele vererek korumaya çalışırken, diğer yandan topluluklar hayatımızı değiştiren bu düzenin sınırlarını çizen yasa tasarılarına, sözleşmelere, anlaşmalara itiraz ediyorlar.

Bu sürecin bir parçası olmanın ve hayatımızın kontrolünü makinelerden önce kendi ellerimize alabilmenin iki yolu var. Yapay zeka, makine öğrenmesi, görüntü işleme, büyük veri gibi teknik konulardan haberdar olmak, günümüzdeki uygulamaları bilmek, hayatımızı nasıl gözetlediklerinin ve etkilediklerinin farkında olmak. İkincisi ise sınırların hala hukuk ile çizildiğini akılda tutarak, yasaları, mevzuatları, kısacası haklarımızı bilmek. Gerisi bizim itiraz etme irademize ve mücadele kararlılığımıza kalıyor.



KAYNAKLAR

- 100 Soruda Kişisel Verilerin Korunması Kanunu.** (2018). Erişim tarihi: 19.11.2019,
<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf>
- ACTA Tehdidi.** (2011). Erişim tarihi: 10.10.2019 Erişim tarihi: 02.10.2019,
<https://blog.piesso.com/posts/acta-tehdidi.html>
- Adalı, E.** (2016). Bilgisayar ve Bilgi Güvenliği ve Yönetimi. İstanbul: İTÜ Ulusal Yazılım ve Sertifikasyon Merkezi.
- Akdeniz, Y.** (2015). Twitter sansürlemede dünya lideriyiz. Erişim tarihi: 15.10.2019,
<http://www.diken.com.tr/twitter-sansurlemede-dunya-lideriyiz/>
- Akdeniz, Y. & Altıparmak, K.** (2014) “Trafik Bilgisi TİB’e verilir” Anayasaya aykırı. Erişim tarihi: 09.10.2019, <https://privacy.cyber-rights.org.tr/?p=1538>
- Akdeniz, Y. & Güven, O.** (2019). Engelliweb 2018: Türkiye’den Erişime Engellenen Web Siteleri, Haber ve Sosyal Medya İçeriklerinin Analiz Raporu. Erişim tarihi: 05.02.2020, https://privacy.cyber-rights.org.tr/wp-content/uploads/2019/06/EngelliWeb_2018.pdf
- AnyVision.** (2018). AnyVision’s full-body scans, which will use AI-powered facial recognition at a London stadium this year so fans can go ticketless. [Fotoğraf]. Erişim tarihi: 15.10.2019,
<https://www.standard.co.uk/tech/ai-face-scanners-will-let-fans-go-ticketfree-at-a-london-stadium-a3868501.html>
- Assange, J., Appelbaum, J., Mler-Maguhn, A. & Zimmermann, J.** (2013). Şifrepunk Özgrlk ve İnternetin Geleceęi zerine Bir Tartışma. İstanbul: Metis Yayınları
- Avrupa İnsan Hakları Sözleşmesi.** (2010). Erişim tarihi: 09.02.2020,
<https://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf>

- Baser, D.** (2018). Hard Questions: What Data Does Facebook Collect When I'm Not Using Facebook, and Why?. Eriřim tarihi: 23.02.2020, <https://about.fb.com/news/2018/04/data-off-facebook/>
- Bauman, Z.** (2000). Liquid Modernity (1. Basım). Cambridge: Polity, 2000
- Bauman, Z. & Lyon, D.** (2013). Akıřkan Gözetim (3. Basım). İstanbul: Polity Press.
- Biddle, S. & Fang, L.** (2020). Location-Tracking Firm Helping Trump Get Reelected Now Wants To Cash In On Coronavirus. Eriřim tarihi: 25.04.2020, <https://theintercept.com/2020/04/09/coronavirus-trump-smartphone-tracking/>
- Blunden, M.** (2018). AI face scanners will let fans go ticket-free at a London stadium. Eriřim tarihi: 07.10.2019, <https://www.standard.co.uk/tech/ai-face-scanners-will-let-fans-go-ticketfree-at-a-london-stadium-a3868501.html>
- BM interneti "temel insan hakkı" olarak kabul etti.** (2016). *Euronews*. Eriřim tarihi: 17.10.2019, <https://tr.euronews.com/2016/07/05/bm-interneti-temel-insan-hakki-olarak-kabul-etti>
- Bozkurt, V.** (2000). Gözetim ve İnternet: Özel Yařamın Sonu mu?. Eriřim tarihi: 02.10.2019, <https://www.birikimdergisi.com/birikim-yazi/2499/gozetim-ve-internet-ozel-yasamin-sonu-mu>
- Brandeis, L. D., Warren, S.** (1890). The Right to Privacy. Eriřim tarihi: 18.09.2019, https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
- Brown, M. S.** (2001). The strange case of United States v. Miller. Eriřim tarihi: 06.11.2019, <http://www.enterstageright.com/archive/articles/0801/0801usvmiller.htm>
- Burgess, M.** (2019). UK police can use controversial facial recognition tech, court rules. Eriřim tarihi: 30.01.2020, <https://www.wired.co.uk/article/police-facial-recognition-south-wales-court-decision>
- Carle, D.** (2011). Leahy, Hatch, Grassley Unveil Targeted Bill To Counter Online Infringement. Eriřim tarihi: 09.11.2019, <https://www.leahy.senate.gov/press/leahy-hatch-grassley-unveil-targeted-bill-to-counter-online-infringement>

- Case of Reklos And Davourlis v. Greece.** (2009). Eriřim tarihi: 07.10.2019,
[https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-90617%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90617%22]})
- Ceza Muhakemesi Kanunu.** (2004). Eriřim tarihi: 11.12.2019,
<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf>
- Chowdhry, A.** (2012). Facebook's DeepFace Software Can Match Faces With 97.25% Accuracy. Eriřim tarihi: 14.12.2019,
<https://www.forbes.com/sites/amitchowdhry/2014/03/18/facebooks-deepface-software-can-match-faces-with-97-25-accuracy/#476eb3a754fc>
- Confessore, N.** (2018). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. Eriřim tarihi: 11.04.2020,
<https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>
- Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures.** (2020). Eriřim tarihi: 01.05.2020,
https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670
- Dağsalı, B.** (t.y.). Kiřisel Verilerin Korunması Kanununun Uygulanma Süreci. Eriřim tarihi: 11.04.2020, <http://yasaizleme.org.tr/kisisel-verilerin-korunmasi-kanununun-uygulanma-sureci/>
- Dereli, M. D.** (2015). Sosyal Medya ve Biz: Bir Daha Asla Yalnız Kal(a)mamak. Eriřim tarihi: 09.10.2019, <http://ayvakti.net/?p=2934>
- DeVries, J. Krolık, A. & Singer, N.** (2020). A Scramble for Virus Apps That Do No Harm. Eriřim tarihi: 13.05.2020,
<https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>
- Dursun, O.** (2014). İnternet Üzerine Güncel Bir Panorama. LaborComm 2014 5. Uluslararası İşçi ve İletişim Konferansı. Eriřim tarihi: 23.09.2019,
https://www.researchgate.net/publication/287216135_LaborComm_2014_-_5_Uluslararası_Işci_ve_İletişim_Konferansı_Bildiriler_Kitabı
- Elektrik Mühendisleri Odası İstanbul Şubesi.** (2006). Gözetim Toplumu Panoptikon. Eriřim tarihi: 23.09.2019,
http://www.emo.org.tr/ekler/dbf17031f5a9c1f_ek.pdf

- E&T editörü.** (2019). Facial recognition technology used by police at derby football match condemned by fans. Erişim tarihi: 04.12.2019, <https://eandt.theiet.org/content/articles/2019/10/use-of-police-facial-recognition-tech-at-football-game-criticised-by-fans/>
- Fierke, K. M.** (2007). Critical approaches to international security. Cambridge, Polity Press.
- Foucault, M.** (1992). Hapishanenin Doğuşu. İstanbul: İmge.
- Gardner, S.** (2014). English Wikipedia anti-SOPA blackout. Erişim tarihi: 11.02.2020, https://foundation.wikimedia.org/wiki/English_Wikipedia_anti-SOPA_blackout
- Greece.** (2020). Erişim tarihi: 29.04.2020, https://www.echr.coe.int/Documents/CP_Greece_ENG.pdf
- Griswold v. Connecticut, 381 U.S. 479 (1965).** (t.y.). Erişim tarihi: 08.10.2019, <https://supreme.justia.com/cases/federal/us/381/479/>
- Gromov G.** (t.y.). Roads and Crossroads of the Internet History. Alındığı tarih: 25.09.2019. Erişim tarihi: 15.10.2019, http://www.netvalley.com/cgi-bin/intval/net_history.pl?chapter=1
- H.R.3523 - Cyber Intelligence Sharing and Protection Act.** (2012). Erişim tarihi: 29.10.2019, <https://www.congress.gov/bill/112th-congress/house-bill/3523/text>
- Harel, A.** (2017). Israel Speeds Up Camera Placements in West Bank in Effort to Deter Terrorism. Erişim tarihi: 21.09.2019, <https://www.haaretz.com/israel-news/.premium-idf-speeds-up-camera-placements-in-w-bank-in-effort-to-deter-terrorism-1.5485764>
- Head, T.** (2019). Where Did the Right to Privacy Come From?. Erişim tarihi: 29.12.2019, <https://www.thoughtco.com/right-to-privacy-history-721174>
- Inclusion in National Sex Offender Database Did Not Infringe The Right To Respect For Private Life.** (2009). Erişim tarihi: 09.10.2019, <https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-4480954-5400075&filename=003-4480954-5400075.pdf>
- Johnson, G.** (2014). Turkey tries to block Twitter, is met with worldwide ridicule. Erişim tarihi: 08.11.2019,

<https://www.latimes.com/world/worldnow/la-fg-wn-turkey-twitter-flap-20140321-story.html#axzz2wcaFYDgd>

Kang, C. (2011). House introduces Internet piracy bill. Eriřim tarihi: 16.11.2019, https://www.washingtonpost.com/blogs/post-tech/post/house-introduces-internet-piracy-bill/2011/10/26/gIQA0f5xJM_blog.html

Kasapoğlu, Ç. (2020). Koronavirüs: Türkiye ve dünyadaki temas takip uygulamaları güvenli mi, hak ve mahremiyet ihlallerine yol açar mı?. Eriřim tarihi: 13.05.2020 <https://www.bbc.com/turkce/haberler-dunya-52638919>

Katz v. United States, 389 U.S. 347 (1967). (t.y.). Eriřim tarihi: 18.10.2019, <https://supreme.justia.com/cases/federal/us/389/347/>

Kelion, L. (2020). Apple and Google release marks 'watershed moment' for contact-tracing apps. Eriřim tarihi: 13.05.2020, <https://www.bbc.com/news/technology-52740131>

Kişisel Verileri Koruma Kurumu. (t.y.). Eriřim tarihi: 17.01.2020 <https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler>

Kişisel Verilerin Korunması Kanunu. (2016). Eriřim tarihi: 12.01.2020, <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>

Leander v. Sweden , 26 March 1987, 9 EHRR 433, para. 74 (t.y.). Eriřim tarihi: 18.10.2019, http://www.hrcr.org/safrica/access_information/ECHR/Leander.html

Linux Kullanıcıları Derneği. (t.y.). Eriřim tarihi: 10.10.2019, <http://www.lkd.org.tr/>

Lyon, D. (2003) Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination (1. Basım). Londra: Routledge, 2003

Mahkeme kararı olmaksızın: Wikipedia'ya 'imaj' gerekçeli erişim engeli geldi. (2017). *Diken*. Eriřim tarihi: 11.02.2020, <http://www.diken.com.tr/mahkeme-karari-olmaksizin-wikipediaya-imaj-gerekceli-erisim-engeli-geldi/>

McCullagh, D. (2012). Opposition grows to CISA 'Big Brother' cybersecurity bill. Eriřim tarihi: 25.12.2019, <https://www.congress.gov/bill/112th-congress/house-bill/3523/text>

McMullan, T. (2017). What does the panopticon mean in the age of digital surveillance? [Fotoğraf]. Eriřim tarihi: 02.10.2019,

<https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham#img-3>

McMullan, T. (2017). What does the panopticon mean in the age of digital surveillance?. [Fotoğraf]. Erişim tarihi: 02.10.2019, <https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham#img-2>

Mcsherry, C & Eckersley, P. (2011). Hollywood's New War on Software Freedom and Internet Innovation. Erişim tarihi: 17.01.2020, <https://www.eff.org/deeplinks/2011/11/hollywood-new-war-on-software-freedom-and-internet-innovation>

Mentha, I. (2020). China's coronavirus detection app is reportedly sharing citizen data with police. Erişim tarihi: 30.04.2020, <https://thenextweb.com/china/2020/03/03/chinas-covid-19-app-reportedly-color-codes-people-and-shares-data-with-cops/>

Nimmer M. (1954). The Right of Publicity. Erişim tarihi: 17.10.2019, <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2595&context=lcp>

Open Letter From Cybersecurity Experts. (t.y.) Erişim tarihi: 17.10.2019 Erişim tarihi: 02.10.2019, <https://www.eff.org/deeplinks/2012/04/open-letter-academics-and-engineers-us-congress>

Öymen, E. (2016). İnternete erişim insan hakkı mıdır?. Erişim tarihi: 10.11.2019, <https://www.dunya.com/kose-yazisi/internete-erisim-insan-hakki-midir/29094>

PIPA Law. (2011). Erişim tarihi: 06.10.2019, <https://www.checkforplagiarism.net/plagiarism-law>

Prosser W. L., (1960). Privacy. Erişim tarihi: 15.10.2019, <https://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1/>

Reitman, R. (2012). CISPA Is Dangerously Vague. Erişim tarihi: 19.11.2019, <https://www.usnews.com/debate-club/should-the-congress-pass-cispa/cispa-is-dangerously-vague>

Reynolds, M. (2018). Facebook and Google's race to connect the world is heating up. Erişim tarihi: 09.12.2019, <https://www.wired.co.uk/article/google-project-loon-balloon-facebook-aquila-internet-africa>

Roagna, I. (2012). Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması. Erişim tarihi:

18.10.2019,

http://www.inhak.adalet.gov.tr/inhak_bilgi_bankasi/el_kitaplari/ozel_hayata_saygi.pdf

Rotaru v Romania. (2000). Erişim tarihi: 18.10.2019, <https://swarb.co.uk/rotaru-v-romania-echr-4-may-2000/>

Schneider G., Evans J. & Pinard K. (2010). The Internet (6. basım). Boston: Course Technology.

Schuppe, J. (2018). Facial recognition gives police a powerful new tracking tool. It's also raising alarms. Erişim tarihi: 20.11.2019, <https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936?cid=related>

Simonite, T. (2014). Facebook Creates Software That Matches Faces Almost as Well as You Do. Erişim tarihi: 02.10.2019, <https://www.technologyreview.com/s/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/>

Solon, O. (2019). Facial recognition's 'dirty little secret': Millions of online photos scraped without consent. Erişim tarihi: 15.02.2020, <https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921>

Solon, O. (2019). Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?. Erişim tarihi: 15.02.2020, https://www.nbcnews.com/news/amp/ncna1072116?__twitter_impression=true

Solon, O. (2012). What is Acta and why should you be worried about it?. Erişim tarihi: 15.02.2020, <https://www.wired.co.uk/article/acta-101>

Strickland, J. (2012). How Protect IP Works. Erişim tarihi: 04.10.2019, <https://computer.howstuffworks.com/protect-ip1.htm>

Surveillance of Protests and the Right to Privacy. (2009). Erişim tarihi: 09.10.2019, <https://www.hrlc.org.au/human-rights-case-summaries/wood-v-commissioner-of-police-for-the-metropolis-2009-ewca-civ-414-21-may-2009>

The Right of Privacy The Issue: Does the Constitution protect the right of privacy? If so, what aspects of privacy receive protection?. (t.y.). Erişim tarihi: 15.01.2020,

<http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html>

Twitter yasağı kalktı. (2014). *Milliyet*. Erişim tarihi: 02.10.2019,
<http://www.milliyet.com.tr/gundem/twitter-yasagi-kalkti-1861721>

T.C. Sağlık Bakanlığı Filyasyon Ve İzolasyon Takip Sistemi(Fitas) Kullanıcı Sözleşmesi Ve Mahremiyet Politikası (t.y.). Erişim tarihi: 25.05.2020, <https://hsys.saglik.gov.tr/mobil/gizlilik>

Tribe Legis Memo on SOPA. (2011). Erişim tarihi: 23.10.2019,
<https://www.scribd.com/document/75153093/Tribe-Legis-Memo-on-SOPA-12-6-11-1>

Türkiye Cumhuriyeti Anayasası. (1982). Erişim tarihi: 22.10.2019,
https://www.tbmm.gov.tr/anayasa/anayasa_2018.pdf

Types of Body Language. (2007). Erişim tarihi: 21.10.2019,
<https://www.simplybodylanguage.com/types-of-body-language.html>

Url-1 <<https://ourworldindata.org/grapher/percentage-of-young-people-engaging-in-social-networking-online>>, [Fotoğraf], erişim tarihi 05.01.2020.

Url-2 <<https://cbsnews1.cbsstatic.com/hub/i/2014/03/19/0b070139-130d-4207-9e83-a368fb802a0b/screenshot-of-study-copy.jpg>>, [Fotoğraf], erişim tarihi 05.01.2020.

Url-3 <<https://www.standard.co.uk/tech/ai-face-scanners-will-let-fans-go-ticketfree-at-a-london-stadium-a3868501.html>>, [Fotoğraf], erişim tarihi 20.02.2020.

Url-4 <<https://home.cern/science/computing/birth-web/short-history-web>>, [Fotoğraf], erişim tarihi 20.02.2020.

Url-5 <<https://ourworldindata.org/grapher/share-of-individuals-using-the-internet?tab=chart>>, [Fotoğraf], erişim tarihi 20.02.2020.

Url-6 <<https://ourworldindata.org/grapher/broadband-penetration-by-country?tab=map&time=2001..2017&country=TUR>>, [Fotoğraf], erişim tarihi 22.02.2020.

Van Kück v. Germany. (2003). Erişim tarihi: 18.10.2019,
<https://www.globalhealthrights.org/health-topics/health-care-and-health-services/van-kuck-v-germany/>

Wikipedi. (2020). Wikimedia Foundation Inc. ve diğerleri. Erişim tarihi: 06.03.2020,
https://tr.wikipedia.org/wiki/Wikimedia_Foundation_Inc._ve_di%C4%9Ferleri

Von Hannover v Germany: Echr 24 Jun 2004. (2004). Erişim tarihi: 18.10.2019,
<https://swarb.co.uk/von-hannover-v-germany-echr-24-jun-2004/>

- Websites blackout in SOPA anti-piracy protest.** (2012). Erişim tarihi: 19.10.2019, <https://www.news.com.au/technology/websites-blackout-in-sopa-anti-piracy-protest/news-story/2ef306ec0c98c988712ea9c0629c0252>
- Where the Web was Born.** (t.y.). Erişim tarihi: 16.01.2020, <https://home.cern/science/computing/birth-web/short-history-web>
- Whittaker, Z.** (2012). 'Last rites' for ACTA? Europe rejects antipiracy treaty. Erişim tarihi: 02.10.2019, <https://www.cnet.com/news/last-rites-for-acta-europe-rejects-antipiracy-treaty/>
- Wikipedia engellendi.** (2017). *Gazete Duvar*. Erişim tarihi: 11.02.2020, <https://www.gazeteduvar.com.tr/teknoloji/2017/04/29/wikipedia-engellendi/>
- Wikipedia erişim yasağı AIHM'de: Türkiye'nin uyguladığı yasağın nedeni ne, hangi adımlar atıldı?.** (2019). *BBC News Türkçe*. Erişim tarihi: 11.02.2020, <https://www.bbc.com/turkce/haberler-dunya-48380473>
- Wikipedia'ya erişim açıldı.** (2020). *Birgün*. Erişim tarihi: 11.02.2020, <https://www.birgun.net/haber/wikipedia-ya-erisim-acildi-284093>
- Yüksel, S.** (2012). *Özel Yaşamın Bir Parçası Olarak. Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale* (1. Basım). İstanbul: Beta
- Z v Finland: ECHR 25 Feb 1997.** (2019). Erişim tarihi: 18.10.2019, <https://swarb.co.uk/z-v-finland-echr-25-feb-1997/>



ÖZGEÇMİŞ

Ad Soyad: İsmail Cem Bakır
Doğum Yeri ve Tarihi: Erzincan, 03.07.1990
E-Posta: icembakir@gmail.com

ÖĞRENİM DURUMU:

- **Lisans:** 2014, İTÜ, Bilgisayar Mühendisliği
- **Yüksek Lisans:** 2020, İTÜ, Bilgi ve Haberleşme Mühendisliği

MESLEKİ DENEYİM:

- 2014 yılında başladığı bilgisayar mühendisliği kariyerinde sırasıyla lojistik, bankacılık, uluslararası göç ve uluslararası havacılık alanlarında yazılım geliştirmesi yaptı.
- 2017 yılında Cenevre’de Birleşmiş Milletler Uluslararası Göç Örgütü’nün mülteci ve göçmenler için geliştirmiş olduğu bir yazılım projesinde yazılım mühendisi olarak 1 sene boyunca rol aldı.
- Kariyerine Amadeus A.Ş’de deneyimli yazılım mühendisi olarak devam etmektedir.